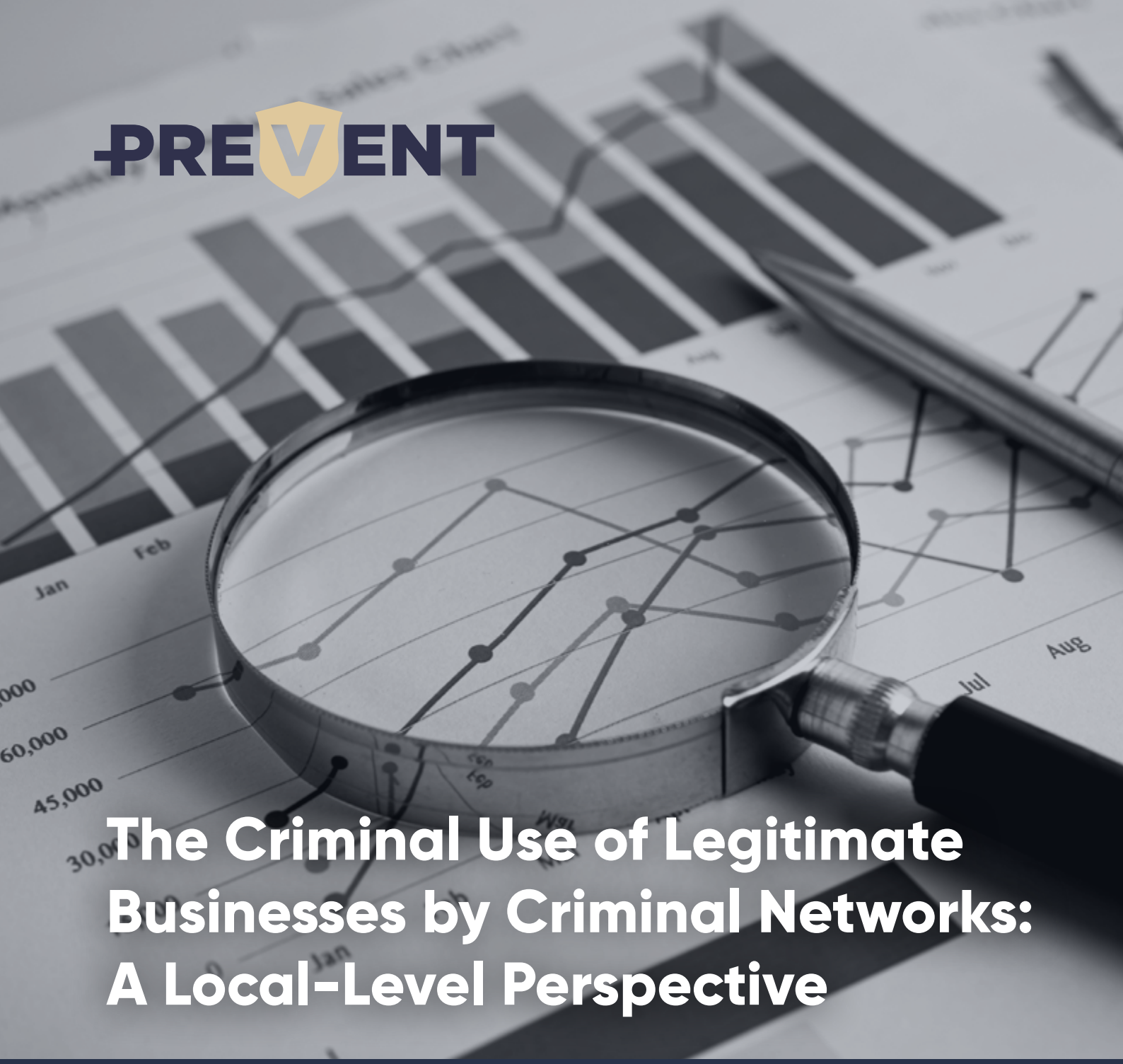


The Criminal Use of Legitimate Businesses by Criminal Networks: A Local-Level Perspective

Case Studies from Nine European Cities

The Criminal Use of Legitimate Businesses by Criminal Networks: A Local-Level Perspective

Case Studies from Nine European Cities

PREVENT

Final Report of Work Package 3 (WP 3) of Project PREVENT – Building Capacity against High-Risk Criminal Networks in the European Union: From an Improved Intelligence Picture towards an Integrated Prevention Approach.

Editors:

Jelle Janssens, Fleur Soete & Billie Baetens

Authors:

Antwerp & Brussels: **Billie Baetens & Fleur Soete** (Universiteit Gent)
Caserta: **Caterina Scialla & Mauro Baldascino** (Università degli Studi di Napoli Federico II – UNINA); **Piera Lepore** (Idee in Rete)
Frankfurt: **Sonja John** (Hessian University of Applied Sciences for Public Management and Security) & **Klaus von Lampe** (Berlin School of Economics and Law)
Madrid: **Jesús Palomo & Luis Vallés** (Fundación para la Investigación Aplicada en Delincuencia y Seguridad – FIADYS)
Paris: F**abrice Rizzoli & Louis Gomes** (Crim'HALT)
Sofia: A**tanas Rusev & Ryan McLaren** (Center for the Study of Democracy – CSD)
Stockholm: J**ohanna Skinnari & Karim Zakhour** (Brå)
Utrecht: **Lienke Hutten, Joeri Vig, Lars Merkus, Johanne Nielsen & Noa Hardy** (Centrum voor Criminaliteitspreventie en Veiligheid – CCV)

Co-funded by the European Union

This publication reflects the views of the author(s) only. Neither the European Union, the European Commission, nor the Associated Partners can be held responsible for the opinions expressed.

This work is licensed under the Creative Commons Atribution-NonCommercial-NoDerivatives 4.0 International License.

Cover photo: Canva

TABLE OF CONTENTS

Table of contents

List of abbreviations 14
List of tables 16
List of figures 16
1. Introduction 17
1.1 Background and objectives 18
1.1.1 General objectives of PREVENT 18
1.1.2 Objectives of the report 18
1.2 Problem statement: criminal use of the legal economy by criminal networks at the local level 19
1.3 Structure of the report 20
2. Definitions of central concepts 21
2.1 Criminal network 22
2.2 Criminal use of legitimate businesses 22
2.2.1 Criminal ownership and control of legitimate businesses 23
2.2.2 Criminal infiltration into legitimate businesses 23
2.2.3 Criminal use or abuse of bona fide businesses and services 24
2.3 Economic (sub)sector 24
3. Criminal use of the legal economy: an overview 25
3.1 Tensions between legitimate and criminal entrepreneurship 26
3.2 Motivators and drivers of criminal networks' use of the legitimate economy 26
3.3 Modus operandi: methods of criminal use of the legitimate economy 28
3.4 Opportunities and vulnerabilities within the legitimate economy 31
3.4.1 Geographical vulnerabilities 31
3.4.2 Sectoral vulnerabilities 31
3.4.3 Business-level vulnerabilities 32
3.5 Financial profile of criminal networks 34
3.6 Criminal activities enabled by the criminal use of the legitimate economy 36
4. Methodology 39
4.1 Selection of case studies 40
4.2 Data collection 41
4.3 Data analysis 43
5. Antwerp – Empirical results 45
5.1 Introduction: Belgium 46
5.1.1 Background and context 46
5.1.2 Data and methodology 46

5.1.3 Critical remarks 47
5.1.4 Identification of vulnerable (sub)sectors in Antwerp 47
5.2 Case Alfa: Laundering Cocaine Profits in Antwerp 49
5.3 Case Bravo: Infiltrating Antwerp's Logistics Chain 49
5.4 Case Charlie: From Cannabis to Concrete 49
6. Brussels – Empirical results 50
6.1 Identification of vulnerable (sub)sectors in Brussels 51
6.2 Case Delta: The Brussels Brazilian Filière 52
6.3 Case Echo: Façades and False Invoices 53
6.4 Case Foxtrot: Games of Chance and Channels of Cash 53
6.5 Financial investigations in Belgium: key challenges and recommendations 53
6.5.1 Challenges in financial investigations in Belgium 53
6.5.2 Recommendations for improving financial investigations in Belgium 57
6.6 Summary of research findings: Belgium (Antwerp and Brussels) 60
7. Caserta – Empirical results 63
7.1 Introduction 64
7.1.1 Background and context 64
7.1.2 Data and methodology 66
7.1.3 Identification of vulnerable (sub)sectors 66
7.2 Case Golf: The Prince and the Ballot Scheme 67
7.3 Case Hotel: From Waste to Wealth 67
7.4 Case India: Gambling as Governance 68
7.5 Case Juliett: Agri-Food Routes to Crime 68
7.6 Financial investigations in Italy: key challenges and recommendations 68
7.6.1 Challenges in financial investigations in Italy 68
7.6.2 Recommendations for improving financial investigations in Italy 70
7.7 Summary of research findings: Caserta 71
8. Frankfurt – Empirical results 74
8.1 Introduction 75
8.1.1 Background and context 75
8.1.2 Data and methodology 76
8.1.3 Identification of vulnerable (sub)sectors 77
8.2 Case Kilo: The Corrupt Cargo Chain 77
8.3 Case Lima: Hidden Hubs, Hidden Hauls 77
8.4 Case Mike: Dining with Dealers 77

8.5 Financial investigations in Germany: key challenges and recommendations 78
8.6 Summary of research findings: Frankfurt 80
9. Madrid – Empirical results 81
9.1 Introduction 82
9.1.1 Background and context 82
9.1.2 Data and methodology 83
9.1.3 Critical remarks 83
9.1.4 Identification of vulnerable (sub)sectors 85
9.2 Case November: The Cartel's Cannabis Network 87
9.3 Case Oscar: Chinese Connections and Criminal Cashflows 87
9.4 Case Papa: Banking on Fame 88
9.5 Summary of research findings: Madrid 88
10. Paris – Empirical results 90
10.1 Introduction 91
10.1.1 Background and context 91
10.1.2 Data and methodology 91
10.1.3 Critical remarks 92
10.1.4 Identification of vulnerable (sub)sectors 92
10.2 Case Quebec: The Luxury Laundering Loop 93
10.3 Case Romeo: Pakistani Forgery and Money Laundering 94
10.4 Case Sierra: Taxi Licence Laundering Scheme 94
10.5 Summary of research findings: Paris 94
11. Sofia – Empirical results 96
11.1 Introduction 97
11.1.1 Background and context 97
11.1.2 Data and methodology 98
11.1.3 Critical remarks 98
11.1.4 Identification of vulnerable (sub)sectors 99
11.2 Case Tango: The Hammers 99
11.3 Case Uniform: Quick Credits 100
11.4 Case Victor: Lords of the Dust 100
11.5 Financial investigations in Bulgaria: key challenges and recommendations 101
11.5.1 Challenges in financial investigations in Bulgaria 101
11.5.2 Recommendations for improving financial investigations in Bulgaria 102
11.6 Summary of research findings: Sofia 103

12. Stockholm – Empirical results 105
12.1 Introduction 106
12.1.1 Background and context 106
12.1.2 Data and methodology 107
12.1.3 Critical remarks 108
12.1.4 Identification of vulnerable (sub)sectors 109
12.2 Case Whiskey: Children in the Care of Criminals 110
12.3 Case X-Ray: Construction and Cash Compensation 110
12.4 Case Yankee: Money, Meat, and MTIC 111
12.5 Financial investigations in Sweden: key challenges and recommendations 111
12.5.1 Challenges in financial investigations in Sweden 111
12.5.2 Recommendations for improving financial investigations in Sweden 112
12.6 Summary of research findings: Stockholm 113
13. Utrecht – Empirical results 115
13.1 Introduction 116
13.1.1 Background and context 116
13.1.2 Data and methodology 116
13.1.3 Critical remarks 117
13.1.4 Identification of vulnerable (sub)sectors 118
13.2 Case Zulu: The Gold Trading Landscape 119
13.3 Case Alfa-Alfa (AA): Fraudulent Healthcare 120
13.4 Case Bravo-Bravo (BB): From Showroom to Shadow 121
13.5 Financial investigations in the Netherlands: key challenges and recommendations 121
13.5.1 Challenges in financial investigations in the Netherlands 121
13.5.2 Recommendations for improving financial investigations in the Netherlands 121
13.6 Summary of research findings: Utrecht 122
14. Conclusion and discussion 124
14.1 Conclusion: general research findings 125
14.1.1 General conclusions 125
14.1.2 Vulnerable sectors and underlying opportunity structures 126
14.1.3 Recurring patterns throughout the criminal process 127
14.1.4 Financial characteristics of criminal networks 129
14.1.5 Harms associated with the criminal use of legitimate businesses 129
14.2 Limitations of the study 131
14.3 Implications and recommendations for policy and practice 134

15. Bibliography 136
16. Annexes 154
Annex 1: Antwerp – Detailed case studies 155
Annex 1.A – Case Alfa: Laundering Cocaine Profits in Antwerp 155
1. Criminal network involved in Case Alfa 156
2. Legitimate businesses involved in Case Alfa 157
3. Crime script based on Case Alfa 158
4. Financial profile of the criminal network involved in Case Alfa 160
5. Harms caused by Case Alfa 162
Annex 1.B – Case Bravo: Infiltrating Antwerp's Logistics Chain 162
1. Criminal network involved in Case Bravo 162
2. Legitimate businesses involved in Case Bravo 164
3. Crime script based on Case Bravo 165
4. Financial profile of the criminal network involved in Case Bravo 170
5. Harms caused by Case Bravo 171
Annex 1.C – Case Charlie: From Cannabis to Concrete 172
1. Criminal network involved in Case Charlie 172
2. Legitimate businesses involved in Case Charlie 174
3. Crime script based on Case Charlie 174
4. Financial profile of the criminal network involved in Case Charlie 177
5. Harms caused by Case Charlie 178
Annex 2: Brussels – Detailed case studies 181
Annex 2.D – Case Delta: The Brussels Brazilian Filière 181
1. Criminal network involved in Case Delta 181
2. Legitimate businesses involved in Case Delta 182
3. Crime script based on Case Delta 184
4. Financial profile of the criminal network involved in Case Delta 187
5. Harms caused by Case Delta 188
Annex 2.E – Case Echo: Façades and False Invoices 190
1. Criminal network involved in Case Echo 190
2.Legitimate businesses involved in Case Echo 190
3. Crime script based on Case Echo 192
4. Financial profile of the criminal network involved in Case Echo 193
5. Harms caused by Case Echo 194

Annex 2.F – Case Foxtrot: Games of Chance and Channels of Cash 194
1. Criminal network involved in Case Foxtrot 194
2. Legitimate businesses involved in Case Foxtrot 195
3. Crime script based on Case Foxtrot 195
4. Financial profile of the criminal network involved in Case Foxtrot 197
5. Harms caused by Case Foxtrot 197
Annex 3: Caserta – Detailed case studies 199
Annex 3.G – Case Golf: The Prince and the Ballot Scheme 199
1. Criminal network involved in Case Golf 199
2. Legitimate businesses involved in Case Golf 200
3. Crime script based on Case Golf 201
4. Financial profile of the criminal network involved in Case Golf 205
5. Harms caused by Case Golf 206
Annex 3.H – Case Hotel: From Waste to Wealth 207
1. Criminal network involved in Case Hotel 207
2. Legitimate businesses involved in Case Hotel 208
3. Crime script based on Case Hotel 209
4. Financial profile of the criminal network involved in Case Hotel 213
5. Harms caused by Case Hotel 215
Annex 3.I – Case India: Gambling as Governance 216
1. Criminal network involved in Case India 216
2. Legitimate businesses involved in Case India 217
3. Crime script based on Case India 218
4. Financial profile of the criminal network involved in Case India 223
5. Harms caused by Case India 225
Annex 3.J – Case Juliett: Agri-Food Routes to Crime 226
1. Criminal network involved in Case Juliett 226
2. Legitimate businesses involved in Case Juliett 227
3. Crime script based on Case Juliett 228
4. Financial profile of the criminal network involved in Case Juliett 232
5. Harms caused by Case Juliett 233

Annex 4: Frankfurt – Detailed case studies 234
Annex 4.K – Case Kilo: The Corrupt Cargo Chain 234
1. Criminal network involved in Case Kilo 235
2. Legitimate businesses involved in Case Kilo 235
3. Crime script based on Case Kilo 235
4. Financial profile of the criminal network involved in Case Kilo 237
5. Harms caused by Case Kilo 237
Annex 4.L – Case Lima: Hidden Hubs, Hidden Hauls 237
1. Criminal network involved in Case Lima 237
2. Legitimate businesses involved in Case Lima 237
3. Crime script based on Case Lima 238
4. Financial profile of the criminal network involved in Case Lima 239
5. Harms caused by Case Lima 239
Annex 4.M – Case Mike: Dining with Dealers 239
1. Criminal network involved in Case Mike 239
2. Legitimate businesses involved in Case Mike 240
3. Crime script based on Case Mike 240
4. Financial profile of the criminal network involved in Case Mike 241
Annex 5: Madrid – Detailed case studies 243
Annex 5.N – Case November: The Cartel's Cannabis Network 243
1. Criminal network involved in Case November 243
2. Legitimate businesses involved in Case November 244
3. Crime script based on Case November 245
4. Financial profile of the criminal network involved in Case November 248
5. Harms caused by Case November 250
Annex 5.O – Case Oscar: Chinese Connections and Criminal Cashflows 251
1. Criminal network involved in Case Oscar 251
2. Legitimate businesses involved in Case Oscar 252
3. Crime script based on Case Oscar 253
4. Financial profile of the criminal network involved in Case Oscar 256
5. Harms caused by Case Oscar 257

Annex 5.P – Case Papa: Banking on Fame 257
1. Criminal network involved in Case Papa 257
2. Legitimate businesses involved in Case Papa 258
3. Crime script based on Case Papa 258
4. Financial profile of the criminal network involved in Case Papa 260
5. Harms caused by Case Papa 261
Annex 6: Paris – Detailed case studies 264
Annex 6.Q – Case Quebec: The Luxury Laundering Loop 264
1. Criminal network involved in Case Quebec 264
2. Legitimate businesses involved in Case Quebec 265
3. Crime script based on Case Quebec 265
4. Financial profile of the criminal network involved in Case Quebec 268
5. Harms caused by Case Quebec 269
Annex 6.R – Case Romeo: Pakistani Forgery and Money Laundering 270
1. Criminal network involved in Case Romeo 270
2. Legitimate businesses involved in Case Romeo 271
3. Crime script based on Case Romeo 271
4. Financial profile of the criminal network involved in Case Romeo 274
5. Harms caused by Case Romeo 274
Annex 6.S – Case Sierra: Taxi Licence Laundering Scheme 275
1. Criminal network involved in Case Sierra 275
2. Legitimate businesses involved in Case Sierra 275
3. Crime script based on Case Sierra 276
4. Financial profile of the criminal network involved in Case Sierra 277
5. Harms caused by Case Sierra 278
Annex 7: Sofia – Detailed case studies 280
Annex 7.T – Case Tango: The Hammers 280
1. Criminal network involved in Case Tango 280
2. Legitimate businesses involved in Case Tango 280
3. Crime script based on Case Tango 281
4. Financial profile of the criminal network involved in Case Tango 283
5. Harms caused by Case Tango 284

Annex 7.U – Case Uniform: Quick Credits 284
1. Criminal network involved in Case Uniform 284
2. Legitimate businesses involved in Case Uniform 285
3. Crime script based on Case Uniform 286
4. Financial profile of the criminal network involved in Case Uniform 291
5. Harms caused by Case Uniform 292
Annex 7.V – Case Victor: Lords of the Dust 293
1. Criminal network involved in Case Victor 293
2. Legitimate businesses involved in Case Victor 294
3. Crime script based on Case Victor 294
4. Financial profile of the criminal network involved in Case Victor 301
5. Harms caused by Case Victor 302
Annex 8: Stockholm – Detailed case studies 304
Annex 8.W – Case Whiskey: Children in the Care of Criminals 304
1. Background: foster care in Sweden 304
2. Criminal network involved in Case Whiskey 305
3. Legitimate businesses involved in Case Whiskey 306
4. Crime script based on Case Whiskey 306
5. Financial profile of the criminal network involved in Case Whiskey 311
6. Harms caused by Case Whiskey 312
Annex 8.X – Case X-Ray: Construction and Cash Compensation 313
1. Criminal network involved in Case X-Ray 313
2. Legitimate businesses involved in Case X-Ray 315
3. Crime script based on Case X-Ray 316
4. Financial profile of the criminal network involved in Case X-Ray 319
5. Harms caused by Case X-Ray 320
Annex 8.Y – Case Yankee: Money, Meat, and MTIC 321
1. Legitimate businesses involved in Case Yankee 321
2. Criminal network involved in Case Yankee 321
3. Crime script based on Case Yankee 323
4. Financial profile of the criminal network involved in Case Yankee 326
5. Harms caused by Case Yankee 327

Annex 9: Utrecht – Detailed case studies 330
Annex 9.Z – Case Zulu: The Gold Trading Landscape 330
1. Criminal network involved in Case Zulu 330
2. Legitimate businesses involved in Case Zulu 330
3. Crime script based on Case Zulu 331
4. Financial profile of the criminal network involved in Case Zulu 333
5. Harms caused by Case Zulu 333
Annex 9.AA – Case Alfa-Alfa: Fraudulent Healthcare 334
1. Criminal network involved in Case Alfa-Alfa (AA) 334
2. Legitimate businesses involved in Case Alfa-Alfa (AA) 336
3. Crime script based on Case Alfa-Alfa (AA) 336
4. Financial profile of the criminal network involved in Case Alfa-Alfa (AA) 339
5. Harms caused by Case Alfa-Alfa (AA) 340
Annex 9.BB – Case Bravo-Bravo: From Showroom to Shadow 341
1. Criminal network involved in Case Bravo-Bravo (BB) 341
2. Legitimate businesses involved in Case Bravo-Bravo (BB) 341
3. Crime script based on Case Bravo-Bravo (BB) 342
4. Financial profile of the criminal network involved in Case Bravo-Bravo (BB) 343
5. Harms caused by Case Bravo-Bravo (BB) 344
Annex 10: Methodological annexes 346
Annex 10.1 − Guide for the identification of five economic sub-sectors 346
Annex 10.2 − Overview of Belgian respondents 347
Annex 10.3 − Overview of Italian respondents 347

List of abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BGN	Bulgarian Lev
CaaS	Crime-as-a-Service
CBD	Cannabidiol
CSA	Crime Script Analysis
CTF	Counter-Terrorist Financing
DIA	Anti-Mafia Investigative Department (*Direzione Investigativa Antimafia*)
EU	European Union
EORI	Economic Operator Registration and Identification
FATF	Financial Action Task Force
FCS	Financial Crime Scripting
FIU	Financial Intelligence Unit
FJP	Federal Judicial Police
GP	General Partnership
HRCN	High Risk Criminal Network
ITL	Italian Lire
IVTS	Informal Value Transfer Systems
KYC	Know Your Customer
LEA	Law Enforcement Agency
LLC	Limited Liability Company
LP	Limited Partnership
LTD	Private Limited Company
MS	Member State(s)
MTIC	Missing Trader Intra-Community
OSS	One-Stop Shop
PGB	Personal Care Budget (*Persoonsgebonden Budget*)

PLC	Public Limited Company
PSP	Payment Service Provider
RIEC	Regional Information and Expertise Centre (the Netherlands)
TAR	Truck Appointment Reference
THC	Tetrahydrocannabinol
SBML	Service-Based Money Laundering
SEK	Swedish Krona
TBML	Trade-Based Money Laundering
THB	Trafficking in Human Beings
VAT	Value Added Tax
WP	Work Package

List of tables

Table 1: Interview protocol: Core topics, subtopics, and guiding questions 41
Table 2: Overview of the core members of the criminal network involved in Case Alfa 156
Table 3: Overview of the businesses involved in Case Alfa 157
Table 4: Overview of the core members of the criminal network involved in Case Bravo 163
Table 5: Overview of the businesses involved in Case Bravo 164
Table 6: Overview of the members of the criminal network involved in Case Charlie 173
Table 7: Overview of the core members of the criminal network involved in Case Delta 181
Table 8: Overview of the businesses involved in Case Delta 182
Table 9: Overview of the core members of the criminal network involved in Case Echo 190
Table 10: Overview of the businesses involved in Case Echo 191
Table 11: Overview of the core members of the criminal network involved in Case Golf 199
Table 12: Overview of the businesses involved in Case Golf 200
Table 13: Overview of the core members of the criminal network involved in Case Hotel 207
Table 14: Overview of the core members of the criminal network involved in Case India 216
Table 15: Overview of the core members of the criminal network involved in Case Juliett 226
Table 16: Overview of the core members of the criminal network involved in Case Romeo 270
Table 17: Overview of the core members of the criminal network involved in Case Whiskey 305
Table 18: Overview of the core members of the criminal network involved in Case X-Ray 313
Table 19: Overview of the businesses involved in Case Yankee 321
Table 20: Overview of the core members of the criminal network involved in Case Yankee 322
Table 21: Respondents interviewed as part of the Belgian (BE) data collection process 347
Table 22: Respondents interviewed as part of the Italian (IT) data collection process 347

List of figures

Figure 1: Geographical distribution of the nine cities included in the study 40
Figure 2: Most prevalent economic sectors identified across the case studies 126
Figure 3: Structure of the criminal network involved in Case Charlie 172

INTRODUCTION

1.1 Background and objectives

1.1.1 General objectives of PREVENT

The **PREVENT project** was carried out with the financial support of the Internal Security Fund (ISF) of the European Commission; DG Home Affairs.[1] This multi-country project focuses on preventing and fighting high-risk criminal networks (HRCNs) in Europe. Its consortium consists of nine partners (universities, public institutions, and civil society organisations) in six EU Member States, supported by thirteen associated partners (law enforcement agencies, asset recovery offices, and local authorities). The project's general objective is to **tackle HRCNs** by contributing to a better intelligence picture of their criminal use of the legal economy and by promoting an integrated preventive approach, including the application of administrative measures and the implementation of the social re-use of confiscated assets.

1.1.2 Objectives of the report

This report presents the final results of **Work Package 3** (WP3) of the PREVENT project. This WP specifically aimed to improve the intelligence picture of the business activities used by criminal networks, and to enhance the understanding of networks' financial profiles and of the nature of the harms caused by their use of legitimate businesses at a local level. This report outlines the step-by-step process of the **criminal use of the legal economy**, based on in-depth sub-sector case studies in nine cities across eight EU Member States.[2] Hence, it forms the basis for the work of WP4 within the PREVENT project, which aims to develop a barrier model that also incorporates administrative measures in order to effectively prevent and tackle criminal networks exploiting legitimate business structures.

WP3 was carried out by a **consortium of nine partners** from universities, research centres, and external experts within eight EU Member States:

- Ghent University (**UGent**, Belgium) – in charge of WP3 coordination;
- Katholieke Universiteit Leuven (**KU Leuven**, Belgium);
- Centre for the Study of Democracy (**CSD**, Bulgaria);
- University of Naples (**UNINA**, Italy);
- Centre for Crime Prevention and Safety (**CCV**, The Netherlands);
- Fundación Para La Investigación Aplicada En Delincuencia Y Seguridad (**FIADYS**, Spain);
- Swedish National Council for Crime Prevention (**Brå**, Sweden);
- External experts conducting research in France;
- External experts conducting research in Germany.

[1] The project is officially titled "*Building Capacity against High-Risk Criminal Networks in the European Union: From an Improved Intelligence Picture towards an Integrated Prevention Approach*".

[2] The cities included in the case studies are: Antwerp and Brussels (Belgium); Caserta (Italy); Frankfurt (Germany); Madrid (Spain); Paris (France); Sofia (Bulgaria); Stockholm (Sweden); Utrecht (The Netherlands) (see Chapter 4).

1.2 Problem statement: criminal use of the legal economy by criminal networks at the local level

Modern societies increasingly promote and strengthen the principle of 'free enterprise' through practices of deregulation and the removal of entrepreneurial restrictions. Article 16 of the Charter of Fundamental Rights of the European Union[3] also recognises the freedom to pursue an economic or commercial activity, in accordance with national laws and practices. However, **free entrepreneurship** inadvertently creates opportunities for criminal entrepreneurship, as legitimate businesses have become key multi-functional tools for criminal networks (CTIF-CFI, 2022; LIEC, 2019; Wittevrongel & De Jaeger, 2024). Over time, the strategies of criminal networks have evolved: whereas they previously primarily relied on subversion and violence, they now increasingly resort to submersion, using the legitimate economy as a key tool (Savona & Riccardi, 2018). As a result, the gap between legal and black markets, often conceptualised as the 'upperworld' and the 'underworld', is narrowing (Anderson, 1995; Janssens et al., 2023).

According to Europol (2024b), 86 percent of the most threatening networks in the EU use legal business structures as part of their business model. The use of legitimate businesses can be an **intrinsic part** of the crime areas in which criminal networks operate and of their *modus operandi*, or it can serve as an important facilitator of criminal activities (Europol, 2024a). It enables criminal networks to carry out illegal practices, conceal criminal activities, and launder illicit profits; both systematically and temporarily. Although some sectors, such as logistics, hospitality, and construction, are particularly at risk, virtually no sector of the legitimate economy remains untouched by organised crime (European Commission, 2023a; Europol, 2024a, 2024b, 2025, 2026). Furthermore, criminal networks using the legitimate economy are constantly adapting their practices to changing laws and regulations, and their techniques are rapidly evolving due to technological and geopolitical developments (Janssens et al., 2023; Lam et al., 2018).

The criminal use of the legal economy by criminal networks has **numerous implications** for various parties. Not only are direct (individual) victims and legitimate businesses affected (and harmed), but it also entails broader economic and social consequences (Greenfield & Paoli, 2022; McDowell & Novis, 2001; Pinotti, 2015). Since it allows organised crime to gain power and influence, it creates a self-sustaining cycle that seriously threatens the foundations of society (Europol, 2025). It poses a significant risk to the integrity of the financial system, as it disrupts a fair market competition, discourages investment, and fosters an environment of economic inefficiency. Within the countries affected, it also leads to corruption, feelings of insecurity, the erosion of trust in the rule of law and democratic institutions, and lower levels of societal and economic growth (Europol, 2024b). Furthermore, such practices can cause damage to the physical environment, for example by affecting air quality or wildlife (Greenfield & Paoli, 2022).

[3] Art. 16 of the Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, 18 December 2000.

Although criminal networks operate globally, they are often deeply rooted in the local community and invest locally (Europol, 2024a; Janssens et al., 2023). Accordingly, the impact of organised crime tends to be most directly and clearly felt at the municipal level (Tops & van der Torre, 2024). However, research on this topic has predominantly been conducted at the country-level, most notably by Transcrime in the OCP (2015), ARIEL (2015) and MORE (2018) projects (see: Savona & Berlusconi, 2015; Savona & Riccardi, 2015, 2018). While these extensive research projects provide useful insights, they offer little information about the methods used to influence and infiltrate legitimate businesses **at the local level** (Janssens et al., 2023; Savona & Berlusconi, 2015). Nevertheless, this local level determines the context in which the criminal use of the legal economy can emerge and flourish, as well as the patterns through which it develops (LIEC, 2019). To enhance understanding of these issues and to address this research gap, this report adopts a local-level focus through in-depth case studies.

1.3 Structure of the report

This report is structured as follows: **Chapter 2** contains (working) definitions of the relevant concepts. **Chapter 3** provides an overview of the relevant literature on the criminal use of the legal economy, with an emphasis on the main drivers, *modus operandi*, and characteristics of 'vulnerable' sectors and businesses. Subsequently, **Chapter 4** describes the methodological approach. **Chapters 5-13** present the (summarised) findings of the analysis for each city examined. Finally, **Chapter 14** discusses the general conclusions and implications of this report, both in terms of research and policy.

The detailed empirical results of the case studies (28 in total) are presented in **Annexes 1-9**, organised by city. Each annex contains a detailed analysis of the cases, structured consistently around the various 'steps' in the process of the criminal use of the legal economy (Motivation; Preparation; Pre-activity; Activity; Post-activity), as well as the financial profile of the criminal networks and the harms caused. Additional information regarding methodological issues is provided in **Annex 10.**

DEFINITIONS OF CENTRAL CONCEPTS

Note: The 'definitions' provided in this chapter should be understood as 'working definitions'. They were developed (or adopted and/or modified) within the context of the PREVENT project to ensure a shared understanding of key concepts among project partners, rather than as formal or universally accepted theoretical definitions.

2.1 Criminal network

In recent decades, both academic and policy discourse on organised crime has increasingly shifted from the term 'organised crime group' to that of '**criminal network**' (Campana, 2016; Europol, 2021, 2025, 2026; Varese, 2010). This shift is indicative of broader developments within the organised crime landscape, including the reduced presence of large-scale, well-structured criminal organisations such as traditional mafia groups (Paoli, 2020), as well as the growing presence of illicit goods and services that are produced and distributed through looser and more flexible configurations (Boerman et al., 2017; Bruinsma & Bernasco, 2004; Europol, 2021, 2025, 2026; Morselli, 2009). From this broader perspective, a 'criminal network' can be understood as a loose network of criminal associates engaging in criminal activities (GI-TOC, 2025a).

However, there is currently **no universal consensus** on an 'official' definition of a criminal network. The purpose of this report is not to provide a definitive definition, but rather to outline the concept in a way that is useful for the scope of the study. In accordance with Work Package 2 of the PREVENT project, it is acknowledged that criminal networks generally vary in structure and durability, existing along a continuum. While some networks are highly organised and long-standing, others may be fluid and loosely connected (Greenfield et al., 2019). Furthermore, it is often challenging to determine the boundaries and membership of criminal networks, particularly when it comes to individuals operating on the periphery of the network, such as low-level recruits, strawmen, or crime-as-a-service providers (Europol, 2025).

Moreover, this study adopts a pragmatic, case-based approach to define '**membership of a criminal network**'. Due to the fluid nature of networks and changing affiliations over time, an individual was considered a 'member' if information provided by LEAs or other relevant authorities indicated a certain degree of consistency regarding his or her involvement in the network. This could be inferred from multiple contacts, repeated interactions, or a recurring role in the activities under investigation. This study thus acknowledges the fluid nature of criminal networks, while also addressing the need for an empirical threshold to determine membership in a network.

2.2 Criminal use of legitimate businesses

In this report, '**criminal use of legitimate businesses**' is understood as an overarching concept encompassing the different ways in which criminal networks may exploit legitimate businesses, business structures, or business services to facilitate, conceal, or support criminal activities, or to derive financial benefit from them. As recent analyses by Europol (2024b, 2025, 2026) show, legitimate businesses can be used in various ways and to varying degrees: they may serve to support criminal operations, disguise illicit activities, or launder criminal proceeds. In this sense, 'criminal use of legitimate businesses' is not a stand-alone offence, but rather a broader process encompassing a range of criminal practices or 'sentinel crimes', such as corruption, money laundering, and document forgery (cf. *infra*) (Savona & Riccardi, 2018). Furthermore, there may be varying levels of criminal involvement and control, as well as differing durations, ranging from temporary and opportunistic use to systematic and long-term exploitation (Europol, 2024b, 2025, 2026).

Although various classifications exist within the literature, the PREVENT project distinguishes between **three categories** of 'criminal use of legitimate businesses' for analytical purposes. This typology provides an analytical framework for capturing the various ways in which criminal networks exploit legitimate businesses, whether through ownership, infiltration, or the use of *bona fide* services.

2.2.1 Criminal ownership and control of legitimate businesses

This first category concerns cases in which criminal networks deliberately establish legitimate businesses or take over already existing ones and succeed in exercising effective control over them. Such businesses may function as front companies, shell companies, laundering vehicles, logistical tools, or operational platforms to carry out criminal practices. For instance, companies may be set up or taken over to conceal illicit activities or to facilitate the laundering of criminal proceedings (Rijksoverheid, 2024; Savona & Berlusconi, 2015). According to Europol (2024b, 2025), the **criminal ownership** of a legal business reflects a high degree of the criminal use of the legitimate economy.

2.2.2 Criminal infiltration into legitimate businesses

A second category of 'criminal use of the legitimate economy' concerns **criminal infiltration**. As part of the PREVENT project, a slightly modified version of the definition developed in the Transcrime ARIEL project (Savona & Berlusconi, 2015) is used:

> *Any case in which a natural person belonging to a criminal network or acting on its behalf, or an already infiltrated legal person, invests financial and/or human resources to participate in the decision-making process of a legitimate business.*

This definition comprises **four central elements**, which have been copied (almost exactly) from the definition used in the ARIEL project:

1. A **criminal network**[4] (cf. *supra*);

2. A **natural person** belonging to a criminal network or acting on its behalf, or an already infiltrated legal person:

   The infiltration is carried out by a member of the criminal network or a person who is used as a cover by the criminal network and acts as a strawman (e.g., relative, lawyer, notary). A legal person (e.g., cooperative, cooperation, company) ultimately controlled by a criminal network through a member of the network or a strawman may also conduct the infiltration process. (Savona & Berlusconi, 2015, p. 19)

3. The **investment of financial and/or human resources**:

   The investment of money is not an essential requirement for the criminal infiltration of a legitimate business. Human resources may also be adopted to acquire control over the management (e.g., a network member becomes director of a legal company). (Savona & Berlusconi, 2015, p. 19)

[4] In the Transcrime ARIEL project, the original definition refers to a 'criminal organisation' rather than a 'criminal network' (Savona & Berlusconi, 2015, p. 19).

4. The **participation in the decision-making process** of a legitimate business:

   The criminal network, through a member, a strawman, or an infiltrated legal business, influences the decision-making processes of a legitimate operating business, i.e. it is able to influence decisions about business strategies and future investments, as well as hiring, promotions and salary increases, subcontracting and supply contracts, security and controls. (Savona & Berlusconi, 2015, p. 19)

2.2.3 Criminal use or abuse of bona fide businesses and services

A third category concerns the **criminal use or abuse of *bona fide* businesses and services**. In these cases, legitimate companies are being (ab)used, with or without their knowledge, to provide legal services, infrastructure, or other resources that facilitate criminal activities (Europol, 2024b, 2025; Rijksoverheid, 2024). The company's name, products, services, logistical capacity, and other assets may be used for criminal purposes, even though the company is not fully controlled by the criminal network. However, the company itself does not benefit (financially) from the crimes committed.

2.3 Economic (sub)sector

The PREVENT project focuses on economic (sub)sectors, in accordance with the priorities set out in the *EU Roadmap to Fight Drug Trafficking and Organised Crime* (European Commission, 2023a), as well as in Europol's (2024a) recent report on the EU's most threatening criminal networks. Within the PREVENT project, the Eurostat (2023) definition of 'economic activity' is used. For semantic reasons, however, it is renamed '**economic subsector**'. It involves practices through which "resources such as capital goods, labour, manufacturing techniques or intermediate products are combined to produce specific goods or services".

CRIMINAL USE OF THE LEGAL ECONOMY: AN OVERVIEW

3.1 Tensions between legitimate and criminal entrepreneurship

As outlined in the Introduction (Section 1.2), the principles of 'free enterprise' and **'free entrepreneurship'** are increasingly promoted in modern societies. However, these principles inadvertently create opportunities for criminal entrepreneurship, as the strategies of criminal networks have evolved significantly in recent decades (CTIF-CFI, 2022; LIEC, 2019; Wittevrongel & De Jaeger, 2024). In Sweden, for example, recent reports show that twenty to thirty percent of individuals known to the police as having ties to organised crime are also registered as being involved in a (legitimate) business (Brå, 2025; Rostami & Mondani, 2024). Sweden's relatively open business environment, characterised by minimal barriers to entry (including the freedom to own, establish, and acquire businesses) and inadequate control systems, increases the country's attractiveness to criminal networks (NOA, 2024a).

Similarly, the Belgian Federal Government intends to promote the principle of 'free enterprise'. However, due to limited control mechanisms on entrepreneurship, deregulation measures, and the simplification of regulations, criminal entrepreneurs are able to continue expanding their criminal activities (Wittevrongel & De Jaeger, 2024). In Bulgaria, political and economic transitions (from a centrally planned socialist economy towards a market-oriented system) have created vulnerabilities that have allowed criminal networks to consolidate their power in various economic sectors (Bezlov et al., 2007).

3.2 Motivators and drivers of criminal networks' use of the legitimate economy

Criminal networks can use the legal economy for a variety of purposes, driven by different motives. The ARIEL and MORE projects have already investigated potential drivers in detail, demonstrating that criminal networks typically do not pursue solely financial objectives (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). Furthermore, different objectives can be pursued within the same network. Although such motivations seem to be universal, they can still vary by country or geographic region. For example, the ARIEL project indicates that Italian mafia groups primarily seek to maximise social consensus and establish (physical) control over certain areas, whereas networks in the Netherlands and Sweden are mainly driven by the intention to commit fraud (Savona & Berlusconi, 2015).

Several of these motives are discussed in more detail below. However, this report does not seek to provide a comprehensive or fully exhaustive overview of all relevant aspects.

Making a profit

First, criminal networks are profit-driven organisations that seek to capitalise on opportunities for profit as soon as they arise, whether in legal or illegal markets. This (financial) motive is particularly linked to money laundering (cf. *infra*), with an emphasis on the lucrative nature of businesses (Savona & Berlusconi, 2015; Savona & Riccardi, 2018; te Pest et al., 2012).

Money laundering

Second, legitimate businesses often serve as an ideal conduit for criminal networks to launder illicit proceeds: they provide a front behind which the criminal identity of the network or the illicit origin of the money can be concealed, and ensure that the inflow and outflow of illicit funds remain hidden (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). To this end, various money laundering techniques can be used, including cash-based transactions, trade-based money laundering (TBML) techniques, and false invoices (cf. *infra*) (Savona & Riccardi, 2018). In addition, criminal networks may also use infiltrated companies to offer money laundering services to other criminals or entrepreneurs (i.e., crime-as-a-service). Although money laundering is generally closely linked to the criminal use of legitimate businesses, certain economic (sub)sectors appear to be more susceptible to this (e.g., construction sector, hospitality sector, wholesale sector) (Savona & Berlusconi, 2015).

Concealing illicit activities

Third, legitimate businesses are used as fronts to conceal illicit activities, such as trafficking in human beings and illegal goods (e.g., drug trafficking) (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). Certain sectors are more frequently used to conceal such activities, such as the hospitality and transportation sector.

Committing fraud

Fourth, criminal networks often use legitimate businesses to commit various types of fraud, such as social fraud, tax fraud, and welfare fraud (cf. *infra*) (Savona & Riccardi, 2018). In addition, many companies that are used for criminal purposes engage in fraudulent practices, regardless of the ultimate objective (or original motive) of the infiltration.

Obtaining information

Fifth, some criminal networks seek to make use of certain businesses to gain specific knowledge (Savona & Berlusconi, 2015). For example, small accounting firms can be infiltrated to obtain relevant information about accounting and tax practice, and to (mis)use the information gathered in the future as a basis for new criminal plans.

Controlling the territory

Sixth, some criminal networks seek to maintain strict control over certain geographic areas and to establish their status within those areas. The criminal use of legitimate businesses can thus also serve this power-oriented objective, often involving economic (sub)sectors with a specific geographic focus (e.g., the construction and hospitality sector) (Savona & Riccardi, 2018).

Influencing politics and public administration

Seventh, linked to the previous motive, criminal networks often seek to exert influence on politics and public administration in order to maintain and strengthen their physical and strategic control (and power) over the territorial area (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). This is consistent with the general trend that criminal networks are increasingly resorting to 'submersion' to maximise their power, as – according to the ARIEL project – is particularly evident in Italy.

Increasing social consensus

Eighth, by aligning themselves with legitimate businesses, criminal networks can gain the support of the local population and thereby increase their social acceptance within the broader community (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). This is achieved primarily through infiltration into certain strategic sectors, such as education or healthcare, by providing goods and services to the population.

Cleaning up criminal reputations

Nineth, appearing to be legitimate entrepreneurs can help criminal networks to clean up their criminal reputation and create the appearance of legitimacy (Savona & Riccardi, 2018).

3.3 Modus operandi: methods of criminal use of the legitimate economy

The criminal use of the legitimate economy can take many forms, involving a variety of techniques. The examples below provide a non-exhaustive overview.

Sham companies

Sham companies (also known as ghost companies) are companies that are (physically) inaccessible or are registered at a fictitious location or address (Janssens et al., 2023). On paper, they operate as legitimate entities, but in practice they are traditionally used as a front to conceal illegal activities, particularly fraud and (trade-based) money laundering. To that end, criminal networks often employ strawmen and figureheads (cf. *infra*). In fact, these companies engage in little or no economic or commercial activity and are often deliberately set up to go bankrupt.

Strawmen and figureheads

In the context of sham companies, strawmen and figureheads are often employed. To the outside world, it appears as though these individuals are acting on their own behalf, but in reality they serve as a front for criminals by concealing the identities of the company's ultimate beneficiaries (i.e., the members of the criminal network) and their activities (Janssens et al., 2023; Savona & Berlusconi, 2015; Savona & Riccardi, 2018; Soudijn & Akse, 2012). Strawmen are primarily involved in cases where members of the network do have criminal records, which prevents them from directly participating in the ownership and management structure of the infiltrated company (Sørensen, 2021). Strawmen can be deployed in four ways: as formal owners of the infiltrated companies, as directors, as employees, or as holders of bank accounts that are used in the criminal business scheme (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). Furthermore, strawmen often share certain characteristics, such as being very young or very old, or having a low level of education.

In addition, different types of natural persons are often appointed as figureheads, which can be classified into five categories (Savona & Riccardi, 2018). Firstly, *figureheads on demand* may be homeless people or poor individuals who are willing to lend their identity for just a few euros. Second, the category of *colluding businessmen* consists of legitimate entrepreneurs who establish or manage companies on behalf of the criminal network in exchange for financial gain. Third, *unwitting figureheads* are people whose identities have been stolen and who, without knowing it, become owners, directors, or employees of a company on behalf of a criminal network. In this context, identity theft and document forgery play a crucial role. Fourth, *professionals* such as lawyers, notaries, and

accountants can provide money laundering services to criminal networks. Finally, *family members* – particularly women – can be mobilised to maintain or maximise control over the business.

Fictitious locations

In close connection with the methods mentioned above, criminal networks can set up companies at fictitious locations, such as P.O. box addresses (Janssens et al., 2023). Since there is generally no formal verification of this, any address can be used as the registered office, even addresses that do not exist or belong to someone else.

Cash payments and money laundering

Cash payments facilitate the laundering of illicit funds through legitimate business structures, because cash is anonymous and usually untraceable (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). Therefore, criminal networks often prefer to make use of businesses operating in cash-intensive sectors (such as the hospitality industry), as this makes it easier to report illicit proceeds as legitimate income, deposit them into the companies' bank accounts, and subsequently launder them. However, to prevent money laundering (and other illegal activities), various regulations have been introduced at European and national levels aimed at reducing the share of cash payments (e.g., by encouraging electronic payments).

The money laundering process traditionally consists of three steps (Van der Veen & Heuts, 2017). First, *placement* refers to the process of channelling money from the criminal circuit into the legitimate financial system. Once the origin of the money has been hidden in the *concealment* stage, it is used for legitimate investments or purchases during the *integration* phase. In practice, however, money laundering is much more sophisticated: criminal networks employ a wide range of methods to launder their illicit proceeds (Europol, 2025, 2026). Europol (2023b) distinguishes between various types and methods of money laundering, which are briefly discussed below.

- **Cash smuggling**
  This refers to cases in which illicit proceeds are physically transported around the globe, with cash being sent in parcels or packages, or transferred by cash couriers (Europol, 2023b).

- **Informal Value Transfer Systems (IVTS)**
  Europol (2023b, p. 13) describes an Informal Value Transfer System (IVTS) as "any system, mechanism, or network of people that receives money to make the funds or an equivalent value payable to a third party in another geographic location, operating outside the regulatory oversight of the legitimate banking sector." This phenomenon is also known as 'underground banking'. Due to the implementation of stricter anti-money laundering (AML) regulations in mainstream financial institutions, IVTSs have become increasingly attractive to criminals and criminal networks.

- **Mule networks**
  These networks consist of money mules; individuals who, often unknowingly, have been recruited to act as intermediaries in money laundering operations for criminals (Europol, 2023b; Janssens et al., 2023; te Pest et al., 2012). Acting on behalf of others, they transfer illicit funds between accounts, frequently across jurisdictions, through both personal and corporate banking accounts.

- **Trade-Based Money Laundering (TBML)**
  TBML is the process by which the proceeds of crime are concealed, and assets are transferred through commercial transactions in an attempt to legitimise their illicit origin (Europol, 2023b; FATF, 2006). In this context, criminal networks exploit trade and currency systems by using false invoices and offering certain goods (such as vehicles, metals, and luxury items) at inflated prices in order to launder the proceeds.

- **Digital assets**
  Virtual currencies are increasingly being used in money laundering practices, in which decentralised exchanges, cryptocurrency mixers, and privacy coins are employed to disguise the origin of illicit funds (Europol, 2023b, 2025).

Complex corporate ownership structures

As is the case with the use of strawmen and figureheads, criminals and criminal networks may also hide behind complex corporate structures, which are characterised, for example, by frequent changes in company ownership, name, or legal form (Janssens et al., 2023; Savona & Berlusconi, 2015). These complex structures result in a limited degree of transparency regarding the corporate structure, making it more difficult for LEAs to conduct financial investigations and identify the beneficial owners of infiltrated companies (Savona & Riccardi, 2018).

This *modus operandi* can be linked to the criminal use of 'tax havens' or 'secrecy jurisdictions', as criminal networks are often drawn to jurisdictions with low levels of financial and corporate transparency (Savona & Riccardi, 2018). However, a trend among European criminal networks is that they are increasingly favouring nearby 'onshore' jurisdictions over notorious 'offshore' tax havens.

Facilitators

Facilitators are individuals who possess scarce knowledge, skills, or resources required to commit certain crimes, making them indispensable to criminal networks in the commission of criminal offences (Kleemans et al., 2002; Soudijn & Akse, 2012). Professions such as notaries, lawyers, accountants, and real estate agents are at particularly high risk of being employed as facilitators (Janssens et al., 2023). In the context of waste management crime, for example, criminals seek to maintain contact with accountants, lawyers, environmental consultants, and waste brokers, as committing such crimes requires knowledge of environmental legislation (NOA, 2023).

Violence and corruption

Although corruption and violence can in themselves be regarded as criminal phenomena, they are generally also seen as tools to conceal and facilitate criminal activities (Janssens et al., 2023). Both are used to evade authorities, including by remaining silent and coercing people to cooperate within the criminal process. As such, criminal networks sometimes resort to violence to ensure their infiltration of legitimate businesses and the compliance of corrupted actors (Europol, 2025). For example, the strategy of Italian mafia groups (the '*metodo mafioso*') is characterised by collusion, corruption, intimidation, and extortion (Savona, 2010; Savona & Riccardi, 2018).

3.4 Opportunities and vulnerabilities within the legitimate economy

Criminal networks often exploit certain opportunities to make use of the legitimate economy, whether in terms of geographic area, economic (sub)sector, or specific businesses. The ARIEL and MORE projects have examined in detail potential 'vulnerabilities' that facilitate the criminal use of legitimate businesses, with a focus on various countries (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). These characteristics may explain why certain (sub)sectors or companies are infiltrated to a greater extent than others.

3.4.1 Geographical vulnerabilities

The empirical findings of the ARIEL project have shown that certain **geographic areas** are more vulnerable to the criminal use of the legitimate economy than others (Savona & Berlusconi, 2015). First, this is the case in areas characterised by a long-standing, deep-rooted presence of criminal groups (and thus of organised crime), as these groups often exercise control over political and economic spheres (for example, mafia organisations in Southern Italy). Since these networks are likely to operate in both legal and illegal markets and often invest in the areas where they are present and active, widespread corruption and a substantial shadow economy are typically also present within these regions. Furthermore, the criminal use of the legitimate economy is more common in urban areas and in regions bordering other countries, as well as in areas with major seaports, airports, and other transportation facilities, as is the case in the Netherlands, for example (Savona & Berlusconi, 2015).

3.4.2 Sectoral vulnerabilities

Economic (sub)sectors may be considered 'vulnerable' to the criminal use of the legitimate economy when the structural characteristics of companies within those sectors entail an increased risk that they may, consciously or unconsciously, facilitate criminal activities, participate in them, or serve as a front (Rijksoverheid, 2024). In this context, various types of '**opportunity structures**' can be identified across sectors, each of which includes its own set of indicators (LIEC, 2019). Some of these factors are explained in more detail below, as they were also identified as risk factors by the ARIEL project (Savona & Berlusconi, 2015).

Social opportunity structures

- High degree of anonymity
- Lack of social control
- Closed nature of the sector (e.g., limited openness towards the outside world)
- Lack of resilience

Financial-economic opportunity structures

- Cash intensity
- Poor socio-economic conditions of employees
- Profits made through fraudulent practices
- Unfair competition and low profit margins

Infrastructure and logistical opportunity structures

- Availability of resources for drug production
- Characteristics of a country's infrastructure (e.g., transportation facilities)

Institutional opportunity structures

- Insufficient regulation, control, and enforcement
- Low barriers to entry
- High degree of autonomy of parties involved
- Access to (confidential) information

Cash intensity

Sectors characterised by a high volume of cash transactions (such as the hospitality industry) are more susceptible to criminal infiltration, as cash is often used to launder illicit proceeds and conceal their illegal origin (cf. *supra*) (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). As briefly mentioned above, cash-intensive sectors are often associated with widespread corruption and a substantial shadow economy, as well as high levels of tax evasion and money laundering.

Limited competition and openness regarding foreign investments

Criminal networks may favour areas and sectors with a 'protected' economy, characterised by limited competition, inelastic demand, and limited openness to international investment (Savona & Berlusconi, 2015).

Traditional nature of activities

Criminal networks tend to target areas and sectors with a high concentration of 'traditional' economic activities, including low levels of technology and little research and development (Savona & Berlusconi, 2015). Furthermore, sectors with low incomes and underdeveloped infrastructure may be vulnerable to criminal infiltration, whereas this is less likely to be the case in affluent areas and sectors.

Limited regulations and inadequate control systems

Sectors with weak or frequently changing regulations and inadequate control mechanisms can facilitate the use of legitimate businesses and the concealment of criminal activities, due to a lack of transparency and the complexity of business structures (Savona & Berlusconi, 2015; Savona & Riccardi, 2018). This is the case, for example, within the construction industry.

Low barriers to entry

The fact that the licences and permits required to carry out certain legal activities are relatively easy to obtain may also facilitate the criminal use of the legitimate economy (Savona & Berlusconi, 2015). This is particularly relevant in light of the opportunities that have emerged in recent years regarding business start-ups, which demonstrate a desire to promote and strengthen the principle of 'freedom of economic activity' (for example, by lowering barriers to entry), with the potential undesirable effect of facilitating criminal activities (cf. *supra*) (CTIF-CFI, 2022).

3.4.3 Business-level vulnerabilities

Certain vulnerabilities also exist at the level of individual businesses, making some companies more susceptible to criminal infiltration than others (Savona & Berlusconi, 2015). On the one hand, the **size of a company** plays a role: criminal networks prefer to infiltrate small and medium-sized businesses, as they seek to minimise their visibility and the risk of (law enforcement) controls. For this reason, criminal networks often decide to set up new companies rather than infiltrating existing ones.

On the other hand, a company's **legal form** appears to play a role in criminal networks' decision to infiltrate that specific business (Savona & Berlusconi, 2015). Before delving into the types of businesses that are most vulnerable to being used for criminal purposes, these various structures of legitimate businesses will be briefly explained in accordance with the categorisation used by Europol (2024b). These legal forms exist under different names in different EU Member States, sometimes with slightly different regulations.

- **Limited liability companies**
  This is the most common legal form for small and medium-sized enterprises (Europol, 2024b). The shareholders are not personally liable for the company's debts, as they function as separate legal entities distinct from the company. Limited liability companies can be either private limited companies or public limited companies; the latter are generally publicly traded and required to have a minimum share capital.

- **Unlimited liability companies**
  Although this category of companies is similar to private limited companies (cf. *supra*), the liability of the owners of unlimited liability companies is not limited to the value of their shareholdings, which means that they are personally liable for the company's debts and obligations (Europol, 2024b).

- **Sole traders**
  Sole traders are companies owned and operated by a single person, who is personally liable for the business's debts and obligations (Europol, 2024b).

- **Partnerships**
  Partnerships are arrangements between two or more individuals to organise business operations and share profits and liabilities (Europol, 2024b). In 'limited partnerships', at least one partner has unlimited liability for the company's debts, whereas all partners have unlimited liability in 'general partnerships'.

- **Trusts**
  A trust is a legal entity in which one party, known as the 'trustor', grants another party, the 'trustee', the right to hold and manage real property or assets for the benefit of a third party (i.e., the 'beneficiary') (Europol, 2024b).

- **Associations**
  The legal form of an association is typically used by non-profit organisations, charities, and foundations (Europol, 2024b).

- **State-owned enterprises**

Overall, the ARIEL project concluded that criminal networks generally base their choice of legal structure on two distinct factors (Savona & Berlusconi, 2015). Either they choose a business structure that aligns with the characteristics of the legal economy in a particular country, by adopting the most common legal form in that country and in that economic (sub)sector. Or they choose the legal structure with the most attractive features, which isn't necessarily the most common one.

At the same time, criminal networks may prefer certain legal business structures over others, depending on their specific motives for using the legitimate economy (cf. *supra*) (Savona & Berlusconi, 2015). For example, they may choose to use **limited liability companies** to better conceal their identities and criminal activities. Since this legal structure allows for greater fragmentation of the share capital, it is more difficult for LEAs to identify the ultimate beneficial owners of the companies in question, and the potential impact of confiscation and seizure is reduced. In addition, such businesses are cheaper and easier to set up, as there are few requirements regarding the necessary start-up capital

(Savona & Riccardi, 2018). On the other hand, when criminal networks wish to establish direct control over their assets – for example, for traditional or cultural reasons, or to enhance their reputation or social prestige – they may prefer **limited liability companies** or **sole traders** (Savona & Berlusconi, 2015).

In **Sweden**, for example, limited liability companies (in Swedish: *Aktiebolag*) appear to be used systematically as a means of committing crimes, concealing criminal activities, and laundering illicit proceeds (Ekobrottsmyndigheten, 2020). These companies must be registered with both the Swedish Companies Registration Office and the Swedish Tax Agency and must have a minimum capital of SEK 25,000 (approximately EUR 2,250). However, criminals often prefer to buy companies through business brokers rather than start their own. These are mainly so-called 'limited liability companies with history' (in Swedish: *Historikbolag*), shelf companies with an established financial history. Unlike a newly registered company, a *Historikbolag* has a track of business activities, tax records, and financial statements, which makes it more credible. Furthermore, these companies can often be purchased very quickly, in less than two hours, while registering a new company takes two weeks or longer. It is reported that more than eighty percent of all these 'impulse acquisitions' are made by people with criminal connections.

In **Belgium**, general and limited partnerships are particularly attractive to criminal entrepreneurs, especially for money laundering schemes, due to their low administrative and financial requirements (CTIF-CFI, 2021b). No start-up capital is required for these legal structures, and they can be established through a private agreement without the need for notarial supervision. One drawback is that creditors can claim the partners' entire personal assets if the partnership defaults, but criminals can easily circumvent this by using strawmen. In addition, criminal networks are increasingly using private limited companies, as the requirements regarding the required start-up capital have recently been relaxed (Wittevrongel & De Jaeger, 2024).[5] Instead, entrepreneurs are now required to submit a financial plan to a notary, but it is not yet clear whether this will provide sufficient oversight to prevent abuse.

3.5 Financial profile of criminal networks

Criminal networks that make use of the legal economy are often characterised by a distinct financial profile comprising several key features. Accordingly, these aspects were also taken into account during data collecting for the local case studies.

Financing sources and start-up capital

The financing of criminal networks may originate from both legal and illegal sources (Levi et al., 2015). While illegal funds originate from past criminal activities, legal funds are obtained through legitimate means. In this context, it is becoming increasingly common for legitimate entrepreneurs to invest proceeds from their legal businesses in illegal activities, in exchange for a share of the resulting profits (Snaphaan & van Ruitenburg, 2024). Legitimate investment ventures are also used to attract additional funding, when deemed necessary. This occurs when criminal networks form partnerships with other criminals or legitimate businessmen, allowing them to share the financial risks and costs of carrying out illegal activities (Levi et al., 2015; Snaphaan & van Ruitenburg, 2024).

[5] Since 1 May 2019, the minimum share capital requirement of EUR 18,550 for a private limited company has been abolished.

Payment methods

A distinction can be made between cash and non-cash payments, with non-cash payments encompassing a range of methods, such as legitimate bank transactions, money transfers, and underground banking (Snaphaan & van Ruitenburg, 2024). Both in the case of underground banking (IVTS; cf. *supra*) and money transfers, there is a limited amount of physical movement of cash. In money transfers, for example, cash is deposited at money transfer offices and then transferred virtually to be withdrawn as cash at another location around the world. In addition to these fiduciary payments, there are also virtual currencies (such as cryptocurrencies) that can be used to make payments. Two additional payment methods that can be used are trade-based money laundering (cf. *supra*) and barter or payment in kind (Levi et al., 2015).

Settlement of payments

Within the context of payments arising from agreements between (associated) partners in criminal networks, a distinction can be made between payments at the organisational level and those at the operational level (Snaphaan & van Ruitenburg, 2024). At the organisational level, three main payment methods can be distinguished: prepayment, revolving credit, and phased payment. The latter appears to be particularly favoured by large (drug trafficking) networks (Levi et al., 2015). For example, in legitimate businesses used to conceal cocaine distribution points, drug couriers receive part of their payment in advance, while the remainder is paid after the drugs have been delivered to their destination. Operational-level payments, on the other hand, relate to personnel costs (Snaphaan & van Ruitenburg, 2024).

Costs of business operations

The operational costs of criminal networks vary depending on the type of criminal activities carried out, and each criminal process entails different costs, depending on the *modus operandi* used (Raets & Janssens, 2019). Costs may arise from the purchase of illegal goods and services, personnel, and materials (Snaphaan & van Ruitenburg, 2024). Examples of costs include corrupt payments (i.e., bribes), payments to facilitators and intermediaries, payments for forged documents, transportation costs for victims of human trafficking, utility costs for drug production, and labour costs for exploited workers (Levi et al., 2015; Raets & Janssens, 2019; Shentov et al., 2018). Criminal networks often try to minimize these costs as much as possible, for example by using cheap materials (Savona & Berlusconi, 2015).

Revenues and proceeds

The proceeds generated by a criminal network depend on numerous factors, such as the type of profit-driven crimes committed, the *modus operandi* used, the size of the network, and the market value of the products traded (Savona & Berlusconi, 2015; Snaphaan & van Ruitenburg, 2024). At the individual level, revenues also vary depending on the member's position within the network. The proceeds can be reinvested in the network's business operations to sustain its criminal activities (Raets & Janssens, 2019). In addition, they are often laundered, for example through investments in the real estate sector.

3.6 Criminal activities enabled by the criminal use of the legitimate economy

Criminal networks make use of the legal economy to commit or facilitate numerous criminal activities. A selection of these activities is briefly outlined below. However, this overview is not exhaustive.

Money laundering

As previously mentioned, money laundering is one of the most common phenomena associated with the criminal use of the legitimate economy. Criminal networks are increasingly outsourcing the laundering of their illegal proceeds to professional money launderers, a practice also known as 'money laundering as a service' (CTIF-CFI, 2022).

Drug crime

Drug trafficking is closely linked to the criminal use of legitimate businesses for transportation purposes, for the concealment of drugs within legitimate cargoes, and for the obtainment of the necessary precursors or chemicals (Europol, 2025). In various sectors, legitimate businesses are being used to facilitate drug-related crimes, such as the agricultural sector (Boelens & Groothuis, 2020) and the real estate sector (Kruize & Gruter, 2020). Other sectors susceptible to such incidents include courier services, the logistics sector, the automotive sector, the wholesale sector, and the hospitality sector, which is often used as a meeting place for criminals (Janssens et al., 2023).

Human trafficking – Sexual exploitation

Although corporate structures are more commonly used in cases of labour trafficking than in activities related to sexual exploitation, the latter is more prevalent in certain legal subsectors. These include prostitution bars, strip clubs, massage parlours, champagne bars, (rendezvous) hotels, homes, and brothels that masquerade as legitimate businesses such as saunas or beauty salons (Janssens et al., 2023).

Human trafficking – Labour exploitation

In the context of human trafficking, concealing criminal activities within a legitimate business through opaque and non-transparent corporate structures and fictitious or shell companies is a common practice (Raets & Janssens, 2019). Criminals make use of various economic (sub)sectors for the purpose of labour exploitation: agriculture and horticulture, the construction sector, the hospitality industry, domestic work, and the real estate sector. More specifically, certain types of businesses are particularly susceptible, including bakeries, nail salons, hairdressers, retail outlets, second-hand clothing stores, waste sorting facilities, car washes, and driving schools.

In Sweden, the term 'labour market crime' has been introduced, referring to illegal activities in the labour market that violate laws and regulations regarding working conditions, taxation, and social security (Jeppson, 2024; SOU, 2025). This phenomenon includes crimes such as undeclared work, tax and payroll fraud, illegal employment, violations of workplace safety regulations, and trafficking in human beings. The term is often associated with organised crime and criminal networks, as well as with the criminal use of the legal economy in the context of labour exploitation, social security fraud, and fiscal fraud.

Trafficking in stolen goods – Fencing

Although arms trade is less frequently linked to the criminal use of the legal economy (Janssens et al., 2023), criminal networks often use legitimate businesses to handle, possess, and transfer assets derived from and obtained through criminal activities (Kruize & Gruter, 2020). Examples in Belgium show that this is the case in the real estate sector, night shops (Janssens et al., 2023), the automotive sector (with trafficking in luxury cars) (Het Nieuwsblad, 2019), and the horse sector (where, according to the Belgian Federal Police, the trade in stolen horse saddles is a recent trend) (Federale Politie, 2024; Houwen, 2023). In the Netherlands, criminal networks make use of the legal economy to trade in metals, particularly copper and gold (PVO Oost-Nederland, 2022).

Counterfeiting

The use of the legal economy also facilitates the sale of (and trade in) counterfeit products (Janssens et al., 2023).

Fraud

The criminal use of the legal economy is often associated with fraudulent practices. A few types of fraud are briefly discussed below.

- **Social fraud**

  Examples of social fraud include the use of bogus self-employed workers, undeclared work, non-compliance with wage and working conditions, and excessive subcontracting that hinders inspections (Janssens et al., 2023). Social fraud can be committed by exploiting various economic (sub)sectors, including the hospitality industry, the industrial and cleaning sectors, carwashes, garden maintenance services, security services, and transportation services (Janssens et al., 2023).

  In addition, some criminal networks use the principle of 'compensation' to launder illicit proceeds. Money from criminal activities is invested directly into undeclared work, such as in construction or cleaning services, to minimise the risk of detection when the money enters the banking system (CTIF-CFI, 2022). The use of illegal labour for money laundering constitutes social fraud, and since these companies rarely fulfil their tax obligations, this can also be classified as serious tax fraud.

- **Value Added Tax (VAT) fraud and Missing Trader Intra-Community (MTIC) fraud**

  VAT fraud and MTIC fraud pose an ongoing threat within the legal economy, involving the systematic criminal use of legitimate businesses (Europol, 2025). MTIC fraud is the most common type of VAT fraud. It involves schemes in which a trader imports goods VAT-free from another EU country and sells them on the domestic market, charging the buyer VAT but failing to remit this tax to the authorities. The trader then disappears, hence the term 'missing trader'. The most common form of MTIC fraud is carousel fraud, which involves a circular trading scheme in which the same goods are repeatedly imported and exported through different Member States, with VAT refunds claimed for taxes that were never paid.

In line with the EU Commission Regulation No 1925/2004, a '**shell company**' is defined as a trader registered for VAT that, potentially with fraudulent intent, acquires or appears to acquire goods or services without paying the VAT due. Common characteristics include large and sudden VAT-free intra-EU acquisitions, the recent replacement of the board by indebted individuals with experience in multiple bankrupt companies, and the absence of a genuine business address or employees. Other indicators include missing or outdated accounting records and annual reports, illogical timing between payments, invoices and the movement of goods, and a failure to pay VAT and other taxes. Furthermore, shell companies typically fail to meet their accounting obligations or declare EUR 0.

- **Customs import fraud**
  In the context of customs fraud involving imports, document fraud and the criminal use of legitimate businesses are common elements, regardless of the specific *modus operandi*. Criminals primarily make use of limited liability companies, sole traders, and shell companies, which they set up and dissolve quickly (Europol, 2025).

- **Welfare fraud**
  Within the legal economy, welfare fraud can occur as well. In Belgium, for example, affected businesses were able to apply for financial aid during the COVID-19 pandemic without undergoing strict pre-approval controls (Lefevere, 2020; Wittevrongel & De Jaeger, 2024). As a result, the aid program was exploited by criminal networks: it is estimated that 10 to 15 percent of the aid disbursed (approximately EUR 13 billion) ended up in the criminal sector, thereby financing activities such as human trafficking and drug trafficking. In Sweden, criminal groups have been detected operating health centres and other welfare companies to profit from municipal and regional subsidies, enabling them to commit welfare fraud on a large scale (NOA, 2024a).

Trade-based sanctions evasion

The evasion of trade-based sanctions relies heavily on a 'crime-as-a-service' model, combined with the criminal use of legitimate businesses for supply chain management (Europol, 2025). The sanctioned entities retain beneficial ownership of corporate structures and exert influence in various economic sectors and Member States. Legitimate companies are infiltrated, and front companies are set up in the retail, import-export, transportation, or financial sectors to purchase and ship goods or assets. This kind of infiltration of legitimate businesses shows how deeply the evasion of sanctions is embedded in established trade structures. Moreover, this integration not only facilitates sanctions evasion, but also incentivises corruption and undermines the integrity of national economies (Europol, 2025).

Environmental crime

Environmental crime is an attractive area of activity for organised crime because the risk of detection is low and the profits for criminal actors are high (Europol, 2025). The legitimate waste sector, in particular, is becoming increasingly vulnerable to criminal infiltration. However, detecting and investigating environmental crimes is complicated, especially when a company engages in both legal and illegal activities (NOA, 2023).

METHODOLOGY

4.1 Selection of case studies

Using a bottom-up approach, Work Package 3 of the PREVENT project examines how criminal networks make use of economic (sub)sectors and legitimate businesses in European cities, and what harm this causes. Since criminal activities often become intertwined with the local economic context, a local-level approach was chosen as a starting point. Accordingly, this report presents the findings of research conducted in nine urban areas across eight EU Member States. The cities to be investigated were identified in PREVENT's initial project proposal, based on the availability of expertise and the composition of the consortium. The city (or cities) that would ultimately be studied could still be revised at the start of the project if, during the initial data collection phase, researchers identified another city of interest for this research. The **nine cities** selected as case studies are the following:

- Antwerp (A) – Belgium;
- Brussels (B) – Belgium;
- Caserta (C) – Italy;
- Frankfurt (F) – Germany;
- Madrid (M) – Spain;
- Paris (P) – France;
- Sofia (SO) – Bulgaria;
- Stockholm (ST) – Sweden;
- Utrecht (U) – The Netherlands.

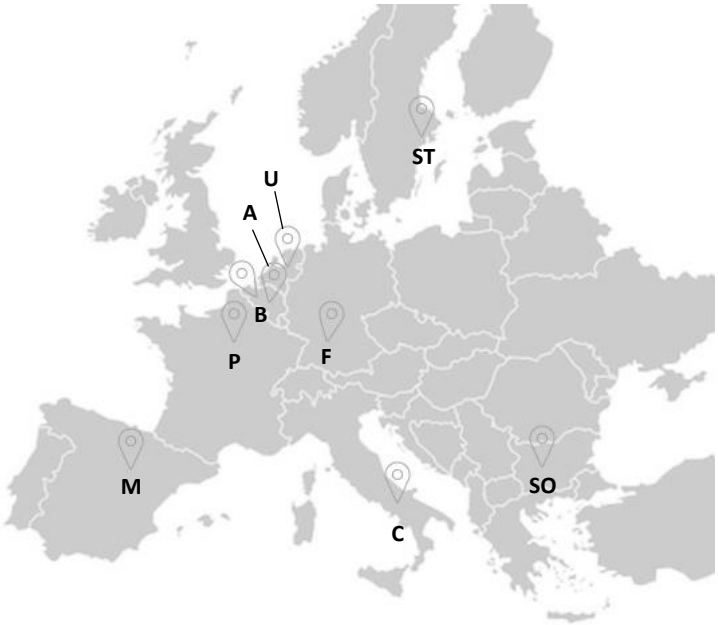


Figure 1
Geographical distribution of the nine cities included in the study

Subsequently, in each selected city, local experts and stakeholders helped identify **five economic (sub)sectors** that appeared particularly vulnerable to criminal use. The sectors were selected based on stakeholders' (local) knowledge and the sectors' potential to cause harm to individuals, businesses, public authorities, and the wider social or physical environment. Theoretically informed by Greenfield and Paoli's (2022) Taxonomy of Bearers and Types of Harm, a guiding questionnaire was developed to help stakeholders identify economic sectors that, within their specific context, contribute to these harms to a greater extent than others (see Annex 10.1). This emphasis on economic (sub)sectors aligns with the priorities set out in the *EU Roadmap to Fight Drug Trafficking and Organised Crime* (European Commission, 2023a), as well as in Europol's (2024a) recent report on the EU's most threatening criminal networks.

After identifying five economic (sub)sectors for each city studied, (at least) **three specific cases** were selected for in-depth analysis, each relating to one of the included (sub)sectors. In total, 28 cases were selected and studied as part of this Work Package. These cases had to meet the following criteria:

- Concerning the criminal use of at least one business in the identified (sub)sector within the city selected for the case study;
- The presence of organised crime;
- Time period: as recent as possible[6];
- Involving more than one perpetrator (i.e., a network)[7];
- Case closed or ongoing;
- Data richness: the quality and quantity of data available for the case must be sufficient.[8]

4.2 Data collection

For each selected case, information was gathered through a combination of **semi-structured interviews** and **case file analyses**. Interviews were conducted with relevant stakeholders who play a crucial role within their respective cities, including representatives from law enforcement agencies (LEAs), public authorities, financial experts, and the business community. They could be interviewed either individually or in (small) groups. To guide the data collection process, address ethical considerations, and maximise the consistency of the collected data across all cities studied, an interview protocol, an information letter, and an informed consent form were provided to all researchers involved. The interviews were structured around several key topics, with related questions, as shown in Table 1. However, interviewers were allowed to deviate from this standardised protocol.

Table 1
Interview protocol: Core topics, subtopics and guiding questions for semi-structured interviews

Key topics	Subtopics and guiding questions
Legitimate business(es) used by the criminal network	- General description of the legitimate business in question; - Legal form of the business; - Business ownership structure (e.g., characteristics of directors and shareholders); - Size of the business; - Additional information.
Criminal network using the legitimate business(es)	- Criminal activities in which the criminal network is involved; - Size of the network (e.g., number of (known) members/leaders); - Network structure (e.g., opportunistic, hierarchical); - Roles of members and their position within the network (e.g., relationships between members, involvement of minors); - Duration of the network's existence;

[6] The determination of the time period was left to the individual researchers, as a balance had to be struck regarding access to information. In recent and ongoing cases, access to judicial files was less likely to be granted due to their (highly) confidential nature.
[7] Currently, there is a trend in which money laundering, a modus operandi of criminal infiltration, is increasingly being 'outsourced' to a professional service provider (i.e., 'money laundering as a service') (CFI, 2021b; Europol, 2021, 2023b). In such cases, however, it must be clear which criminal network instructed the money launderer.
[8] The individual researcher had to determine whether the available data were sufficient in terms of both quantity and quality.

	– Cooperation with other networks; – Use of (legitimate or illegal) facilitators (e.g., crime-as-a-service model); – Additional information.
Crime script on the criminal use of a legitimate business	***Motivation / Purpose of the criminal use of the business*** – Organised crime activities involving the criminal use of the legitimate business; – Stage(s) of the criminal process during which the criminal use of the legitimate business occurs; – *Modus operandi* used during this stage; – Additional information.
	Stage 1: Preparation – Opportunities (i.e., vulnerabilities) of the legitimate business targeted by the criminal network; – Opportunities of the economic (sub)sector targeted by the criminal network (e.g., technology, entry barriers, regulations, levels of competition); – Additional information.
	Stage 2: Pre-activity or enabling conditions – Degree of criminal use of the business (e.g., criminal ownership, infiltration, use of *bona fide* services); – Degree of the company's culpability; – Detailed description of the *modus operandi* of the criminal use of the legal business; – Opportunities utilised during this stage; – Additional information.
	Stage 3: Activity – Management of the legitimate business; – *Modus operandi* used to manage the legitimate business; – Additional information.
	Stage 4: Post-activity or post-conditions – The way LEAs and other authorities have intervened; – Stage of the process at which the case came to the attention of authorities; – Signals of criminal use (e.g., ownership structure, frequent change of company details, profitability); – Additional information.
Harm caused by the criminal use of the legitimate business	– Harm caused to individuals; – Harm caused to other businesses; – Harm caused to public institutions; – Harm caused to the physical environment; – Harm caused to the social environment; – Additional information.

Financial profile of the criminal network	– Origin of the network's start-up capital; – Payment methods used by the network; – Payment arrangements commonly used within in the network; – Costs of carrying out business activities – Revenues and assets of the network – Financial investigations; – Additional information.

All interviews conducted were transcribed *verbatim* and pseudonymised. Where possible, these were complemented with an analysis of police, judicial, or other official records. By combining these two sources of information, the data collected could be compared, verified, and further explored. A document to guide the analysis of these files was also provided to the researchers involved in the project, covering topics similar to those included in the interview protocol. However, not all project partners were able to collect both types of information due to confidentiality issues (cf. *infra*).

4.3 Data analysis[9]

The purpose of the data analysis was to provide, for each case, a descriptive overview of the economic (sub)sectors and legitimate businesses used for criminal purposes, the criminal networks involved, the specific methods applied for the criminal use of the legitimate economy (*modus operandi*), the resulting harm(s), and the network's financial profile. From an analytical perspective, the aim was to reconstruct and describe the operational practices regarding the criminal use of legitimate businesses across various cases and cities. To achieve these objectives, this study combined two analytical methods: **Crime Script Analysis** (CSA) and **Financial Crime Scripting** (FCS). By structuring the analysis in this way, it was possible to identify recurring methods, sector-specific vulnerabilities, and cross-case patterns related to the criminal use of the legitimate economy.

Crime Scripting is a method for generating, organising, and systematising knowledge about the procedural aspects of committing crime (Cornish, 1994). Rather than focusing exclusively on the actors involved, CSA aims to examine how criminal processes unfold step by step in practice (Chiu et al., 2011). Within this research project, CSA was used to reconstruct the sequence of events through which a criminal network made use of a legitimate business, from the initial opportunity to the eventual outcomes. This allowed the analysis to move beyond general descriptions of criminal use of the legal economy, thereby providing a more fine-grained understanding of the specific mechanisms by which legitimate businesses were used for criminal purposes (Chiu et al., 2011; Savona & Riccardi, 2018).

In line with previous research based on Crime Scripting, the criminal process was broken down into four broad stages: the preparation stage, the pre-activity stage, the activity stage, and the post-activity stage (Savona & Riccardi, 2018). However, the data analysis process began with identifying the criminal network's **purpose** (or motivation) to make use of the legitimate business. More specifically, researchers investigated why the business was used as part of the broader criminal operation. In this context, various motives could be identified, such as money laundering, concealing illegal activities,

[9] This data analysis process was carried out for all cases examined as part of this study. For each city, a separate 'city report' was prepared (following a standardised format), based on the analysis of the interview transcripts and case file data. The information from these individual reports was ultimately compiled into this final report.

facilitating labour or sexual exploitation, providing logistical support, or strengthening the network's control over a market. Establishing this 'purpose' was essential, as it enabled researchers to situate the (role of the) legitimate business within the broader criminal process.

The first stage within the crime script, **'Preparation'**, focuses on the opportunities that made a business or (sub)sector attractive to criminal networks. In this context, 'opportunities' are understood as aspects of everyday social and economic life that enable criminal processes (EUCPN, 2018). The second phase, **'Pre-activity'**, refers to the enabling conditions that allowed a criminal network to enter, infiltrate, influence, or control a legitimate business (i.e., *modus operandi* related to the criminal use of the business). These include, for example, the use of front individuals, strategic investments, the abuse of weak regulations or internal controls, and other facilitating arrangements. The third stage, **'Activity'**, describes the manner in which the criminal network practically used, managed, or exploited the business during the criminal process. The fourth and final stage, **'Post-activity'** (or 'post-conditions'), examines what happened after the primary criminal use of the legitimate business had taken place. This includes the continuation of the criminal use, adaptation, concealment, termination, or the persistence of harmful effects.

To complement the CSA analysis, this study also includes a financial analysis based on the method of **Financial Crime Scripting** (FCS), which can be viewed as an extension of Crime Scripting (Cornish, 1994). FCS is a method used to analyse profit-driven crime by generating, organising and systematising knowledge about the financial aspects of the process of crime commission, as well as its interconnections with financial crimes such as money laundering (Snaphaan et al., 2024; Snaphaan & van Ruitenburg, 2024). By focusing on the proceeds, costs, and payment methods within criminal networks, FCS provides insight into the economic processes of organised crime and helps LEAs estimate criminal profits (van Santvoord & van Ruitenburg, 2022). This is particularly relevant given that more than 98% of criminal proceeds in the EU remain unaccounted for, despite the widely recognised importance of a financial approach in the fight against organised crime (Europol, 2016, 2025, 2026; van Santvoord & van Ruitenburg, 2022).

As part of this study, FCS was applied by collecting and analysing information about the financial profile and operations of the criminal network. Where available, this included data on investments, revenues, operational costs, profit structures, payment methods, and the movement of money between legal and illegal activities. The resulting **financial scripts** complemented the 'regular' crime scripts by revealing the economic processes underlying the criminal use of the legitimate economy.

ANTWERP

EMPIRICAL RESULTS

5.1 Introduction: Belgium

5.1.1 Background and context

Belgium's organised crime landscape is shaped by the strategic position of its transportation and trade infrastructure: the **Port of Antwerp** has made Belgium one of the main European entry points for cocaine originating in South America (GI-TOC, 2025b). Moreover, the country functions as a production and distribution centre for synthetic drugs and cannabis, primarily within the Belgian-Dutch border region (Colman, 2018; EMCDDA & Europol, 2024). These illegal markets generate high profits and intensify competition among criminal networks, which has contributed to an increase in drug-related violence in recent years, particularly in Antwerp and Brussels (De Schutter, 2024). Alongside drug trafficking, Belgium serves both a transit and destination country for human trafficking, with criminal networks using legal businesses – such as retail and transportation companies – to facilitate those activities. In addition, the Port of Antwerp is also considered a major entry point for illegal firearms, and a transit point for other illicit trade flows, including counterfeit goods and flora-related crimes (e.g., timber trafficking) (De Schutter, 2024; GI-TOC, 2025b). Antwerp's historic role in the diamond trade also contributes to Belgium's importance as a hub for diamond and gold trafficking (GI-TOC, 2025b).

In Belgium, the legal economy appears to be closely intertwined with organised crime. Criminal networks **systematically use legal businesses** to facilitate and conceal criminal activities, and to launder illicit proceeds (Europol, 2024b; Janssens et al., 2023; Savona & Riccardi, 2018). Furthermore, money laundering is increasingly being separated from the predicate offences that generate illicit proceeds and is being offered as a standalone, specialised service, which can enhance the resilience of criminal networks by enabling them to outsource key financial functions (CTIF-CFI, 2024a). Recent National Risk Assessments in Belgium have identified a particular vulnerability to criminal use and infiltration within certain economic (sub)sectors, including the construction sector, the cash-intensive hospitality industry, and the logistics sector (CTIF-CFI, 2023). In particular, transportation and import-export activities appear to be critical nodes in both legal trade and illicit supply chains (CTIF-CFI, 2024a). Finally, various facilitators and intermediaries have been linked to criminal networks in Belgium, including professionals such as accountants, notaries, and lawyers, as well as employees in strategic positions who have access to sensitive information or critical infrastructure, particularly port workers (CTIF-CFI, 2024a; GI-TOC, 2025b).

5.1.2 Data and methodology

In the process of identifying the economic (sub)sectors most attractive to criminal networks in Belgium, the associated **PREVENT partners** in Antwerp and Brussels were involved, as they were able to provide relevant contacts and open-source references to judicial files. However, after obtaining authorisation from the Attorney General to access specific files via the Public Prosecutor's Office, the information proved insufficient. The judicial files revealed no clear link to organised crime; rather, they involved breaches of social law. To address this, staff members from the Financial and Economic Crime Section of the **Federal Judicial Police** (FJP) in Antwerp and Brussels were consulted to amend the list of economic (sub)sectors. These officials expanded the list of sectors initially drawn up by the associated partners (i.e., the City of Antwerp, the Municipality of Saint-Gilles, and the local police of Brussels South, who were consulted informally) and provided reference numbers of judicial files, which were

then used to formally request access through the Public Prosecutor's Office.[10] Once approved, the court registry made the files available via the Digital Portal of the Justice Federal Public Service (FPS) for a limited period, ranging from one day to three months. In Brussels, however, access to three cases was not possible, as most files were still under investigation. Additional insights were therefore obtained through an interview with an official from the Belgian **Financial Intelligence Unit** (FIU).[11] An overview of all respondents interviewed as part of the Belgian data collection process can be found in Table 21 (see Annex 10.2).

5.1.3 Critical remarks

First, it should be noted that there is a **difference in perspective** between local authorities and LEAs regarding the phenomenon of the criminal use of the legal economy: municipal authorities tend to focus on the facilities and processes that support organised crime, whereas the police and judicial authorities are primarily concerned with the criminal activities themselves (Algemene Directie Veiligheid & Preventie, n.d.). This divergence is understandable, given their differing institutional responsibilities. Moreover, these divergent approaches also entail a potential for bias, as several cases that the municipal officials identified as potentially linked to organised crime could not be substantiated in judicial files held by the Public Prosecutor's Office. However, this does not necessarily imply the absence of such links. As an official from FJP Antwerp noted, capacity constraints within the police and prosecution services can hinder thorough investigations and cross-case analyses. Consequently, the public prosecutor may prioritise prosecuting smaller social or financial offences with a higher likelihood of conviction over broader, resource-intensive investigations into organised crime, where the risk of non-conviction is greater.

Second, attention should also be paid to the varying approaches of the **administrative approach** across Belgium, and the unintended consequences of administrative inspections, since they may prompt fraudulent businesses to regularise their licensing and administration, thereby making themselves temporarily immune to further administrative sanctions. This paradox illustrates a tension in the administrative approach being used: the pursuit of order can inadvertently contribute to the continued existence of suspicious businesses.

5.1.4 Identification of vulnerable (sub)sectors in Antwerp

Both representatives of the City of Antwerp and the Antwerp FJP indicated that the criminal use of the legal economy has **increased significantly** in recent years. City officials, however, added an important nuance: heightened public and policy attention has led municipal authorities to focus more closely on this issue. In other words, the observed increased in the criminal use of legitimate businesses can be attributed to both an actual rise in criminal activity and to a greater policy focus and public attention, resulting in more cases being detected. Although the FJP asserts that the level of criminal use has increased substantially, its exact magnitude remains difficult to quantify.

[10] As the FJP operates in the final stage of the investigative chain and handles cases that have already been addressed by local authorities and the local police, its involvement ensured that the cases under consideration were linked to criminal networks operating within the legal economy.

[11] The Belgian Financial Intelligence Unit is called 'CTIF-CFI' (*Cellule de Traitement des Informations Financières – Cel voor Financiële Informatieverwerking).*

Perceptions of **'vulnerable' economic (sub)sectors** differed across respondent groups. According to municipal officials, the hospitality industry, massage parlours, the real estate sector, the taxi industry, and newsagents are particularly attractive for criminal use. City officials consider these sectors high-risk due to low entry barriers, their cash-intensive nature, and the high degree of anonymity. Officials of the Antwerp FJP [R1_BE; R6_BE; R7_BE] have also identified the hospitality industry as a vulnerable sector, alongside construction, cleaning and service industries, garages, car dealerships, beauty salons, hairdressers, and barbershops. These sectors are characterised by large-scale cash transactions, limited transparency, the relative ease with which employees can be registered, opportunities for renovations, and the potential to conceal undeclared work through partial or full cash payments. For this reason, the Belgian FIU [R3_BE] also considers the construction and automotive sectors to be particularly vulnerable, as well as business centres. In addition, some FJP representatives mentioned the diamond industry, which is unique to Antwerp, and the logistics sector, as the Port of Antwerp is known for the import of prohibited goods. Finally, one respondent [R1_BE] pointed to the travel sector, specifically travel agencies that still accept cash payments and thus operate outside the regular financial control systems.

Based on these insights, five economic (sub)sectors emerged as recurring themes in the case studies: the **hospitality, car rental, logistics, construction, and real estate** sectors. In August 2025, the City of Antwerp had a total of 99,208 registered businesses. Of these, 5,449 establishments were active in the hospitality industry[12]; 18,263 in wholesale, retail and motor vehicle repair; 6,145 in construction; 3,409 in transportation and logistics; and 3,100 in the real estate sector (Stad Antwerpen, 2025). However, there is no publicly available data that allows to assess or measure the size of the illegal economy, nor the extent to which legitimate businesses in these sectors are being used for criminal purposes sectors.



[12] In the context of Antwerp, the hospitality sector is particularly relevant, as the city positions itself as one of the leading hospitality destinations in Flanders (Stad Antwerpen, n.d.).

5.2 Case Alfa: Laundering Cocaine Profits in Antwerp

Case Alfa concerns a criminal network that operated in and around Antwerp and was involved in large-scale **cocaine imports** through the Port of Antwerp (see Annex 1.A). To conceal and **launder their illicit profits**, the network systematically used legitimate businesses, particularly in the hospitality industry and car rental sector. The main methods used by the organisation to launder money included the use of false payslips and invoices, undocumented transfers of business assets, and cash compensation schemes. The judicial investigation revealed that the network generated more than EUR 5 million in illicit proceeds between 2014 and 2020.[13]

5.3 Case Bravo: Infiltrating Antwerp's Logistics Chain

Case Bravo concerns a criminal network that operated in and around Antwerp and used a legitimate logistics provider operating in the Port of Antwerp to facilitate the **import of cocaine** (see Annex 1.B). Collaboration of this company's employees was secured through bribery and the threat of violence. To conceal and launder their criminal proceeds, they also infiltrated companies operating in the hospitality sector. The main methods used by the network include trade-based money laundering through fictitious invoicing between companies connected to the network, as well as fiscal fraud through intra-community acquisitions of luxury vehicles.

5.4 Case Charlie: From Cannabis to Concrete

Case Charlie concerns a criminal network that operated in Antwerp and infiltrated legitimate limited partnerships to **launder drug proceeds** through company accounts, the use of intermediaries, and real estate transactions (see Annex 1.C). The network is centred around the international family clan of the *de facto* leader C1_C, who diverted funds to C2_C. This money was invested in real estate and, to a lesser extent, cryptocurrency. However, since the ongoing investigation focuses only on one branch of a larger international clan, the evidence base in this case remains rather fragmented.

[13] It should be noted that all monetary figures mentioned in the Belgian cases studies should be regarded as lower-bound estimates. They represent exclusively the transactions and assets that the authorities were able to identify and include in the case files, and therefore do not reflect the full extent of the financial flows within criminal networks. When calculating unlawfully obtained assets in criminal investigations, it is common practice to apply a methodology that favours the suspect (Arts. 42 to 43quater of the Belgian Criminal Code). This ensures that all uncertainties are interpreted in favour of the dependant, in accordance with the presumption of innocence as established in Article 6.2 of the European Convention on Human Rights (ECHR). The calculated amount therefore represents a minimum estimate and serves as a lower limit for the unlawfully acquired assets.

BRUSSELS

EMPIRICAL RESULTS

6.1 Identification of vulnerable (sub)sectors in Brussels[14]

According to the official of the Brussels FJP [R5_BE], **cash compensation schemes** appear to be common in Brussels (and Antwerp, and to a lesser extent in Ghent) but are virtually non-existent elsewhere in Belgium. This is closely linked to the fact that the labour market in the Brussels-Capital Region is characterised by a high density of companies in the services sector (Leefmilieu Brussel, 2025). Given the sheer number of existing entities, it is relatively easy to set up additional (shell) companies that blend into the vast mass of businesses and service providers, thereby facilitating the concealment of fictitious invoices and compensation flows [R5_BE]. However, notable geographical differences exist in the number of suspicious enterprises in Brussels. The police zone Brussels South recorded the highest number, closely followed by Brussels West. Brussels North and Brussels Capital also reported relatively high numbers, reflecting their location in the city centre, while Montgomery and Marlow recorded substantially fewer cases [R8_BE].

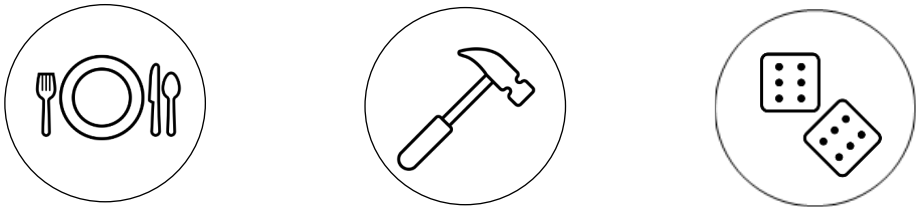
Law enforcement officials [R5_BE; R8_BE] have noted an **increase in investigations** concerning the criminal use of the legitimate economy. Although this may reflect an actual increase in the use of the legal economy by organised crime groups, the respondents also pointed to the appointment of a new public prosecutor in Brussels, who explicitly prioritises a 'follow the money' approach. Every major drug investigation now includes a dedicated money laundering investigation, which means that financial follow-ups are no longer considered a side issue. Furthermore, these officials also identified several specific trends. Between 2019 and 2024, an inconsistency existed between the requirements in Brussels and Flanders for operating a business: in Flanders, proof of professional competence was no longer required, whereas it remained mandatory in Brussels (Vlaamse Overheid, n.d.-a). This resulted in a substantial relocation of businesses to business centres just outside the Brussels periphery. However, after Brussels adopted the same approach in 2024, businesses began relocating back (Brussels Hoofdstedelijk Gewest, n.d.).

Consultations with the local police of Brussels South and officials from the municipality of Saint-Gilles allowed to identify several **vulnerable economic (sub)sectors** in Brussels. The hospitality and construction industries, in particular, were identified as vulnerable, just as in Antwerp. Other sectors mentioned included the beauty industry, hair salons, barbershops, newsagents, and car washes. Unlike in Antwerp, stores selling workwear and professional attire, night shops, gold and silver buyers, and bars with gambling machines were also mentioned. Law enforcement officials [R5_BE; R8_BE] have confirmed that these sectors are particularly vulnerable, citing the construction and hospitality sectors, as well as the cleaning industry and the services sector more broadly. These sectors are attractive to criminals because of their accessibility, even for people without formal qualifications, combined with high cash flow and the difficulty of controlling the services provided. During the COVID-19 period, LEAs also observed a shift from hospitality businesses to taxi companies being used by criminal networks.

[14] For a general introduction to the background, context, data, methodology, and critical remarks relating to the case study in Brussels, see Sections 5.1.1 to 5.1.3.

Findings from the interviews further suggest that the **hospitality sector** is perceived as particularly attractive to criminal networks in specific areas of the city. For example, one respondent [R8_BE] noted: "Take the hospitality sector around the Brussels South Station; ninety-nine percent of the hospitality establishments there is somehow connected to the criminal milieu." With regard to the hospitality industry, particular attention was paid to bars and cafés offering games of chance. The presence of bingo machines and other **gambling devices** in Brussels cafés has been reported for several years, with open-source information indicating a particularly high concentration of such establishments in the Brussels-Capital Region compared with other provinces (Hendrickx, 2024). As of February 2026, the Region reportedly contained 800 establishments operating such games of chance, 246 of which are located in the Brussels South area (Kansspelcommissie, n.d.-a).

Based on these insights, two economic (sub)sectors emerged as recurring themes in the case studies: the **hospitality and construction** sectors, including bars where **gambling facilities** are provided. This selection reflects both the economic significance of these sectors within the Brussels urban economy and their perceived relevance in relation to the criminal use of legitimate business structures. According to 2024 registered-establishment figures, Brussels contained 7,260 hospitality establishments, 14,938 construction establishments, and 115 establishments classified under lotteries and gambling activities (BISA, 2026). However, no publicly available data source allows a systematic assessment of the degree of criminal use of legitimate businesses in these (sub)sectors or its general development over time.



6.2 Case Delta: The Brussels Brazilian Filière

Case Delta concerns a Brussels-based criminal network, specialised in **money laundering through cash compensation schemes** and centred on C1_D, his close relatives, and associates (see Annex 2.D). Two accountancy firms were established as central hubs linking the various parties involved in the compensation system. Through these firms, the network facilitated collaboration between criminal actors holding large volumes of illicit cash and companies requiring cash to pay employees off the books. Cash derived from organised criminal activity – including prostitution exploitation, drug trafficking, and the trade in forged documents – was handed over by money couriers to Belgian companies operating in sectors susceptible to fraud, primarily cleaning and construction. In return, these companies executed bank transfers of equivalent value to accounts in Belgium and abroad, justified through fictitious invoices. This structure ensured that the most suspicious element, the handling of cash, remained outside the formal banking system. Meanwhile, the criminals who had initially supplied the cash received seemingly legitimate balances that had been laundered through invoicing chains. This case exemplifies the '**Brazilian *filières***' phenomenon in Belgium.

6.3 Case Echo: Façades and False Invoices

Case Echo concerns a Brussels-based criminal network, specialised in **money laundering through cash compensation schemes** involving several façade companies that issued false invoices to labour-intensive businesses, primarily in the construction sector (see Annex 2.E). The network was also involved in intra-Community VAT fraud linked to the trade in telecommunications products. In 2025, its members and the associated legal entities were convicted, and more than EUR 19 million was confiscated.

6.4 Case Foxtrot: Games of Chance and Channels of Cash

Case Foxtrot concerns practices of **gambling-related money laundering** through legal games of chance in Brussels bars (see Annex 2.F). Unlike the other Brussels cases discussed in this report, the discussion of Case Foxtrot is not based on judicial files but solely on a semi-structured interview with an official of the Brussels FJP. This methodological limitation substantially constrained the level of detail available, particularly regarding the criminal network involved and its financial profile. The case was nevertheless included in this report, as the Brussels stakeholders (i.e., the Municipality of Saint-Gilles, the local police of Brussels South, and the Brussels FJP) consistently identified the phenomenon as highly problematic yet marked by limited objective information and legal ambiguity.

6.5 Financial investigations in Belgium: key challenges and recommendations

6.5.1 Challenges in financial investigations in Belgium

In Belgium, **financial investigations** typically begin with a referral from the Belgian FIU, which receives reports from banks, notaries, lawyers, and other entities subject to reporting obligations under the Law of 18 September 2017.[15] Once a reporting entity identifies a suspicious transaction, it conducts an internal assessment and forwards the relevant information to the FIU (Art. 79). FIU analysts then examine the financial flows and may request additional information, for example from police liaison officers, who verify whether the individuals or companies concerned appear in judicial databases (Art. 81). Where there are sufficient indications of money laundering or terrorist financing, the FIU may refer the case to the Public Prosecutor's Office (Art. 82). In certain circumstances, the FIU may also temporarily freeze a transaction for up to five business days pending a judicial decision on seizure (Art. 80). This mechanism helps ensure that potentially illicit funds remain within the financial system and can subsequently be confiscated, where appropriate. If the public prosecutor decides to refer the case to the FJP, a financial judicial investigation is conducted. Such investigations may originate from FIU reports, but may also arise in the context of broader criminal investigations in which financial elements come to light.

[15] Wet van 17 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, *BS*, 6 oktober 2017.

Against this background, a first set of challenges concerns the **institutional organisation** and **case flow** of financial investigations in Belgium. Respondents from the FJP [R1_BE; R8_BE] highlighted a lack of consistency in how cases are assessed and handled across judicial arrondissements. Similar facts may result in different operational or prosecutorial responses depending on the arrondissement concerned, leading to fragmentation and inconsistency (see quotation below).[16]

> **Challenge 1 – Institutional organisation and case flow**: *"On one side of the road, if I establish the same infringements as in the specific restaurant I am inspecting there, then I know that I will affix the seals here. But when I am on the other side of the road and I have been in consultation with the Public Prosecutor's Office for fifteen minutes, and I cannot get them to agree to sealing it. That is a problem."* [R8_BE]

A second set of challenges concerns **capacity constraints** and **investigative prioritisation**. Limited staffing across the FIU, Public Prosecutor's Offices, the FJP, and inspection services makes the prioritisation of cases unavoidable. For law enforcement officials, triage and prioritisation create a persistent dilemma: whether to broaden an investigation to uncover the wider criminal financial infrastructure or to conclude it once a prosecutable evidentiary threshold has been reached (see quotation below) [R6_BE; R7_BE].[17] Although narrowing the scope of a case may increase the likelihood of conviction, it may simultaneously limit the ability to identify and dismantle criminal networks operating across multiple sectors and cases [R6_BE; R7_BE; R8_BE].

> **Challenge 2 – Capacity constraints and investigative prioritisation**: *"And that is the difficult part in our department, I think. Either, on the one hand, you are going to open it up further, and you can spend years working on all those companies, because that's how it works. Those are all shell companies. And then you are going to involve all of them, but we simply do not have the capacity, the resources, or the time for that. Or you discuss it with your Public Prosecutor's Office and say: 'Okay, this and this is what we have demonstrated now, that is the evidence. We cut it off there.'"* [R6_BE]

[16] Original quotation in Dutch: "[…] zeer dicht op de Brusselse rand (…), dus eigenlijk een grote steenweg. Aan de ene kant is Brussel, aan de andere kant is Halle-Vilvoorde. Aan de ene kant van de steenweg, als ik dezelfde inbreuken vaststel als het specifieke restaurant dat ik daar controleer, dan weet ik dat ik hier de zegels opleg. Maar nu zit ik aan de andere kant van de steenweg en ben ik een kwartier in overleg met het parket en krijg ik het niet verkocht om het te verzegelen. Dat is een probleem."

17 Original quotation in Dutch: "En dat is het moeilijke bij ons op de afdeling, denk ik. Oftewel ga je enerzijds opentrekken, en ben je jaren bezig aan al die ondernemingen, want zo werkt het. Dat zijn allemaal schermvennootschappen. En dan ga je die allemaal betrekken, maar daar hebben wij de capaciteit, de middelen en de tijd niet voor. Oftewel ga je bespreken met uw parket en zeg je: 'Oké, dit en dit hebben we nu aangetoond, dat is het bewijs. We kappen het af.'"

However, respondents emphasised that the challenges related to financial investigations are not solely a matter of staffing. A third and closely related challenge concerns **inefficiencies in administrative procedures**, information management, and investigative tools. Several interviewees stressed the absence of an efficient, chain-oriented system that allows for the systematic exchange and cross-referencing of information [R1_BE; R5_BE; R8_BE]. Financial investigators often encounter fragmented data environments, where relevant information is scattered across different institutions and stored in incompatible formats. This slows down the investigative process, makes cross-referencing difficult, and absorbs considerable investigative time. One respondent, for instance, noted that banks provide account data in different Excel formats, using varying coding systems, meaning that simply organising and merging the files can take more than a week [R6_BE]. Respondents also referred to excessive bureaucratic hurdles for relatively basic operational tasks, illustrating how cumbersome procedures can reduce the efficiency of financial investigations (see quotation below).[18]

Challenge 3 – Inefficiencies in administrative procedures: *"To purchase a CD-ROM, we have to request a written instruction from the public prosecutor. That means we have to ask a magistrate whether we are allowed to buy a DVD."* [R7_BE]

A fourth, more general challenge is that law enforcement officials often struggle to keep pace with ongoing **criminal innovation** (see quotation below).[19] This suggests that professional money laundering networks adapt more rapidly than investigative knowledge, training, and technical capabilities. In the same vein, respondents also noted the relative underuse of special investigative techniques in financial investigations. Methods such as communication interception, covert observation, infiltration, and other special investigative techniques are standard practice in organised crime and drug investigations but appear to be less systematically integrated into financial investigations, despite their potential added value in mapping the broader criminal infrastructure underlying financial flows [R5_BE].

Challenge 4 – Adapting to criminal innovation: *"I think, for the real professional criminal money launderers, this is old-school money laundering. (…) We catch the 'simple ones' when they make mistakes. (…) The techniques being used [by criminal networks, red.] are, in my view, techniques that were popular five years ago. And now, there are new techniques that we simply do not know yet.'"* [R6_BE]

[18] Original quotation in Dutch: "Om een cd-rom aan te kopen moeten wij een kantschrift vragen. Dan moeten wij aan een magistraat vragen of we een dvd'tje mogen kopen."

[19] Original quotation in Dutch: "'Ik denk, voor de echte professionele criminele witwassers, is dit oldschool witwassen (…). De dommeriken halen we eruit, als zij foutjes maken. (…) De technieken die worden gebruikt, dat zijn technieken die volgens mij vijf jaar geleden populair waren. En nu zijn er lang nieuwe technieken die wij gewoon nog niet kennen.'

A fifth challenge concerns access to financial information and **reliance on private actors**. Banks hold crucial real-time transaction data and are legally required to monitor and report suspicious activity. However, respondents noted that compliance functions are often viewed primarily as a cost centre rather than a revenue-generating activity, which may reduce incentives for proactive, sophisticated or real-time detection [R5_BE]. These challenges are compounded by the international nature of financial flows. Funds can move across borders within seconds, whereas access to the corresponding financial information is constrained by legal safeguards, prosecutorial filters, and differences between national systems. Requests for information must pass through domestic procedures and mutual legal assistance channels, slowing the transmission of intelligence to frontline investigators. Even within the EU, practices vary: in some jurisdictions, law enforcement authorities have more direct access to FIU information, whereas in Belgium an additional prosecutorial layer is always required. Although such safeguards are important for protecting privacy and personal data, they can reduce the agility of complex financial investigations [R5_BE]. In addition, funds may be channelled through countries that are unwilling or unable to cooperate effectively with requests for legal assistance [R3_BE; R5_BE]. Respondents also identified geopolitical tensions within the Egmont Group as a factor that can further complicate **cooperation between FIUs**.

A sixth challenge concerns the characteristics of financial flows themselves. Several interviewees emphasised that **cash** remains highly significant in criminal circles. As cash transactions leave limited traceable records, investigators must often rely on indirect indicators, such as observations or encrypted communications. At the same time, digitalisation and the emergence of **new financial technologies** are creating additional blind spots. The boundaries between traditional banks, technology companies, and commercial financial service providers are becoming increasingly blurred.

> **Challenge 6 – Increasing use of cryptocurrencies**: *"If it is already converted into crypto, it leaves immediately and then it starts. You can follow that blockchain, you can see those cryptos moving like that, but then it goes to that wallet, to that wallet, to that wallet, and you first have to find out where that wallet was created. And then, in all those countries, you basically have to request the identification of who is behind that wallet. So, well, very often we do not even start working on those cases."* [R5_BE]

Within the payment service provider (PSP) sector, traditional banks increasingly operate alongside newer players, such as Wise and Klarna, which function as electronic money institutions or fintech companies.[20] Technology firms also provide the underlying payment infrastructure and software used by these PSPs [R3_BE]. While this evolution reflects technological innovation and increasing business complexity, it also creates regulatory and supervisory challenges. The fragmentation of responsibilities within digital payment systems can make it unclear which party is responsible for Know Your Customer (KYC) controls and the reporting of suspicious activity, potentially weakening the effectiveness of financial oversight.[21]

[20] For the current consolidated version of the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366.

[21] The 'Know Your Customer' (KYC) policy was established in Europe with the first AML Directive (91/308/EEC) in 1991.

A particularly important development in this regard is the growing **use of cryptocurrencies** [R3_BE; R5_BE; R6_BE; R7_BE; R8_BE]. Although transactions on public blockchains remain visible and can often be traced, the underlying data are pseudonymous, making attribution difficult. This challenge is compounded when criminal actors rapidly transfer funds between multiple wallet addresses, frequently generate new wallets and abandon previously used ones, thereby fragmenting transaction trails and obscuring the identities of those involved. The challenge is even greater in peer-to-peer transfers through unhosted wallets, where no virtual assets service provider or other obliged entity is involved (see quotation above).[22] In such cases, no intermediary may collect customer identification data or file suspicious transaction reports, which reduces the visibility of competent authorities and increases the investigative burden across jurisdictions (FATF, 2026).

Finally, respondents highlighted **broader structural tensions** that shape the environment in which financial investigations take place. Certain policy measures intended to promote entrepreneurship, such as removing minimal capital requirements for private limited companies and simplifying incorporation procedures, may simultaneously lower barriers to criminal use (Wittevrongel & De Jaeger, 2024). The lack of effective identity checks in the Crossroads Bank for Enterprises was cited as a further example. This tension is particularly evident in the Port of Antwerp, where efforts are made to maintain its position as a major hub. Although accelerated container handling enhances economic efficiency, it also reduces opportunities for inspection, thereby potentially increasing the port's vulnerability to organised crime.

6.5.2 Recommendations for improving financial investigations in Belgium

Recommendation 1 – Prioritise the financial dimension from the outset

A first recommendation is to address the financial dimension of criminal activity from the outset, rather than waiting until the predicate offence has been established. Respondents repeatedly emphasised that financial investigations are often introduced too late, despite the potential of financial flows to reveal the wider criminal infrastructure underlying a case. One way to address this would be to initiate parallel money laundering investigations alongside investigations into the underlying offence as a matter of course. As money is often the common denominator across different forms of organised crime, financial expertise should be integrated earlier and more structurally into investigative processes. In this regard, respondents' observations on the increased attention for financial crime under the new public prosecutor in Brussels suggest that prosecutorial leadership can play an important role. This recommendation is closely linked to the relatively **low operational priority** still assigned to financial offences. Respondents indicated that financial investigations are often ranked below offences involving drugs, violence, or terrorism because they are not perceived as posing an immediate threat to physical safety. As a result, financial investigators may face difficulties in accessing special investigative methods, even where these are necessary to trace criminal financial flows or identify the wider network behind them.

[22] Original quotation in Dutch: "Als het al in crypto's wordt omgezet, dan vertrekt dat direct en dat begint. Je kunt die blockchain volgen, hé. Je ziet die crypto's zo gaan, maar dan gaat dat naar die wallet, naar die wallet, naar die wallet, en je moet al te weten komen waar die wallet is gecreëerd. En dan moet je in alle landen eigenlijk die identificatie gaan opvragen, wie er achter die wallet zit. Dus heel vaak starten wij zelfs niet aan die dossiers."

"But the big problem with those offences is simply that you are not really harming third parties in terms of physical integrity. We always come last… We have investigations where we use special investigative methods. (…) That also works through a list of priorities. (…) Yes, in terms of priority, we end up at the bottom because nothing dangerous is happening."[23] [R6_BE]

Therefore, a more systematic integration of financial expertise should be accompanied by a corresponding shift in operational and prosecutorial priorities, ensuring that financial investigations are not treated as secondary to other forms of organised crime.

Recommendation 2 – Reassess high-risk cash-intensive sectors

A second recommendation is to reassess sectors in which cash payments remain permitted, with particular attention to their vulnerability to money laundering. In Belgium, the legal limit for cash transactions is currently set at EUR 3,000 (FOD Economie, 2024). Although this limit provides a degree of control, cash transactions remain difficult to trace and therefore continue to present anti-money laundering risks. At the same time, respondents emphasised that the complete abolition of cash would be unrealistic and could have unintended consequences. Cash continues to serve legitimate purposes and provides resilience in the event of digital outages or cyber incidents. Moreover, stricter domestic limits could simply displace criminal activity to other jurisdictions or informal systems. Rather than seeking to eliminate cash altogether, a more targeted approach would therefore be preferable. Policymakers should identify the **cash-intensive sectors** that pose the greatest risks and consider whether sector-specific restrictions, enhanced reporting requirements, or additional safeguards are warranted.

Recommendation 3 – Modernise investigative tools and streamline procedures

Building on the first recommendation, the third one is to improve the operational conditions under which financial investigations are conducted. Respondents highlighted the continued reliance on outdated software and the manual processing of substantial volumes of banking data, often without access to specialised analytical tools. The factors unnecessarily slow down financial investigations. Respondents also pointed to disproportionate bureaucratic hurdles in basic operational matters, which further constrain investigative capacity. Strengthening financial investigations therefore requires investment in **modern digital tools**, specialised software, and data-processing capacity, alongside a more user-friendly operational infrastructure. Administrative procedures that delay routine investigative work should also be reviewed and streamlined.

Recommendation 4 – Improve information sharing

A fourth recommendation is to improve the flow of financial information between the Belgian FIU, Public Prosecutor's Offices, police services, inspection bodies, and other relevant actors. Respondents repeatedly emphasised that information remains fragmented across institutions, resulting in inefficiencies, duplicated efforts, and missed links between cases. A **more structured cooperation** framework is therefore needed to facilitate the systematic exchange and cross-referencing among relevant partners. In addition, respondents stressed the need for greater standardisation in the

[23] Original quotation in Dutch: "Maar het grote probleem met die misdrijven is gewoon... Je schaadt er eigenlijk geen derden mee, de fysieke integriteit. Wij komen altijd als laatste... Wij hebben zo onderzoeken waar je dan de BOM-maatregelen (Bijzondere Opsporingsmethoden, red.) doet. (…) Dat is ook via een prioriteitenlijst. (…) Ja, prio-gezien vallen wij onderaan, want er is niks gevaarlijks aan het gebeuren."

transmission of banking data. Banks currently provide account and transaction data in different formats and coding systems, requiring investigators to spend considerable time reorganising the data before substantive analysis can begin. Introducing a uniform format for the transmission of such data would therefore provide immediate operational benefits.

Recommendation 5 – Keep pace with digitalisation and technological change

A fifth recommendation is to ensure that financial investigators' knowledge and expertise keep pace with digitalisation and ongoing technological developments. Respondents emphasised that criminal actors often innovate more rapidly than investigative knowledge, training, and capabilities can adapt. This is particularly evident in the growing significance of cryptocurrencies, unhosted wallets, new payment service providers, and hybrid fintech structures. To remain capable of tracing value across increasingly complex digital and cross-border environments, financial investigators therefore require continuous training and specialised expertise.

Recommendation 6 – Strengthen and expand specialised multidisciplinary teams

A sixth recommendation is to strengthen and expand specialised multidisciplinary teams within the Federal Judicial Police (FJP). Both FJP Brussels and FJP Antwerp have developed such specialised capacity, albeit in different forms. In Brussels, the 'BELFI team' was created in 2014 as part of efforts to disrupt terrorist financing, but has since evolved into a broader **multidisciplinary model** aimed at dismantling commercial structures linked to organised crime.[24] In Antwerp, the 'DIFA approach' focuses on the direct and indirect financial disruption of businesses connected to major drug-related criminal networks (Federale Politie, 2020). Although these models differ in scope and operational approach, both demonstrate the added value of specialised teams that combine financial expertise with intelligence-led, field-based interventions involving relevant partners. A broader national rollout of such specialised capacity could promote greater consistency across judicial districts and reduce the risk of displacement or 'waterbed effects', whereby stricter enforcement in one area merely shifts criminal activity elsewhere. At the same time, respondents also highlighted the value of more targeted, integrated initiatives that bring together relevant actors around a clearly defined phenomenon.

Recommendation 7 – Strengthen the administrative approach

A seventh recommendation is to further strengthen the administrative approach to organised crime, while also ensuring adequate safeguards. Both respondents and the existing literature emphasise that criminal law interventions alone are insufficient to disrupt the business models and core structures of organised crime groups (Kruisbergen et al., 2012; Spapens et al., 2015). **Administrative measures** can complement criminal investigations by providing additional opportunities for intervention through licensing, local controls, permits, inspections, and information exchange (ENAA, 2020). At the same time, the interviews indicated that the administrative approach remains uneven across Belgium (Janssens et al., 2023). In some areas, local authorities are unaware of the possibilities available to them, while in others, its implementation depends heavily on local political will. This points to a need for stronger administrative action, clearer guidance, and additional training, as well as greater national consistency in the use of these powers.

[24] De Kamer van Volksvertegenwoordigers – Schriftelijke vraag en antwoord nr. 55-367: BELFI-project – Belgian Fighters, 08/06/2021, www.lachambre.be.

Recommendation 8 – Close loopholes in specific legislation

An eighth recommendation is to close loopholes in specific areas of legislation, particularly **gambling regulation**. For example, respondents pointed out that Article 27 of the Belgian Gambling Act can be circumvented in practice.[25] Although gambling operators are not permitted to own the premises in which gambling activities take place, this restriction can reportedly be bypassed through rental and subletting arrangements, whereby operators become tenants rather than owners while retaining substantial control over the premises and gambling activities. According to the interviews, this loophole is not yet being adequately addressed in practice. This points to a need for a stricter interpretation or amendment of the legal framework to ensure that the intended safeguards cannot be circumvented through formal contractual arrangements. Respondents also noted that municipalities currently have limited scope to act when they issue negative advice on gambling licences that are nevertheless granted (Hendrickx, 2024). If local authorities are expected to identify and contain local criminal risks, they should also be given sufficient regulatory powers to do so.

6.6 Summary of research findings: Belgium (Antwerp and Brussels)

The case studies of Antwerp and Brussels consistently show that the legitimate economy is an indispensable environment for criminal networks. Legitimate businesses are used as multifunctional tools to launder criminal proceeds, facilitate predicate offences, provide concealment, embed criminal actors within legal markets, and normalise illegal activity in everyday economic life. Several cross-case study findings stand out.

Firstly, the Belgian case studies suggest that **certain economic sectors** are **more vulnerable** to criminal exploitation than others. At the same time, many of these vulnerable sectors are attractive for similar reasons, as they facilitate the same underlying functions. The hospitality sector, for instance, is appealing because it is cash-intensive, generates high volumes of small and difficult-to-verify transactions, allows manipulation of turnover, and often relies on flexible staffing arrangements. Construction and cleaning are vulnerable because labour can be partly undeclared, service delivery is difficult to verify, subcontracting chains are opaque, and false invoicing can appear plausible. Accounting firms and company service providers are particularly important because they can facilitate criminal activity by setting up companies, managing mandates, opening accounts and coordinating invoice chains. Therefore, vulnerability lies less in the sector itself than in the combination of functions it offers, such as opacity, cash intensity, administrative flexibility, weak verification, and the possibility of creating credible documentary cover. In practice, this means that some criminal networks do not depend on a single type of business in a specific sector, but maintain what one interviewee described as a 'wallet' of businesses that can be used *à la carte* whenever a specific function is needed. This supports the methodological observation made by several interviewees that the focus should be placed less on fixed 'vulnerable sectors' and more on the *modus operandi* that these sectors enable.

[25] Art. 27 of the Law of 7 May 1999 on games of chance, betting, gaming establishments and the protection of players, *Belgian Official Journal,* 30 December 1999.

Secondly, the case studies primarily revealed a high level of criminal use of the legitimate economy, including businesses that were criminally owned from the outset and deliberately established to launder money, issue fictitious invoices, or provide an appearance of legitimacy. This finding is partly shaped by the data collection methodology, as the case files were obtained primarily through the FJP and therefore concern cases that had progressed beyond the remit of local authorities. Nevertheless, the material makes clear that the **criminal use** of businesses **takes multiple forms**. Alongside outright criminal ownership, some cases involve *bona fide* businesses that were infiltrated by employees without the business's knowledge. Other cases occupied an intermediate position, involving businesses that combined legitimate economic activity with criminal activity or that began as legitimate enterprises but gradually became incorporated into a criminal business model.

A third finding concerns **money laundering**, which the case studies showed could be both an objective in itself and a means of facilitating the criminal use of the legitimate economy. It rarely relies on a single technique but instead involves methods ranging from relatively simple arrangements to highly complex schemes. Common methods include commingling illicit cash with legitimate turnover, fictitious payrolls and invoices, TBML through fabricated invoices, undocumented asset transfers, and cash compensation systems. These methods are used to facilitate tax and social fraud, bankruptcy offences, documentary fraud, and the operation of the wider criminal business model. According to the Belgian FIU, a significant proportion of money laundering transactions are linked to the drug economy, as drug-related organised crime generates financial flows on this scale.

Closely related to this, several respondents [R1_BE; R3_BE; R5_BE] and the case studies point to two broad types of criminal network: some networks maintain their own internal money-laundering structures, while others operate as professional money-laundering networks providing services to multiple criminal groups. Case Delta illustrate a business model in which intermediaries connect criminal actors with surplus cash to legitimate businesses in need of off-the-books cash, profiting from this interface. This represents a clear example of '**crime-as-a-service**'. In recent years, money-laundering activities appear to have become increasingly detached from the underlying predicate offences and are increasingly offered as autonomous services within the illegal economy.

Beyond money laundering, the case studies reveal a **wide range of *modus operandi*** used by criminal networks. Recurring methods include the use of strawmen, facilitators such as accountants and logistics planners, and corrupt employees in businesses essential to the criminal business model. These methods are often combined, for example through sham companies operated by strawmen, the coercion or intimidation of facilitators, and complex corporate structures designed to maximise illicit profits through tax and intra-Community fraud, social fraud, and the laundering of criminal proceeds.

Furthermore, the case studies highlight the **instrumental use of corporate forms** with low barriers to entry and limited transparency requirements, which interviewees explicitly linked to features of the Belgian business environment. The most commonly used legal form was the private limited company (LTD; n = 30), followed by general partnerships (GP; n = 3) and limited partnerships (LP; n = 3). Although an LTD no longer requires a fixed minimal capital contribution, sufficient starting capital must in practice be demonstrated through a financial plan (Vlaamse Overheid, n.d.-b). Belgian law enforcement officials [R5_BE and R6_BE] and CTIF-CFI (2019) have also warned of the increasing use of GPs and LPs by organised crime groups. These forms are particularly attractive because they require no initial capital

contribution and can be established through a private rather than a notarial deed. This removes notaries, who are legally required to report suspected money laundering to the FIU, as a potential point of detection. LPs are generally not required to prepare annual accounts and, where they are, may not be required to publish them. Their main disadvantage is that active partners may be held personally and without limitation liable for company debts. This risk can, however, be mitigated by appointing strawmen as managing partners (Wittevrongel & De Jaeger, 2024).

Finally, although the Belgian case studies demonstrate that criminal networks use businesses in flexible and adaptive ways, they also reveal several **recurring red flags**. These include inverted cash-to-card ratios, substantial cash deposits after business closure, repeated use of strawmen, missing annual accounts and tax filings, vague invoice descriptions and generic consultancy claims, rounded transaction amounts, a lack of staff or infrastructure despite high transaction volumes, frequent changes in registered office or management, commingling of personal and business funds, fictitious payrolls, unexplained property acquisitions, and high-throughput company accounts without a genuine commercial rationale.

CASERTA

EMPIRICAL RESULTS

7.1 Introduction

7.1.1 Background and context

The Campania Region in Southern Italy, which includes the Province and City of Caserta, is widely associated with various forms of **mafia-type criminality** referred to as 'Camorra'. Although often treated as a single phenomenon, these organisations differ considerably depending on the local contexts in which they emerged. Alongside smaller groups, typically organised around family networks and primarily engaged in drug dealing, extortion, and other predatory crimes, more structured and historically rooted organisations operate with far greater resources and criminal capacity. Over time, some of these groups have evolved into complex organisations pursuing a wide range of illicit activities and cooperating with other criminal actors through alliances or informal coalitions.

In many cases, these groups operate through strategies that resemble those of business enterprises, seeking to extend their influence beyond their traditional territories. The **infiltration of the legitimate economy** is often facilitated by complicit entrepreneurs and professionals who channel and reinvest illicit profits into legitimate economic activities, thereby distorting market competition. Within the Italian legal framework, the prevention of the criminal use of the legitimate economy is also pursued through administrative preventive measures adopted by the Prefectural authorities. Among the most significant instruments are **anti-mafia interdiction measures** (in Italian: *interdittive antimafia*), which aim to prevent companies suspected of mafia influence from maintaining economic relations with public administrations or participating in public procurement (Servizio Analisi Criminale, 2023). These measures are based on administrative assessments informed by data collected by LEAs and inter-agency investigative units, and are designed to disrupt potential channels through which organised crime may penetrate the legitimate economy.

These criminal groups have also developed a significant capacity to infiltrate local administrations: often, there is an interference by organised crime in **local authorities**, aimed at influencing decision-making processes related to the awarding of public contracts. By establishing complex networks of relationships with representatives of local administrations and businesses, criminal clans can secure major public contracts, either through direct awards to affiliated companies or via subcontracting arrangements. Often, such forms of infiltration are only partially visible, as companies formally operate within the legal economy while maintaining hidden links with criminal organisations.

Although these groups are strongly present in both **Naples and Caserta**, the two provinces are characterised by markedly different configurations of organised crime activity. On the one hand, Naples is a metropolitan setting marked by fragmented and polycentric Camorra groups, with multiple clans competing for territorial control at the neighbourhood level. By contrast, Caserta, particularly the Agro Aversano (historically known as Terra di Lavoro), has long been characterised by a more hierarchical and economically structured criminal structure with sustained political influence.[26] An example of such a group is the **'**Casalesi clan' (in Italian: *Clan dei Casalesi*), a major organised crime network in Campania originating from the City of Casal di Principe, situated in the Province of Caserta.

[26] The Province of Caserta, located in the Campania Region of Southern Italy, represents an important agricultural, commercial, and industrial area. With around 70,000 inhabitants, the City of Caserta is located 36 kilometres north of Naples.

Within the **'Casalesi clan'**, core bonds are traditionally based on familial connections, complemented by economic and political ties. During the 1990s, its main activities centred on the construction sector and the waste cycle, one of the most profitable sectors in the history of organised crime in Italy and largely controlled by the clan. Over time, however, the clan has adapted its *modus operandi* by operating less visibly: whereas previously a strongly hierarchical and centralised structure controlled both traditional criminal and economic activities, it now appears more fragmented and horizontal.[27] The clan operates simultaneously as an entrepreneurial, political, and managerial actor, following two coexisting and interconnected dimensions: one more visible and territorial, and another more entrepreneurial.

On the one hand, the **territorial dimension** concerns smaller and less structured groups managing 'traditional' criminal activities, such as drug trafficking and control over local dealing spots. Previously, these activities had partly been outsourced to other criminal groups, such as the Nigerian mafia, which the clan sought to confine to the territorial margins. Today, however, the Casalesi directly manage these activities once again, particularly younger individuals seeking to establish themselves on the territory. On the other hand, the **entrepreneurial dimension** is no longer based on a rigid chain of command but on a network of actors linked to the clan, often formally autonomous. Entrepreneurs, politicians, and professionals may form part of a stable network of cooperation without being formal members. Nonetheless, they play a key role in lending illicit activities a veneer of legality. Simultaneously, these actors benefit from the clan's support and networks through access to public contracts, protection, and political opportunities.

For the Casalesi clan, **infiltration of the legitimate economy** through complex corporate networks is not peripheral but central to its operational model.[28] For example, investigations conducted by the Financial Police (in Italian: *Guardi di Finanza*) in 2024 uncovered a criminal organisation composed of entrepreneurs based in the Province of Caserta, systematically engaged in tax fraud, (international) money laundering, and fictitious asset registration aimed at benefitting the Casalesi clan. Its scheme relied on valse invoicing through shell companies and complex financial transactions involving cryptocurrencies, waste management companies, and dairy-sector businesses (DIA, 2024). The investigation into this case demonstrated that the criminal use of the legitimate economy is a **systemic phenomenon** affecting multiple areas of economic activity, resulting in the consolidation of its territorial presence and criminal control over certain economic sectors.

[27] For a prolonged period, the Casalesi clan exercised direct **territorial control** through traditional violent and illicit activities, including feuds, murders, extortion and trafficking, alongside a sustained presence in the area and a strong entrepreneurial orientation. Following major trials and arrests in the 2000s, the formal leadership structure has changed, with several historical leaders imprisoned or deceased. However, the positions previously occupied by clan affiliates have often been maintained by descendants, associates, or strawmen. At the same time, the system of political-clientelist territorial control has proved more resilient than the clan's overtly coercive and military structures. As a result, the more visible violent component and reliance on intimidation had declined.

[28] In several municipalities within the Caserta area, **awareness** of the presence of criminal networks within the legal economy is widespread, including among business actors, educational personnel, and priests. Yet this rarely results in formal reporting, owing not only to fear of retaliation but also to limited trust in institutional protection. The resulting **normalisation** of criminal influence fosters passive acquiescence and reinforces the resilience of the system.

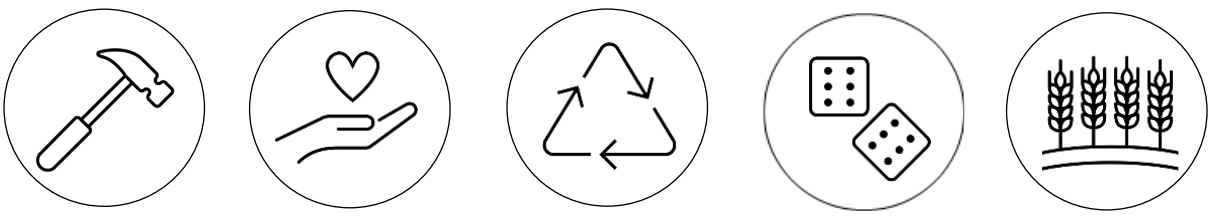
7.1.2 Data and methodology

The economic (sub)sectors were selected based on **institutional data and expert knowledge**. In particular, recent reports of the Anti-Mafia Investigative Department (in Italian: *Direzione Investigativa Antimafia*) (DIA) provided detailed information about anti-mafia interdiction measures across sectors, enabling the identification of those most vulnerable to organised crime infiltration (DIA, 2024). This empirical basis was complemented by insights from interviews and exchanges with practitioners and experts on the criminal use of the legitimate economy. Interviewees were selected based on their direct professional involvement in the cases or their expertise in organised crime in the local context. The sample comprised two senior public prosecutors with extensive experience in anti-mafia investigations, both directly involved in the cases analyses and affiliated with the DIA, and one investigative journalist (see Table 22; Annex 10.3). For the case studies, various documents – primarily pre-trial detention orders – were analysed, as they provide the most detailed account of the mechanisms of criminal use of the legitimate economy. These materials were obtained directly from the prosecutors involved.

7.1.3 Identification of vulnerable (sub)sectors

An initial mapping of vulnerable economic (sub)sectors was conducted using institutional data, particularly recent reports of the *Direzione Investigativa Antimafia* (DIA), which map anti-mafia interdiction measures across economic sectors (DIA, 2024). On this basis, five subsectors structurally exposed to organised crime infiltration in the Campania Region were identified: **real estate and construction**, **waste and environmental services**, **hydrocarbon trade and distribution**, **funeral services**, and the **illicit trade in antiquities**. This selection was guided by expected empirical availability and validated through exchanges with local prosecutors and practitioners (cf. *supra*).

However, the initially identified cases were revised, leading to a partial adjustment of the selected economic (sub)sectors. The research thus shifted from a structural risk assessment to a more case-oriented approach, resulting in the inclusion of three additional sectors: **social services, gambling and betting, and transport and agriculture.** This selection was based on empirical evidence documenting criminal involvement in these sectors, as well as on the availability of well-documented cases and access to judicial materials. The selected sectors are characterised by high capital intensity, significant cash flows, frequent interaction with public authorities through licensing or public procurement procedures, and regulatory vulnerabilities, making them particularly conducive to market distortion and corruption. Moreover, these sectors proved relevant in illustrating less visible forms of the criminal use of the legitimate economy, including the manipulation of public services, regulatory exploitation, and the integration of illicit capital into legitimate business activities.



Four specific cases were subsequently identified as clear, well-documented examples of criminal use of the legitimate economy, illustrating different forms of organised crime involvement in the legitimate economy: social services (Case Golf), waste management (Case Hotel), gambling and betting (Case India), and the agri-food sector (Case Juliett).[29] In all cases, the criminal use of the legitimate economy was carried out by the Casalesi clan, one of the most powerful Camorra organisations operating in the Campania Region (cf. *supra*). As a result, the financial profile applies across all four cases, albeit with sector-specific variations depending on the nature of the business activity involved. These cases were selected as they demonstrate the existence of structured systems of economic control: the network penetrated and coordinated several businesses simultaneously, confirming the systematic nature of its infiltration strategy. Although not recent, the cases offer detailed insights into the mechanisms of criminal use of the legitimate economy. Owing to their temporal distance, judicial proceedings have been completed, and extensive documentation has become available, allowing for a thorough reconstruction of key dynamics. Interviews with the prosecutors in charge further contextualised the cases and enabled an assessment of longer-term effects.

7.2 Case Golf: The Prince and the Ballot Scheme[30]

Case Golf concerns the infiltration and systematic exploitation of the **social services sector** in the municipality of Casal di Principe, located in the Province of Caserta, by members and associates of the Casalesi clan (see Annex 3.G). The investigation covered the period 2000-2011 and revealed a system of political-criminal collusion through which the clan exploited legitimate social services and publicly funded welfare programmes. Its aim was twofold: to **launder illicit proceeds**, and to consolidate territorial and political control by securing **electoral support**. The latter was linked to the so-called 'ballot scheme' (in Italian: *scheda ballerina*), through which control over voting was ensured. Moreover, by turning access to employment and social assistance into instruments of electoral control, the clan was able to distort democratic processes and reinforce its territorial dominance within the local environment.

7.3 Case Hotel: From Waste to Wealth

Case Hotel concerns the infiltration of companies operating in the **waste management sector** by members of the Casalesi clan (see Annex 3.H). These businesses serviced the interests of the criminal organisation by securing public contracts, laundering illicit capital, and controlling the sector through stable relationships with entrepreneurs, politicians, and public officials. The case is closely linked to the broader context known as 'Terra dei Fuochi', concerning illegal waste dumping and burning.[31] Following years of illicit trafficking and disposal of toxic waste, criminal groups progressively shifted towards the formal management of the urban waste cycle. In this respect, Case Hotel represented a pragmatic

[29] The cases were selected based on the availability of comprehensive documentation and access to prosecutors who conducted the financial investigations. Priority was given to cases at an advanced judicial stage, enabling detailed reconstruction of the *modus operandi*. Additional criteria included public relevance and their capacity to illustrate different modalities of the criminal use of the legitimate economy across sectors.

[30] The original Italian title of the case is "*Il Principe e la scheda ballerina*".

[31] In the **Case of Cannavacciuolo and others v. Italy**, the European Court of Human Rights (ECHR) found a violation of the right of life (Article 2 ECHR) due to the Italian authorities' prolonged failure to adequately assess and address the environmental and health risks linked to illegal waste dumping and burning in the 'Terra dei Fuochi' area (ECHR 30 January 2025, 51567/14, 39742/14, 74208/14, 21215/15). It held that the State had failed to fulfil its positive obligations to take timely and effective measures to protect the population, including risk assessment, information disclosure, and remediation.

turning point, marking the transition from overtly illegal practices to the **systematic infiltration** of the lawful waste management market.

7.4 Case India: Gambling as Governance

Case India concerns the infiltration of companies operating in formally lawful economic sectors, particularly the **gambling and betting** industries (see Annex 3.I). In 2014 and 2015, a faction of the Casalesi clan operated across two main domains: the management of slot machines, with a network of approximately four hundred units installed in the Agro Aversano area of the Province of Caserta, and the control of online betting platforms, thereby establishing a system of enforced distribution. Infiltration was achieved through control over ostensibly lawful businesses without formal ownership, using standard mechanisms of the criminal economy, in particular intimidation and territorial domination.

7.5 Case Juliett: Agri-Food Routes to Crime

Case Juliett concerned the control exercised by the Casalesi clan over the road **transport of fruit and vegetable products** destined for the Fondi wholesale market (in Italian: *MOF di Fondi*), a major agri-food distribution hub located in Lazio (see Annex 3.J). Transport routes connected Campania, Sicily, and the Fondi market. Through transport companies linked to the clan, the organisation established a system whereby transport operators and independent truck drivers could access the market only after obtaining authorisation from the clan. Control over the sector was maintained through intimidation, violence, obstruction of competitors, and agreements with other criminal organisations, including Sicilian mafia groups linked to the Corleonesi faction. The investigation further revealed that the same transport infrastructure was used to conceal and transport illicit goods, including drugs and weapons.

7.6 Financial investigations in Italy: key challenges and recommendations

7.6.1 Challenges in financial investigations in Italy

In Italy, financial investigations typically begin with the identification of anomalous signals that lack a plausible economic justification, such as disproportion between the costs incurred and the actual economic capacity of the business under scrutiny. The emergence of large commercial activities involving substantial investments, for example, raises the fundamental question of how such initiatives are financed and from which sources. Similarly, the opening of bars, pizzerias, or restaurants accompanied by disproportionately high investment, rental, or operating costs may constitute **red flags** warranting further investigation. From these initial signals, the investigation proceeds through a structured sequence of analytical steps. It begins with an examination of company balance sheets and suspicious transaction reports, followed by a more detailed analysis of the sectors in which the companies operate, including their suppliers and clients. This phase requires extensive cross-referencing of data from multiple databases held by different public authorities. Although technically demanding and time-consuming, this process is essential for mapping relationships between individuals and companies and identifying relevant connections. Once the financial flows have been reconstructed, the investigation focuses on identifying the sources of capital, the channels through which financing was provided, and the methods used to transfer funds. This makes it possible to

determine whether illicit funds have been injected into a business and to identify potential money laundering schemes or the reinvestment of criminal proceeds.

Among the most effective practices in investigating criminal financial networks, the systematic use of **wiretaps** stands out not merely as a means of obtaining evidence of specific criminal acts, but also as a tool for mapping the broader economic architecture of a criminal organisation. Intercepted conversations can reveal who pays whom, who makes commitments to whom, which contracts are involved, and how the wider network of economic relationships is structured. Used in this way, wiretaps can serve as a source of economic intelligence. Another effective practice is the systematic analysis of public procurement data. Cross-referencing awarded contracts with information on relationships between entrepreneurs and individuals under investigation, as well as tracing subcontracting chains, can reveal patterns of infiltration that might otherwise remain undetected. However, this approach requires analytical expertise that is not always available within prosecutorial offices or contracting authorities.

Against this background, several challenges in conducting financial investigations in Italy can be identified. Firstly, financial investigations often **take years to complete**, during which assets may be transferred, companies may change ownership, and capital may be moved abroad. By the time confiscation is ordered, the assets remaining are therefore frequently worth less than those available at the outset. This temporal gap between the initiation of an investigation and the implementation of asset recovery measures provides criminal organisations with an opportunity to anticipate and circumvent judicial intervention.

A closely related challenge is the **fragmentation of information sources**. Wiretap data are managed by the prosecution, banking data are held by financial institutions, property ownership records are distributed across municipal registries, company information is held by the Chambers of Commerce, and fiscal data are held by the tax authority. Integrating these sources requires not only time and specialised expertise, but also sustained coordination between institutions that do not always communicate effectively. The necessary information often exists, but is not identified or connected across separate data sources. Specialist units such as the DIA and the Carabinieri's Investigative Nucleus (in Italian: *Nuclei Investigativi*) have undertaken substantial work in this area. However, available resources have consistently fallen short of the complexity of the financial structures requiring analysis.

These challenges are compounded by insufficient investment in **technology, artificial intelligence** (AI), and **database interconnection**, as well as inadequate training of judicial police in financial investigation techniques, which differ fundamentally from traditional investigative methods. The use of cash presents an additional challenge, as higher thresholds for cash transactions create greater opportunities to circumvent financial controls. Tax evasion remains characterised by regulatory interventions that are fragmented and inconsistent.

A further, often underacknowledged gap concerns the **role of compliant professionals**, including accountants, lawyers, and notaries, who can facilitate the concealment of financial flows through the creation of opaque corporate structures, the preparation of sham contracts, and the opening of accounts in foreign jurisdictions. Without such professional support, complex money laundering schemes would be significantly more difficult to implement. Yet their role and responsibility remain insufficiently recognised and prosecuted within the Italian judicial system, with enforcement efforts focused predominantly on criminal organisations rather than on the enabling infrastructure that facilitates their financial operations.

The **limited media and political visibility** of financial investigations constitute a further weakness. Unlike traditional operations, such investigations do not necessarily produce immediately tangible outcomes, such as arrests or high-profile seizures, and are therefore less likely to attract public attention or institutional prioritisation. This dynamic risks creating a systematic bias in the allocation of investigative and prosecutorial resources, favouring interventions that generate visible short-term outcomes over those aimed at dismantling criminal financial structures at their root. Moreover, financial investigations often target individuals from economic and professional elites whose integration into legitimate social and economic networks can make them more difficult to detect and prosecute.

Finally, **international judicial cooperation**, despite the progress made in recent years, continues to present significant challenges. Criminal organisations systematically exploit opaque jurisdictions and complex legal structures by transferring economic activities to foreign foundations or companies in other jurisdictions. This can make it extremely difficult to identify beneficial ownership and reconstruct financial flows. In some cases, jurisdictions may also have limited incentives to cooperate effectively, as they benefit from incoming capital without bearing the social costs associated with the underlying criminal activity. At the European level, the absence of full harmonisation of legal frameworks governing economic and financial crime further complicates and can delay cooperation. Differences between legal systems, varying thresholds of criminal relevance, and divergent rules governing access to financial data can hinder the rapid and effective exchange of information. Major criminal organisations operate across the European single market and beyond, investing in real estate, commercial activities, and corporate holdings across multiple jurisdictions. A financial investigation that stops at regional or national borders therefore remains incomplete. Effectively countering such organisations requires not only strong bilateral and multilateral judicial cooperation but also sustained political commitment to establishing and maintaining it.

7.6.2 Recommendations for improving financial investigations in Italy

Recommendation 1 – Improve integration of databases

Although investigative authorities already have access to the relevant data on companies, land registries, fiscal records, and banking flows, these sources remain fragmented across institutions that do not communicate effectively in real time. Enabling investigators to cross-reference this information simultaneously is therefore not primarily a technological challenge, as the necessary technology already exists. Rather, it is a matter of political will and institutional governance. In parallel, a coherent normative framework is required to establish consistent rules governing access to and the sharing of financial data across jurisdictions and between authorities.

Recommendation 2 – Strengthen specialised human and technological capacity

Investment in specialised human and technological capacity must be significantly increased. Financial investigations require professional profiles and competencies that differ qualitatively from those employed in traditional criminal investigations, yet these capabilities are not uniformly available across prosecutorial offices and investigative units. While highly skilled professionals are present within anti-mafia prosecutorial structures, they remain insufficient in number relative to the volume and complexity of the work. As organised crime continues to invest in increasingly sophisticated financial structures, the state must strengthen its capacity to identify and dismantle them. This requires not only recruiting and training specialised personnel, but also deploying advanced technological tools, including artificial intelligence and integrated analytical systems, and providing judicial police with adequate and continuous training in financial investigation methods.

Recommendation 3 – Strengthen early warning mechanisms for public procurement

On the preventive side, the systematic deployment of early warning mechanisms in public procurement should be prioritised. Where a municipality repeatedly awards contracts to the same company, tender specifications consistently favour the same operators, or award prices are systematically anomalous, such patterns should automatically trigger an alert to the prefectures and anti-corruption authorities.

Recommendation 4 – Address the cultural dimension of organised crime

Finally, a cultural obstacle must be addressed. Criminal organisations frequently bring economic resources into territories where legitimate investment is scarce and, in some contexts, are perceived as drivers of local development. However, when their presence becomes structural, it distorts the economic fabric, undermines public institutions, and weakens democratic processes. In territories where financial flows are heavily influenced by organised crime, public decision-making itself becomes vulnerable to criminal influence. It is therefore essential to foster broader awareness that wealth generated through criminal activity does not constitute sustainable development, but rather contributes to economic distortion and the progressive erosion of the rule of law.

7.7 Summary of research findings: Caserta

The phenomenon of organised crime in the Province of Caserta must first be understood by distinguishing between mafia-type organisations and other forms of organised criminality. As several scholars have observed, Italian mafia organisations cannot be reduced to ordinary criminal enterprises primarily oriented towards profit (Paoli, 2003, 2004). Unlike criminal groups that operate mainly through illegal market transactions, **mafia-type organisations** exercise territorial, social, economic, and political power. Their strength lies not only in their involvement in illicit activities, but also in their capacity to regulate economic relations, infiltrate public institutions, influence democratic processes, and establish systems of social mediation and control within specific territories.

Within this broader category, **the Camorra** itself presents important peculiarities. Unlike the relatively hierarchical and centralised structure historically associated with Sicilian Cosa Nostra, the Camorra has traditionally developed as a more fragmented and polycentric system, composed of autonomous clans and alliances between factions. This fragmentation provides considerable adaptive resilience. In the Province of Caserta, however, and particularly in relation to the Casalesi clan, the analysis reveals a stable model of organised crime capable of combining territorial control, entrepreneurial capacity, political influence, and long-term financial investment strategies. In this context, criminal use of the

legitimate economy constitutes one of the central mechanisms through which criminal power is exercised.

The examined case studies, spanning the social services sector, waste management, gambling and betting, and agri-food sectors, reveal a **consistent operational logic** through which the Casalesi clan systematically combined criminal violence, entrepreneurial capacity, political influence, and financial reinvestment to consolidate territorial control and generate long-term economic power. Organised crime thus operated simultaneously as a criminal, economic, and managerial actor, capable of shaping markets, influencing public decision-making, controlling employment opportunities, and conditioning access to public resources. In this context, the legal economy became one of the primary arenas through which criminal power was exercised and normalised.

Several overarching findings emerge from the comparison of the different cases. First, criminal use of the legal economy appears particularly effective in **sectors** characterised by high levels of public funding, administrative discretion, weak transparency mechanisms, or intensive cash circulation. Public procurement, outsourced public services, regulated sectors, and activities involving close interaction with local administrations proved especially vulnerable to criminal penetration. Second, organised crime increasingly relies on **hybrid networks** comprising not only traditional criminal actors, but also entrepreneurs, accountants, professionals, local politicians, and other facilitators operating within the so-called 'grey zone' between legality and illegality. These systems depend on the ability to exploit formally lawful structures and procedures while concealing criminal objectives behind apparently legitimate economic activities.

Third, the analysed cases confirm the progressive **evolution of organised crime** from predominantly violent and predatory forms of control toward models based on economic infiltration, corruption, market monopolisation, and institutional influence. Although violence remains present, both explicitly and implicitly, it increasingly functions as a background resource supporting systems that rely on financial capacity, political connections, and entrepreneurial strategies. From this perspective, organised crime in Caserta demonstrates considerable adaptive capacity, continuously reshaping its methods in response to economic opportunities, regulatory changes, and institutional vulnerabilities.

Furthermore, the case studies point to broader trends affecting the territory. One evident tendency is the **diversification** of criminal investments across multiple sectors of the legal economy, which reduces reliance on traditional illicit markets alone. Another trend is the increasing **sophistication** of financial and corporate structures used to conceal ownership, fragment responsibilities, and facilitate the movement of capital across jurisdictions. The growing transnational dimension of financial flows further complicates investigative activities and reinforces the need for stronger European and international cooperation mechanisms.

At the same time, the cases highlight the persistent **territorial vulnerabilities** that continue to facilitate criminal use. Economic fragility, limited employment opportunities, weak administrative capacity in some municipalities, and dependence on informal systems of mediation create conditions in which organised crime can present itself as a provider of resources, employment, or stability. This dynamic contributes to the normalisation of criminal influence within local economic and social relations, and risks the progressive erosion of democratic trust and institutional legitimacy.

From a preventive perspective, the analysis confirms the importance of **administrative anti-mafia instruments**, particularly anti-mafia interdiction measures, in limiting the access of criminally infiltrated companies to public contracts and economic relations with public authorities. Effective prevention requires a broader strategy capable of combining financial investigation, institutional transparency, technological innovation, social awareness, and long-term investment in the territory. Furthermore, strengthening **financial investigations** and improving the integration of databases across judicial, fiscal, banking, and administrative authorities should be prioritised. Greater investment in specialised personnel, advanced analytical technologies, and continuous training for investigative authorities is equally essential. In addition, enhanced monitoring of public procurement procedures and early warning systems capable of identifying anomalous contracting patterns would further strengthen preventive capacity. Finally, effective prevention also requires a broader **cultural and social response**. Strengthening institutional trust, democratic participation, transparency, social cohesion, and sustainable local development is essential in reducing the conditions that allow criminal economic power to become socially tolerated or perceived as inevitable.

FRANKFURT

EMPIRICAL RESULTS

8.1 Introduction

8.1.1 Background and context

As is commonly assumed to be the case internationally, **organised crime in Germany** in many ways appears to be intertwined with the legal economy. Criminal actors are believed to systematically utilise legal businesses to facilitate and conceal criminal activities, including the laundering of illicit proceeds (Europol, 2024b; Savona & Riccardi, 2018). However, while the infiltration of the legal economy in Germany has long been perceived as a great threat (Fernstädt, 1987; Klima et al., 2009), research on the subject is scarce. Early studies on organised crime in Germany since the 1970s have focused on the structures and *modus operandi* of criminal groups, with relatively little emphasis on criminal influence on the legal economy.

The only empirical study focussing specifically on the infiltration of the legal economy in Germany was conducted within the framework of the MORE project (Savona & Riccardi, 2018). Verena Zoppei, who authored the country report for Germany, noted that the country is particularly prone to **criminal infiltration of the legal economy**, primarily due to risk factors such as high cash intensity, the absence of effective cash-payment limits, financial secrecy, and complex ownership structures. Her analysis further identified wholesale and retail trade, transportation and storage, and the construction and real estate industries as the sectors most frequently affected (ibid., 2018, p. 114). Key vulnerabilities include the shadow economy (despite its relatively limited size by international standards), extensive cash usage, limited corporate transparency – for instance, through links to offshore and high-risk jurisdictions – as well as loopholes in the anti-money laundering framework (ibid., pp. 118-121).

Since at least the 1970s, **Frankfurt am Main** (hereafter, Frankfurt) and the surrounding Rhine-Main region, which extends into neighbouring federal states, have been regarded as a centre of organised crime in Germany (Gemmer, 1983, 1992).[32] The region's perceived attractiveness to criminal actors may be partly linked to Frankfurt's role as a major transportation and communication hub within Germany and Europe. The city is situated at the intersection of the A5 and A3 interstate highways, linking major German industrial centres with the Netherlands, France, and Switzerland to the West, and with Austria and the Balkans to the South-East. This also provides criminal actors operating from Frankfurt with relatively easy access to several strategically significant locations. For example, the ports of Antwerp, Rotterdam, and Hamburg are all located within a five-hour driving radius. Similarly, Frankfurt is home to one of the busiest railway stations and one of Europe's busiest airports in terms of passenger traffic, as well as the continent's largest airport by cargo volume. In addition, Frankfurt hosts Europe's largest and one of the world's leading Internet Exchange Points (IXPs).

[32] In 2019, the Rhine-Main region had a population of approximately 5.8 million people. Around 28% of the residents lived in the region's core cities, while the remaining 72% resided in surrounding districts and independent cities. Frankfurt alone currently accounts for nearly 13% of the region's total population (Trippen et al., 2021). In 2024, approximately 473,000 employed individuals commuted to Frankfurt from their places of residence (Hessisches Statistisches Landesamt, 2025).

Frankfurt also holds a central position in **business and finance**. The Frankfurt metropolitan region ranks among the top three regions in Germany by Gross Value Added (GVA) (Statista, n.d.). Through the Frankfurt Stock Exchange, the city provides the largest trading venue in Germany and one of the world's leading electronic trading platforms. It is also the seat of the European Central Bank and hosts numerous financial institutions, including Deutsche Bank. Nevertheless, socio-economic polarisation is increasing, with growing risks of structural disadvantage among children and adolescents affected by, or at risk of, poverty. For example, average monthly gross earnings are substantially higher in Frankfurt's central districts than in peripheral urban areas (Stadt Frankfurt am Main, n.d.). The geographical and economic characteristics of the Frankfurt region place it along major **drug trafficking routes**, providing easy access to illicit drugs while also supporting a high-spending market for substances such as cocaine.

In its **approach to crime control**, the State of Hesse stands out in at least two respects. It was the first federal state in Germany to deploy the controversial 'Palantir' data integration and analysis software, which has been credited with significant investigative successes since its introduction in 2017 (Iskandar, 2025). Furthermore, since summer 2025, public prosecutors, police officers, and tax investigators have operated under one roof to conduct financial investigations into organised crime cases. The Hessian Joint Financial Investigation Centre (in German: *Gemeinsames Finanzermittlungszentrum*; GFEZ) is a permanent joint investigative body comprising the Public Prosecutor's Office in Frankfurt, the Hessian State Criminal Police Office, and the Regional Finance Directorate in Frankfurt. Adopting a follow-the-money approach, the GFEZ aims to uncover illicit activities, trace illegally acquired assets, and identify offender structures (Hessisches Ministerium der Finanzen, 2025).

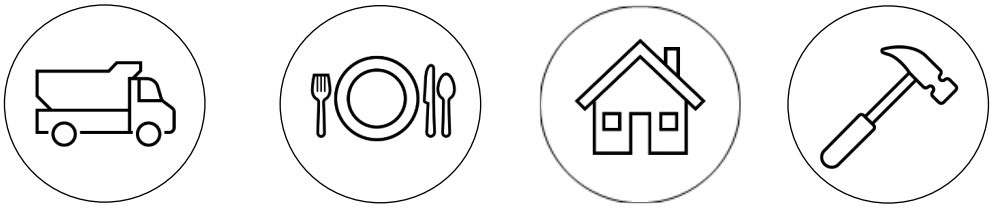
8.1.2 Data and methodology

Business sectors and specific cases of criminal use of the legitimate economy were identified through an initial round of thirteen **expert interviews** with investigators from the police and customs services. These included organised crime investigators, analysts from a specialised unit providing business expertise in criminal investigations, financial investigators, and investigators from a customs service unit targeting undeclared labour. Additional information on specific cases was obtained through six follow-up interviews with selected participants from the first round. Access to judicial case files was not available for analysis.

The interviews provided valuable insights into offender structures and *modi operandi*, including the use of businesses for money laundering and other criminal activities. However, only **limited information** was obtained on criminal influence over specific legitimate businesses. This was partly due to concerns that disclosing overly detailed information could assist criminal actors. A further explanation may be that German criminal law does not explicitly address the infiltration of legitimate businesses, while applicable anti-money laundering provisions often carry insufficient penalties to become a primary focus in organised crime investigations. Of the 647 organised crime cases investigated in Germany in 2024, only 32 involved money laundering as the primary offence (Bundeskriminalamt, 2025).

8.1.3 Identification of vulnerable (sub)sectors

The following economic (sub)sectors emerged from the interviews as the most prevalent in Frankfurt, and/or the best documented, with regard to the use of legitimate businesses in the context of criminal activities, including money laundering: **cargo handling and logistics** (including warehousing and storage), **hospitality** (restaurants), **real estate**, and **construction**. These sectors were also identified as particularly relevant in the findings of the MORE project (Savona & Riccardi, 2018).



These subsectors were selected for two additional reasons. First, the cases enable an analysis of how legitimate businesses are used for cocaine and cannabis trafficking, which represent the most common types of criminal activity among groups monitored by LEAs. Second, they illustrate three distinct levels of criminal use of legitimate businesses: infiltration at the level of lower-level employees in Case Kilo, infiltration at the management level in Case Lima, and businesses under the legal ownership and control of criminals in Case Mike.

8.2 Case Kilo: The Corrupt Cargo Chain

Case Kilo concerns a criminal network involved in **drug trafficking**, comprising an estimated thirty to forty actors engaged in the smuggling – through Frankfurt Airport – and local distribution of hundreds of kilograms of cannabis and cocaine in a rural part of the Rhine-Main area (see Annex 4.K). The drugs, arriving from outside the EU through Frankfurt Airport, were retrieved with the assistance of corrupt employees of an international logistics company.

8.3 Case Lima: Hidden Hubs, Hidden Hauls

Case Lima concerns a criminal network involved in **drug trafficking**, primarily in cannabis (see Annex 4.L). Drug consignments amounting to several tonnes were transported from other European countries to the Frankfurt area by road, using legitimate haulage companies that had been contracted for transportation services. Subsequently, a local legitimate logistics business operating under corrupt management was used as a distribution hub.

8.4 Case Mike: Dining with Dealers

Case Mike concerns a criminal network involved in a drug trafficking operation that exploited the legitimate hospitality sector, notably through the use of a restaurant and a bar (see Annex 4.M). The network members were involved in the distribution of cocaine and cannabis sourced from Spain, Belgium, and the Netherlands, with consignments reaching the double- and triple-digit kilogram range. Operating from the Frankfurt area, the network supplied recipients in various European countries, while a portion of the drugs was also distributed on the domestic market. Drug proceeds were primarily laundered abroad.

8.5 Financial investigations in Germany: key challenges and recommendations

Interviewees acknowledged that recent legislative and institutional innovations in Germany are having positive effects. At the same time, they pointed to various shortcomings. Observations on good practices, as well as recommendations for further improvement, concern the following topics:

Topic 1 – Cash use

In international comparison, cash remains relatively important in Germany, both culturally and economically, despite a steady decline in cash-based transactions, which accounted for approximately 50% of all transactions in 2023 (Deutsche Bundesbank, 2025). The prevalence of cash transactions is regarded as a major facilitating factor for introducing illicit proceeds into the legitimate economy (Bundeskriminalamt, 2025). Legal limits on cash-based transactions have recently been introduced, and cash payments for the purchase of real estate are now subject to an absolute ban. Most interviewees considered the absence of an **upper limit on cash payments** in Germany to be a major financial and structural problem. They similarly regard the EUR 10,000 threshold for mandatory identification in cash transactions as too high. Moreover, they argued that these regulations are not enforced strictly enough. According to one interviewee, these vulnerabilities contribute to Germany's continued appearance as a 'money-laundering haven'.

Topic 2 – Quantitative and qualitative capacities

In assessing staffing levels, a difference in perception emerges between those working exclusively as criminal investigators and those (also) involved in financial data analysis. The latter reported relatively few grounds for concern. For example, the launch of the Hessian Joint Financial Investigation Centre (GFEZ), which brings together resources to facilitate more effective financial investigations, was viewed positively. The **financial analysts** interviewed reported excellent access to tax data, economic databases, and police files. They are also closely integrated to the EU-wide system for reporting suspicious transactions and generally succeed in obtaining bank account information. Challenges arise primarily when data from banks and payment service providers are unavailable, for example because financial services have been outsourced. Moreover, the use of cryptocurrencies presents a particular challenge. Although transactions on public blockchains remain visible and can often be traced, the underlying transaction data are inherently pseudonymous, making attribution difficult. These challenges are further exacerbated by chain-hopping and the use of privacy coins.

By contrast, interviewees not involved in financial analysis reported challenges related to **limited staffing**, noting that there are insufficient financial investigators within the police and the FIU. However, the challenge is not solely one of staffing. Interviewees pointed out that criminal investigators often lack the time and expertise required to fully understand schemes designed to obscure the flow of illicit funds. They therefore call for additional financial analysts and for these specialists to be involved from the earliest stages of criminal investigations.

Moreover, a distinction emerges between the **centre and the periphery**. While Frankfurt has a considerable number of financial investigators, auditors/accountants (in German: *Wirtschaftsprüfer*), and asset recovery specialists (in German: *Vermögensabschöpfer*), local authorities in rural areas face shortages in these areas. According to interviewees, criminal groups are also aware of these disparities and tend to operate in peripheral areas rather than establishing themselves in Frankfurt.

Topic 3 – Data protection

Several interviewees indicated that data protection in Germany is stricter than in many other EU countries. It is a central area of concern among the investigators interviewed. They welcomed a recent court decision permitting the use of AI-based software to combine heterogenous data, citing its usefulness in resolving cases (Bäuerle et al., 2025). Hesse was the first of currently only three federal states to use 'Palantir' software, which is viewed unanimously as a tool that can be used in highly effective and productive ways. The use of software from this particular provider is not considered essential; rather, similar AI-based tools are regarded as indispensable.

Topic 4 – 'Mini-reversal of the burden of proof'

Although a provision partially shifting the burden of proof in asset forfeiture was introduced in 2017, interviewees considered it insufficient. One respondent referred to the provision allowing the seizure of assets of unclear origin where there is a gross disproportion between the value of the asset and the lawful income as a 'mini-reversal of the burden of proof' (in German: *Mini-Beweislastumkehr*). Interviewees advocated a reversal of the burden of proof similar to those in Italy, Albania, or Spain, where seizure is easier to execute and the affected party is required to demonstrate the legitimate origin of the assets.

Topic 5 – Banks and payment service providers

According to several respondents, banks should be subject to stricter obligations to scrutinise assets under anti-money laundering legislation. In financial investigations, they report having to work with data in which relevant information is scattered across different institutions and stored in incompatible formats. This reportedly slows down investigations, makes cross-referencing difficult, and consumes considerable investigative time. Respondents would therefore prefer standardised and streamlined digital data, enabling investigators to keep pace with funds that can be moved by criminals quickly and with just a few clicks.

Due to the international nature of the financial system, funds can move across borders within seconds, while access to the corresponding financial information is constrained by legal safeguards, rules, and regulations. Requests for information sharing must pass through domestic procedures and mutual legal assistance channels, increasing the time required for relevant intelligence to reach investigators. Moreover, funds may be channelled through countries that are unwilling or unable to cooperate effectively with requests for legal assistance. In this regard, interviewees emphasised the need for a **global information system** based on a uniform data structure. They also called for stricter cooperation obligations for payment service providers of all kinds, including blockchain service providers and cryptocurrency exchanges.

8.6 Summary of research findings: Frankfurt

Frankfurt's position as one of Germany's most important transport, logistics, and financial centres creates a concentration of opportunities that can be leveraged by criminal actors. First, a central finding emerging across the German cases is the pivotal role of the **logistics and transport sector**. The scale and complexity of Frankfurt's logistics sector, including its airport operations, cargo handling facilities, and extensive road connections, create an environment in which illicit flows can be concealed within large volumes of legitimate commercial activity. Both Case Kilo and Case Lima demonstrate how legitimate businesses can be integrated into criminal operations, particularly drug trafficking. Criminal actors involved in the cases primarily embedded illicit activities within existing commercial supply chains to conceal the transportation, storage, and distribution of drugs.

Moreover, the cases highlight the importance of **social networks** and **personal connections** in facilitating the criminal use of legitimate businesses. In both Case Kilo and Case Lima, insiders were recruited through existing social contacts, while Case Mike demonstrated the importance of family-based structures in organising criminal activities and business operations. These observations suggest that the social embeddedness of criminal actors remains a key enabling factor and that vulnerabilities can also arise from broader social and relational dynamics.

The findings also demonstrate that legitimate businesses may serve purposes beyond the direct facilitation of criminal operations. Case Mike, for example, illustrates how a legitimate business can function simultaneously as a source of legitimacy, a status symbol, and a networking platform. The restaurant provided employment opportunities, enhanced the public image of network members, and offered opportunities to establish social relationships with influential individuals. This suggests that **strategic and social objectives** are often important complementary goals alongside profit generation.

Furthermore, the financial dimension of the analysis highlighted the continuing importance of **cash-based transactions** in organised crime. Interviewees consistently identified cash as a key facilitator of both criminal activity and money laundering, with the persistence of cash-intensive economic practices in Germany regarded as a significant vulnerability. At the same time, criminal proceeds were not retained exclusively in cash. Investments in real estate, luxury assets, vehicles, boats, and cryptocurrencies were repeatedly identified as means of storing or transferring illicit profits. Overall, the findings point to a diversified approach to the management and concealment of criminal proceeds, combining traditional methods with emerging financial technologies.

Finally, the interviews revealed a growing recognition of the importance of **financial investigations** and intelligence-led policing, while simultaneously highlighting several challenges. Recent innovations, including the establishment of the Hessian Joint Financial Investigation Centre (GFEZ) and the use of advanced data analysis tools, were generally perceived as positive developments. Nevertheless, interviewees identified persistent obstacles relating to staffing shortages, access to financial information, international cooperation, and data-sharing restrictions.

MADRID

EMPIRICAL RESULTS

9.1 Introduction

9.1.1 Background and context

The crime landscape in Madrid is characterised by the presence of **various high-risk criminal networks** and their deep infiltration into the region's economic, social, and administrative fabric. Madrid hosts several prominent criminal entities, including Spanish family clans (primarily engaged in drug trafficking), Russian mafias, Latin American cartels, and Nigerian and Chinese networks, as well as groups specialised in fraud affecting significant public interest, including corruption-related crimes. These criminal networks are primarily involved in drug trafficking (notably cocaine and hashish), tax and excise fraud, corruption, human trafficking, and cybercrime. These groups demonstrate considerable resilience to police interventions, sophisticated money-laundering capabilities, and continuous adaptation of their *modus operandi* to circumvent anti-fraud measures. They also show notable flexibility in responding to legislative reforms and in evading countermeasures introduced by the authorities to control crime.

The primary objective of these criminal networks is **financial gain**, with infiltration serving as a key strategy to expand and secure their profit base, enabling control over territories and societal sectors. Building on this objective, they actively seek to infiltrate public administration, the private sector, and civil society. In public administration, corruption has been identified in urban planning, development, and public procurement processes, involving senior officials and city councillors. In the private sector, these criminal groups embed themselves in company management, turning legitimate businesses into vehicles for criminal activity. In civil society, attempts have been made to influence neighbourhood associations, professional bodies, and NGOs to obtain legitimacy, social acceptance, and influence. However, economic infiltration and **money laundering** remain the most pervasive and harmful forms of criminal infiltration in Madrid. Money laundering linked solely to drug trafficking is estimated to amount to approximately EUR 500 million annually in the region.

Several **characteristics of Madrid** appear to facilitate the criminal use of the legitimate economy. First, its strategic geographic position and well-developed transport infrastructure (including highways, rail connections, and an international airport) make it an attractive logistical hub for criminal activities. The dry port in Coslada provides rail links to major Spanish seaports such as Algeciras, Barcelona, Bilbao, and Valencia. In addition, extensive coastlines offer opportunities for the illicit movement of people and goods. Moreover, socioeconomic factors contribute significantly to the enabling environment for criminal enterprises in Madrid. The extensive shadow economy, the presence of vulnerable immigrant populations, and demand for drugs and low-cost consumer goods create opportunities for criminal exploitation. Impunity and the uncritical social acceptance of illicit products and services further facilitate and reinforce sophisticated criminal activity. Finally, LEAs face significant constraints arising from limited technological and human resources, as well as insufficient interoperability. Criminal organisations exploit these weaknesses by employing sophisticated countermeasures to evade surveillance and conceal illicit financial activities. Despite progress at EU level, judicial cooperation remains insufficient, slow, and often ineffective. The low asset confiscation rate (estimated at below 2%) highlights the substantial financial resources available to criminal groups, enabling them to sustain and expand their infrastructures and reinvest in further criminal activities.

9.1.2 Data and methodology

The identification of the economic (sub)sectors most attractive to criminal networks in Spain was based on **triangulation** of semi-structured interviews, written responses, and supporting documentary materials provided by key law enforcement, regulatory, and private-sector stakeholders. These interlocutors represent the institutional ecosystem with statutory responsibilities in relation to organised crime, money laundering, fiscal fraud, and market infiltration. Although fieldwork in Spain was conducted across Madrid, Barcelona, and Andalusia, involving bodies with both national jurisdiction and regional operational roles, this report focusses on the City of Madrid.[33]

Respondents were selected on the basis of their **operational knowledge** of criminal network behaviour and their statutory roles in detecting or preventing criminal use of the legitimate economy, including investigative practices, financial intelligence, tax fraud detection, customs surveillance, and real estate market monitoring. The research drew on contributions from law enforcement agencies (*Cuerpo Nacional de Policía* and *Guardia Civil*), financial intelligence units (SEPBLAC; Spain's FIU), tax and customs authorities (AEAT and DAVA), intelligence services (CITCO), and private-sector actors, particularly within the real estate sector. The analysis draws on interviews with these respondents, as well as written notes, internal reports shared by agencies, and academic materials.[34] By incorporating multiple **institutional perspectives**, the aim was to reduce bias and enhance analytical validity. Law enforcement emphasised operational intelligence and criminal network structures, while tax and customs agencies highlighted administrative fraud patterns. In addition, FIU experts provided insight into money laundering techniques and suspicious financial flows, while private-sector respondents outlined market vulnerabilities exploited by organised crime.

9.1.3 Critical remarks

The analysis of criminal use of the legitimate economy in Madrid highlights a range of structural, operational, and methodological **challenges** that must be considered when interpreting the findings. These stem from divergent institutional perspectives, the under-detection of criminal infiltration, weaknesses in regulatory, administrative, and judicial frameworks, and the growing sophistication of criminal networks. Collectively, these factors create a criminological landscape in which organised crime appears to retain strategic advantages over state authorities, both in Spain and internationally.

First, **methodological limitations** must be acknowledged when interpreting the findings of this case study. Although the analysis focuses on Madrid, the research process revealed that the scale and sophistication of criminal infiltration of the legal economy is considerably more pronounced in Andalusia. As a result, the evidence collected for Madrid provides only a partial representation of the national situation and is necessarily more limited than the insights that could have been obtained had Andalusia fallen within the scope of the study. An additional limitation stems from the lack of direct access to judicial case files that have not yet been adjudicated, restricting the extent to which ongoing criminal activities can be systematically assessed. Nevertheless, the operational expertise and insights

[33] The selected cases are not representative or generalisable. They provide context-specific illustrations of recurring patterns within the legal economy of Madrid, rather than comprehensive evidence of criminal infiltration across Spain.

[34] All interviews were conducted with informed consent, and respondents were anonymised by institutional role rather than personal identity. Sensitive operational information has been excluded or generalised to avoid compromising investigations, national security intelligence, or ongoing law enforcement operations. Recordings and transcripts were produced where permitted. Otherwise, detailed written notes were taken.

provided through expert interviews partially mitigate this constraint and offer valuable perspectives on emerging trends and investigative challenges. However, the intelligence derived from these interviews should be regarded as a non-exhaustive reflection of investigative realities rather than a comprehensive account of criminal infiltration.

A second challenge concerns the **heterogeneity of institutional perspectives** and the fragmentation of intelligence flows. Spanish institutions assess criminal infiltration through distinct operational and legal lenses. Law enforcement agencies such as the *Cuerpo Nacional de Policía*, the *Guardia Civil*, and CITCO tend to focus on hierarchical criminal networks, drug trafficking routes, and associated violence. Tax and customs authorities (AEAT and DAVA) prioritise VAT fraud, excise offences, hydrocarbons, and complex commercial schemes. SEPBLAC examines financial flows, beneficial ownership concealment, and systemic money laundering operations, while private-sector respondents, particularly in real estate, emphasise price distortions, opaque ownership structures, and cash-intensive transactions. These differing perspectives reflect variations in institutional mandates, access to information, and investigative priorities rather than substantive disagreement. However, they create analytical blind spots and hinder the development of a coherent national assessment. In some cases, municipal or sectoral perceptions of criminal infiltration exceed what can be evidenced through judicial or financial investigations.

Another major challenge is the structural **under-detection of criminal infiltration**, a concern consistently raised by law enforcement, regulatory authorities, local administrations, and private-sector stakeholders. The scale of illicit financial flows appears to far exceed the number of cases formally detected and investigated. Criminal networks employ increasingly sophisticated methods to conceal assets, obscure ownership structures, and move funds across jurisdictions, while asset recovery rates remain low. These dynamics limit the visibility of criminal activity and complicate enforcement efforts. As a result, detected cases represent only a partial picture of the phenomenon. The adaptability, resilience, and international embeddedness of organised crime suggest that the complete dismantling of major criminal networks is becoming progressively more difficult to achieve.

Additional concerns arise from administrative and regulatory **blind spots**. Madrid provides criminal networks with multiple entry points into legal and administrative systems. Vulnerabilities in urban planning, procurement, and licensing have already resulted in corruption cases involving public officials. Opaque corporate structures, the routine use of frontmen, rapid company formation, and inadequate verification of beneficial ownership are systematically exploited. Industrial estates, particularly Cobo Calleja, function as semi-autonomous commercial enclaves where illicit and semi-illicit activities flourish, often in cash-intensive sectors subject to limited regulatory oversight. These activities are closely linked to illegal imports, tax fraud, corruption, product counterfeiting, and labour exploitation. Such blind spots hinder the detection of irregularities and facilitate criminal control, market distortion, and influence over local institutions. Consequently, law enforcement is undermined, facilitating the concealment of illicit activities and criminal liability.

9.1.4 Identification of vulnerable (sub)sectors

Based on the available evidence, expert interviews, and financial intelligence indicators, several **economic (sub)sectors** in Madrid appear particularly vulnerable to criminal use. These vulnerabilities stem from factors such as cash intensity, high transaction volumes, regulatory gaps, limited oversight, technical complexity, and opportunities for money laundering and concealment. The sectors include real estate, retail trade, import-export, logistics, and professional, scientific, and technical activities.

- The **real estate sector** is consistently identified as the principal vehicle for money laundering by both domestic and international criminal networks. Key vulnerabilities include large cash-based transactions and property undervaluation to conceal the origin of funds; the use of industrial warehouses for drug storage, illicit imports, counterfeit goods distribution, and labour exploitation; luxury property investments as stable stores of value; and the involvement of intermediaries, notaries, and law firms in creating layered corporate structures that obscure beneficial ownership. Criminal networks may also influence property prices, particularly in municipalities on the periphery of Madrid. Real estate further facilitates territorial control by enabling the establishment of semi-protected operational areas.

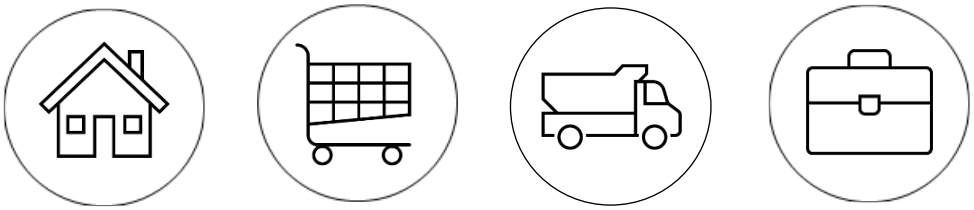
- The **retail trade sector** is highly vulnerable to criminal infiltration due to its cash intensity, fragmented oversight, and the convergence of licit and illicit supply chains. Several subsectors are particularly exposed. First, the *hydrocarbons and energy sectors* exhibit a particularly high level of vulnerability due to complex VAT carousel and excise fraud schemes in fuel distribution, evidenced by significantly below-market fuel prices at numerous gas stations across Madrid and confirmed persistent interference documented by the authorities. Second, the *vehicle sector*, including new and second-hand dealerships, is exploited through invoice manipulation, falsified mileage records, and fictitious export schemes. It facilitates cross-border VAT and excise evasion, and involves high-end vehicles used as a means of payment and drug delivery.

  Third, *alcohol and tobacco markets* are attractive to organised crime due to sustained risks of smuggling, counterfeiting, diversion of excise goods, and under-declaration of sales. Transnational organised crime structures use Spain as both a destination and transit point. The retail trade in cannabidiol (CBD) and cannabis-derived products has also expanded rapidly in Madrid, creating regulatory gaps exploited for money laundering, tax fraud, and irregular imports. Certain networks engage in fraudulent CBD extraction for pharmaceutical purposes and chemical manipulation, linking the sector to broader trafficking operations. Moreover, *electronics and mobile phone retail*, particularly in high-volume commercial areas, is associated with smuggling, unauthorised imports and VAT fraud. Its cash intensity and high turnover of easily resold goods facilitate the integration of undeclared cash into the legal economy. Lastly, *gold-buying businesses* are particularly vulnerable due to gold's high value-to-weight ratio, ease of transport, and difficult provenance tracing, enabling criminal networks to convert illicit proceeds into an asset that can be stored, melted, transformed, or transferred with relative anonymity.

- Madrid's **logistics** ecosystem (including airport cargo, the dry port of Coslada, and industrial corridors) provides strategic infrastructure exploited by criminal networks. Key vulnerabilities include high cargo volumes that complicate inspection, subcontracting chains that reduce accountability and transparency, the movement of counterfeit goods, illicit drugs or undeclared merchandise through mixed consignments, and corruption attempts targeting operational insiders such as drivers, handlers, and planners. Available data indicate that infiltration typically occurs at employee level rather than at corporate ownership level.

  Particularly, the **import-export sector** is a high-risk vector for smuggling, counterfeiting, money laundering, and tax fraud. This includes misdeclared imports from China (with Cobo Calleja as a central hub), the use of shell companies to conceal ownership and financial flows, labour exploitation in warehousing and logistics, and fraudulent documentation enabling over- and under-invoicing typical of TBML. It is also associated with the trafficking of toxic, hazardous, or environmentally harmful products, and constitutes a key operational channel for transnational criminal networks across Europe, Africa, and Latin America.

- **Professional, scientific, and technical activities** include lawyers, notaries, consultants, accountants, and corporate service providers. The sector is vulnerable to misuse for business incorporation, contract drafting, and asset transfers, either unwittingly or through complicity in providing crime-as-a-service to criminal networks, as well as for the fabrication of documentation, facilitation of international transfers, and concealment of beneficial ownership. Several Madrid cases indicate the involvement of paid legal professionals embedded within criminal networks.



Ultimately, **three cases** were selected, demonstrating how high-risk criminal networks become structurally embedded in legal markets, exploit regulatory and institutional weaknesses, and maintain transnational connections that significantly complicate investigation and prosecution. These case studies illustrate key criminological features of criminal networks in Madrid, including the convergence of multiple crime types within single organisations, the strategic use of legal companies and professional services, the exploitation of high-risk sectors (cf. *supra*), and reliance on transnational infrastructures and international financial circuits.

9.2 Case November: The Cartel's Cannabis Network

Case November concerns an international drug trafficking network with direct links to the Mexican 'Sinaloa Cartel' (see Annex 5.N). In Spain, the network operated through a family-based clan that provided criminal services to the organisation, particularly in cocaine and hashish trafficking, money laundering, violence, and the corruption of public officials, including advisers and accountants, as well as attempted corruption of police officers. The case illustrates the nexus between drug trafficking, the use of cash-intensive businesses such as petrol stations, the acquisition of farmland for large-scale tetrahydrocannabinol (THC) production, and **cannabis-related markets**. The group's activities also involved the fraudulent extraction and processing of CBD-derived products in laboratories located in Portugal and Switzerland, demonstrating a high degree of technical and financial sophistication. The network generated substantial volumes of cash, which were laundered through a multinational network of ostensibly legitimate companies. It also relied on violence, extortion, and intimidation, both internally and externally, while accumulating a significant portfolio of luxury properties, vehicles, investment gold, and corporate assets across multiple jurisdictions. Despite extensive law enforcement efforts, the network has not been fully dismantled, highlighting its resilience and transnational reach.

9.3 Case Oscar: Chinese Connections and Criminal Cashflows

Case Oscar concerns a highly sophisticated **Asian criminal network** operating primarily from the Cobo Calleja industrial area in Fuenlabrada (Madrid), a key hub for the illegal importation and distribution of Chinese goods in Spain and the wider EU (see Annex 5.O). The network specialised in large-scale TBML, fiscal fraud, and underground banking, using a corporate structure of approximately forty companies to disguise substantial illicit cash flows.[35] It laundered over EUR 3 million per week by combining large-scale **smuggling** from China with the scale of **counterfeit and undeclared goods** across several EU Member States. The structure relied on a complex corporate network to generate undeclared cash, and investigations also identified alleged labour abuses. The organisation further functioned as a financial facilitator for third-party criminal groups, enabling cross-border value transfer and supporting drug trafficking, human trafficking, and prostitution networks. Given its cross-border scope, the case required extensive international cooperation and led to the creation of an Operational Task Force coordinated by Europol and Eurojust, involving law enforcement officers from multiple jurisdictions.

[35] However, it should be noted that the investigation into Case Oscar resulted only in the partial dismantling of one of the businesses operating under the broader criminal scheme described, which is widely applied in the physical area under study, as well as in other locations at national and international level.

9.4 Case Papa: Banking on Fame

Case Papa concerns a highly complex, hierarchical, transnational criminal network engaged in large-scale fraud, tax evasion, drug trafficking, and money laundering (see Annex 5.P). Since at least 2017, the network has used more than seven hundred shell companies to fraudulently secure over EUR 50 million in financing. The network systematically deceived banks, investors, and other entities through shell companies, the acquisition of firms with strong credit profiles, and the fabrication of commercial documentation. Illicit proceeds from **fraud and drug trafficking** were laundered through complex financial and commercial schemes, including fraudulent hydrocarbon trading. In addition to laundering its own criminal proceeds, the network provided high-volume laundering services to third-party narcotrafficking organisations (i.e. crime-as-a-service). The case further demonstrates extensive use of document forgery and tax fraud, reliance on specialised facilitators with expertise in banking and financial markets, and a significant capacity to evade law enforcement. This included the involvement of a complicit notary and the use of transport companies to support operations. The organisation also displayed a capacity for intimidation and violence, including the hiring of Colombian contract killers.

9.5 Summary of research findings: Madrid

The analysis suggests that criminal networks in Madrid are structurally embedded within legitimate economic sectors, with the criminal use of legitimate businesses emerging as a **core strategic component** of organised crime. In many instances, however, the distinction between legal and illegal economic activities is deliberately blurred, as networks increasingly rely on complex forms of economic infiltration that closely resemble legitimate business activity.

A first overarching finding concerns the centrality of **money laundering** and financial reinvestment. Across all three case studies, criminal organisations demonstrated a strong capacity to transform illicit profits into apparently legitimate wealth through the systematic use of businesses, real estate, corporate structures, and financial schemes. In particular, real estate, luxury assets, front companies, and complex corporate arrangements emerged as preferred vehicles for laundering and reinvesting criminal proceeds.

A second recurring pattern is the extensive use of legitimate companies as **multifunctional criminal tools**. Businesses rarely served a single criminal purpose. Instead, legitimate enterprises simultaneously fulfilled operational, logistical, financial, and reputational functions. In Case November, companies operating in the real estate, hospitality, automotive, and pharmaceutical sectors were used to conceal illicit cultivation, facilitate money laundering, provide logistical support, and create a veneer of legitimacy. Similarly, in Case Oscar, a network of import-export companies supported customs fraud, trade-based money laundering, and illicit cross-border value transfers. In Case Papa, hundreds of shell companies enabled large-scale fraud and laundering activities. Taken together, these findings suggest that legitimate businesses are increasingly being used as part of broader criminal operations, rather than simply as vehicles for money laundering.

Moreover, the findings demonstrate a significant **convergence between crime types**. The analysed networks were rarely specialised in a single criminal activity. Rather, drug trafficking, money laundering, fiscal fraud, VAT fraud, customs fraud, corruption, and illicit financial services frequently coexisted within the same organisational structures. This diversification increases organisational resilience and reduces dependence on any single revenue stream. It also complicates law enforcement responses, as investigations often span multiple legal domains, sectors, and jurisdictions.

Furthermore, the cases highlight the significance of **professional facilitators** and institutional insiders, including lawyers, notaries, financial advisors, bank employees, and corrupt public officials (e.g., police officers). These actors provided specialised expertise and facilitated access to sensitive information, administrative advantages, protection from scrutiny, and enhanced operational security. Corruption consequently took multiple forms across the cases, ranging from the involvement of public officials to the complicity of private-sector professionals. Relatedly, the analysis indicates the exploitation of administrative, regulatory, and institutional **vulnerabilities**. The cases demonstrate how weaknesses in oversight, information-sharing, company registration, customs controls, and financial regulation can create opportunities for criminal exploitation.

Another prominent trend is the importance of **transnationality** and international connectivity. None of the criminal networks operated exclusively within Madrid or even within Spain. Instead, they were embedded in extensive international infrastructures spanning Europe, Latin America, Asia, and beyond. The network linked to the Sinaloa Cartel in Case November relied on financial, logistical, and criminal connections across Mexico, Portugal, Switzerland, Colombia, Argentina, and the United States. The network in Case Oscar exploited international supply chains linking Spain, China, Greece, Hungary, and Dubai, while Case Papa involved financial flows extending to Panama, Switzerland, and the Maldives. Madrid's position as a major transport, logistics, and commercial hub appears to facilitate these transnational activities. The findings therefore indicate that local manifestations of organised crime cannot be understood separately from global criminal markets and international financial systems.

Finally, the cases highlight the continued importance of **cash-based economies**, with cash remaining central to all three networks, whether in the form of drug proceeds, undeclared commercial revenues, corruption payments, or large-scale value transfers. At the same time, the cases reveal increasingly sophisticated methods for converting, moving, and concealing cash through commercial transactions, underground banking systems, front companies, luxury assets, and international financial infrastructures. This further illustrates the adaptability of criminal networks.

PARIS

EMPIRICAL RESULTS

10.1 Introduction

10.1.1 Background and context

In France, the definition of organised crime draws on the UN Palermo Convention (2000). Following Europol's approach, it characterises a criminal organisation or network as a collective form of criminality, devoid of political motivation – unlike terrorism – that seeks to influence the lawful sphere through corruption and money laundering. Under French law, however, the notion of a **criminal organisation** has never been accorded an autonomous definition. A notable development has emerged in the context of the so-called 'narcotrafic' law, which seeks to introduce one by defining a criminal organisation as any conspiracy structured and organised among its members for the purpose of preparing one or more felonies and, where applicable, one or more offences listed in subparagraphs 1° to 10°, 12° to 14° and 17° of Article 706-73 of the Code of Criminal Procedure. To date, organised crime continues to be addressed primarily through substantive offences under the Criminal Code, including drug trafficking, money laundering, financial fraud, cybercrime, and certain forms of corruption. The French authorities regard such networks as an increasing threat to the legal economy and institutions.

One of the central issues is the **criminal use of the legal economy**, which relies on money laundering mechanisms designed to reintroduce illicit funds into ostensibly legitimate economic activity. The sectors most exposed in France include real estate, luxury goods, the restaurant sector, and company domiciliation services. While international laundering – through the purchase of luxury watches, vehicles, gold, or real estate abroad – appears widespread, it has a more limited impact on the domestic economy than so-called 'proximity laundering', which refers to laundering methods within traffickers' immediate environment. It typically involves the use of cash to fund everyday consumption such as cash-based payments for goods and services to integrate illicit proceeds into the legal economy. It also includes real estate transactions in France, as well as the acquisition of small businesses which can be used both to inject illicit funds and to facilitate underreported turnover and undeclared work. 'Cash-for-cargo' settlements are also used, whereby cash in France is used to pay for goods intended for export (e.g., textiles, phone cards), which are then shipped abroad and subsequently resold on local markets.

10.1.2 Data and methodology

The analysis of the French cases is based on a combination of **primary and secondary sources**, aimed at capturing both the structural dimensions of organised crime and its concrete impact on the legal economy of the Île-de-France region.

- Primary data collection relied on two complementary sources. Frist, **semi-structured interviews** were conducted with key informants holding direct professional knowledge of the cases, namely a financial investigator with experience in asset recovery and money laundering detection and an investigative journalist who reported on Case Sierra in real time. These interviews provided contextual interpretation and operational detail not available from documentary sources alone.

Second, and most substantially, the study drew on **judicial case files** from the Paris Specialised Interregional Court (JIRS; *Jurisdictions Interrégionales Spécialisées*), including synthesis reports, rogatory commission reports, financial investigation records, and a final judgement. These materials, produced by multiple law enforcement units, constituted the primary evidence basis and covered the period 2015-2024, encompassing the full investigative process from preliminary inquiries and telephone intercepts to judicially ordered investigative measures and final reporting.[36]

- **Secondary sources** complemented the primary material. Institutional data from Strategic Intelligence and Analysis Service on Organised Crime (SIRASCO) and the Central Office for the Repression of Major Financial Crime (OCRGDF) provided sectoral and typological context on money-laundering methods prevalent in the region. Statistical and economic data on the subsectors analysed (i.e., taxi licences, construction, luxury retail, and automotive) were drawn from the National Institute of Statistics and Economic Studies (INSEE) and the National Observatory of Private Passenger Transport (ONT3P).

10.1.3 Critical remarks

Several methodological constraints should be acknowledged. **Access to judicial files** was necessarily partial, as some investigative lines remained open at the time of writing, limiting the completeness of the financial reconstructions. Certain quantitative figures – such as monthly withdrawal estimates in Case Romeo – are averages derived from multi-account analysis rather than verified accounting data, as explicitly noted in the source material. Finally, the lack of access to foreign judicial databases (in Spain, Lebanon, Pakistan, and the Netherlands) constrained verification of the networks' transnational dimension, particularly regarding assets and corporate structures held abroad.

10.1.4 Identification of vulnerable (sub)sectors[37]

The selection of 'vulnerable' (sub)sectors was based on two converging criteria: their recurrent identification by specialised services (SIRASCO; OCRGDF; GIR) as channels for proximity money laundering, particularly in cash-intensive activities such as passenger transport, construction, security, and cleaning; and the concrete manifestation of such vulnerabilities in the judicial case under review. The selected cases concern luxury retail outlets (Case Quebec), the construction sector (Case Romeo), and the private passenger transport sector (Case Sierra).





[36] The following law enforcement units were involved in this investigation: the *Groupe Interministériel de Recherches de l'Essonne* (GIR 91), the *Section de Recherches de Versailles*, the *Office Central pour la Répression de l'Immigration Irrégulière et de l'Emploi d'Étrangers sans Titre* (OCRIEST), and the *Office Central de Répression de la Grande Délinquance Financière* (OCRGDF).

[37] The Paris City Report did not identify five vulnerable (sub)sectors. Accordingly, this section discusses only the sectors addressed in the examined cases.

First, Île-de-France has the highest concentration of **luxury retail outlets** in France. In the watchmaking and jewellery sector, approximately 17% of employees were based in the Paris region (over 2,800 individuals), mainly in city-centre brand stores and department stores. The sector employed nearly 16,800 people nationally, with annual turnover estimated at EUR 5.6 to 6 million. The region is also a major hub for used-car sales, with around 715,000 vehicles sold in Île-de-France between 2023 and 2024. The 'grand touring and luxury' segment was particularly significant, with strong demand for German brands, including Porsche, BMW, and Audi.

Second, the **construction sector** constitutes a major economic pillar of the Val-d'Oise, particularly in dense urban areas such as Argenteuil. Nationally, it accounts for approximately 8.3% of private-sector salaried employment. The local business landscape comprised over 90% very small enterprises (VSEs), offering a wide range of small-scale legal structures. Proximity to Paris and large-scale urban renewal projects make the department a zone of intense construction activity, facilitating the rapid establishment and high turnover of new companies. Analysis of the proceedings revealed a systemic and structural exploitation of the construction sector by criminal networks.

Third, the taxi subsector was selected as it combined three risk factors: cash-based operations, a high-value asset subject to limited oversight, and an administrative loophole in its transfer. The region's level of economic development and commercial weight make it one of the wealthiest in Europe, generating strong demand for **private passenger transport**. According to the National Observatory of Private Passenger Transport, France had in 2021 approximately 61,500 taxis and 40,000 ride-hailing vehicles (in French: *Véhicule de Tourisme avec Chauffeur*) (VTC), with 21,000 new authorisations issued. Taxi supply is closely correlated with population density: French regions averaged nine taxis per 10,000 inhabitants, compared with seventeen in Île-de-France. With nearly 19,960 inhabitants per km² in the inner city, the capital remains highly attractive for the sector despite a dense public transport network. In 2025, the price of a Paris taxi licence ranged between EUR 160,000 and EUR 200,000 (compared with around EUR 100,000 in other regions), with only the city of Nice recording higher prices.

10.2 Case Quebec: The Luxury Laundering Loop

Case Quebec concerns a vast international **money-laundering network** linked to drug trafficking (see Annex 6.Q). The network functioned as a covert financial services platform specialising in the laundering of proceeds of cocaine trafficking on behalf of Colombian cartels. Cash collectors operated covertly across Europe (in France, Germany, Belgium, Italy, Spain, and the Netherlands), aggregating illicit proceeds. These funds were then laundered through the **purchase of luxury goods** such as high-end vehicles and prestige watches, before being transferred to Lebanon or settled via hawala-based settlement systems to facilitate onward flows to cartels in Colombia.

10.3 Case Romeo: Pakistani Forgery and Money Laundering

Case Romeo concerns a criminal network specialising in the supply of **forged administrative documents** from various Schengen countries, including passports, identity cards, residence permits, and driving licences, as well as Pakistani passports (see Annex 6.R). Manufactured in Turkey, Greece, and Pakistan, these documents were smuggled into France via express courier services. The network was led by two brothers of Pakistani nationality, who operated primarily through a company domiciled in Eaubonne (Val-d'Oise). They oversaw the network's administrative and commercial activities, directed financial flows, and issued instructions relating exclusively to deposits and withdrawals. Distribution of the forged documents and execution of the brothers' financial instructions were managed by a key intermediary. The network also involved several coordinators and associates responsible for, *inter alia*, fund transfers and document forgery. To dismantle the network, authorities employed interceptions of telecommunications and extensive urban CCTV surveillance. The investigation ultimately resulted in a request to open a judicial investigation into facilitating irregular residence through an organised criminal group, repeated forgery and use of forged documents, and aggravated money laundering.

10.4 Case Sierra: Taxi Licence Laundering Scheme

Case Sierra illustrates a classic *modus operandi*, namely the integration of proceeds from drug trafficking into a legitimate commercial activity (see Annex 6.S). Although seemingly rudimentary and not reliant on a dedicated laundering network, it fell within the scope of self-laundering in a common, multifaceted and heterogeneous form, involving various accomplices (e.g., accountants, frontmen, and unwilling sellers). In 2024, the press reported the dismantling of a drug-trafficking network in the Île-de-France region. The case was notable for the identification of a laundering scheme based on the **purchase and leasing of taxi licences**. With regard to this case, several schemes were observed, including settlement mechanisms, opaque financing, and localised laundering. It was further characterised by practices that had long remained outside the compliance radar, as well as a specific vulnerability, namely the absence of any verification of the origin of funds at the point of licence transfer.

10.5 Summary of research findings: Paris

The findings from Paris and the wider Île-de-France region indicate that criminal networks use the legal economy as an **enabling environment** for concealing, converting, and reintegrating criminal proceeds. Across the three cases, they strategically exploited structural vulnerabilities within legitimate markets to facilitate money laundering, generate apparently lawful income streams, and sustain their longer-term activities.

A recurring pattern concerns the exploitation of **cash-intensive** and asset-based sectors. The selected sectors, namely luxury retail, construction, and private passenger transport, display characteristics that may increase their attractiveness to criminal actors. These include significant financial turnover and opportunities to absorb substantial amounts of cash. In this context, **money laundering** emerged as a central activity across all three cases. The examined networks relied on a range of laundering mechanisms, from cash-based methods to more complex transnational financial arrangements. In Case Quebec, luxury watches, vehicles, and other high-end goods were used to convert and transfer proceeds from international cocaine trafficking across jurisdictions. In Case Romeo, construction companies facilitated the circulation and concealment of funds linked to document fraud and irregular employment. In Case Sierra, taxi licences provided a means of channelling proceeds derived from drug trafficking into seemingly legitimate commercial activities.

Moreover, the analysis highlighted the **transnational character** of the criminal infrastructures involved. None of the investigated networks operated solely within France. Instead, they formed part of wider international systems connecting actors and activities across Europe, Latin America, the Middle East, North Africa, and other regions. Case Quebec involved Colombian cocaine cartels and Lebanese financial brokers, while Case Romeo involved document-production and distribution networks extending to Pakistan, Turkey, Greece, Italy, and other European countries. Case Sierra similarly combined drug-trafficking routes connecting France, Morocco, Spain, and the Netherlands. The findings therefore suggest that the criminal use of the legal economy in France is embedded within broader transnational criminal networks and financial flows.

The findings further demonstrate the continued relevance of **cash-based criminal economies**. Despite increasing digitisation within the legitimate economy, cash remained an important medium across the three cases. Even where criminal proceeds were subsequently invested in legitimate assets or businesses, the initial stages of the laundering process often involved the physical collection, transportation, conversion, and redistribution of cash. Informal value-transfer systems, including hawala-type arrangements, could further facilitate the movement of funds outside conventional financial channels.

Finally, the cases underline the considerable **investigative challenges** associated with detecting and dismantling economic infiltration in France. In all three cases, the criminal use of the legal economy remained difficult to identify until specialised financial investigations, intelligence collection, undercover measures, communications intercepts, or international cooperation helped expose the underlying activities.

SOFIA

EMPIRICAL RESULTS

11.1 Introduction

11.1.1 Background and context

The use of legitimate businesses by criminal networks in Bulgaria is acknowledged in the recent National Risk Assessment of Money Laundering, where it is ranked among the main money laundering risk areas, particularly in sectors such as trade, construction, real estate, metal scrap trading, and the production, import, and trade of food, petroleum products, pharmaceuticals, and medical equipment (Държавна агенция Национална сигурност, 2022). Sofia is the largest and most populous city in Bulgaria, concentrating more than one third of the country's economic activity and registered enterprises (Столичната общинска агенция за приватизация и инвестиции, 2025). The anonymity afforded by a major urban centre is often instrumental in evading law enforcement scrutiny, while the laundering of criminal proceeds serves to legitimise illicit gains. In this respect, the **organised crime environment** in Sofia closely resembles that of other major cities throughout the EU.

Primarily due to its geographical position, Bulgaria functions as a source, transit point, and destination for migrant smuggling, trafficking in human beings (THB), drug trafficking, and the movement of various illicit goods, including cash, firearms, cigarettes, and fuel. A significant share of these illicit flows passes through the capital, Sofia, where criminal networks exploit the city's economic scale and institutional density. Networks operating in Bulgaria, and in particular in Sofia, are also involved in MTIC fraud, EU funds fraud, and various **predatory criminal activities**, including real estate fraud and predatory lending. The latter, often conducted through ostensibly legitimate payday loan companies, is particularly concerning and frequently accompanied by debt entrapment, coercion, extortion, and physical violence. It expands rapidly alongside the growth of non-bank financial institutions offering short-term consumer credit following the country's accession to the EU and the rapid digitalisation of the sector. Despite tighter regulation, this activity continued to thrive and remained the primary driver of violence in Sofia, exceeding even drug trafficking and distribution (CSD, 2020). Moreover, investigative evidence indicates that the country, together with Romania, is increasingly used by Italian mafia groups to establish shell companies, launder illicit proceeds, and relocate businesses to evade asset seizure (Savona & Riccardi, 2018).

Bulgaria's and Sofia's large shadow economies continue to facilitate criminal infiltration, with **cash** remaining widely used: approximately 54% of all daily retail payments were still made in cash in 2024, highlighting persistent vulnerabilities to illicit financial flows (Denislova & Minkov, 2025). Although the Limitation of Cash Payments Act (2011; effective from 2016) introduced a EUR 5,113 limit on cash purchases, enforcement challenges remain. Furthermore, accession to the Eurozone in early 2026 was also preceded by a marked increase in cash deposits by both individuals and companies, which rose by 13.6% in 2025, alongside a 6.5% annual increase in real estate investment (Bulgarian National Bank, 2025b). Sofia, in particular, recorded its highest number of **real estate transactions** since 2008, with an average annual increase of 15.2% compared with 2024 (Capital, 2026; Dimitrova & Toteva, 2026). Notably, 45% of purchases were financed entirely with buyers' own funds. The transition from the Bulgarian lev (BGN) to the euro required the withdrawal of approximately BGN 29 billion in cash from circulation (Bulgarian National Bank, 2025a). Given the scale and political sensitivity of the process, this inevitably placed considerable pressure on regulatory oversight and heightened risks of money

laundering. The most recent estimates indicated that illicit financial outflows amounted to 3.55% of GDP, while illicit inflows reached 4.81% of GDP (Georgiev et al., 2023).

11.1.2 Data and methodology

The identification of vulnerable (sub)sectors and the analysis of the Bulgarian case studies were based on a series of **structured interviews** with key informants regarding Sofia's criminal networks, their activities, and related issues. Interviewees primarily included law enforcement officers from the Sofia Directorate for Interior Affairs, the City Prosecution Office, and the Ministry of the Interior's Directorate-General Office for Combating Organised Crime. In addition, representatives of Sofia Municipality were consulted to identify the legitimate business sectors they considered most vulnerable to criminal exploitation in Sofia. Municipal authorities have no formal responsibility for policing or public security, as law enforcement is directly subordinate to the Ministry of the Interior. In total, fifteen participants were interviewed. The interviews were conducted in person and typically lasted 60-90 minutes. Upon request, the City Prosecution Office also provided eight indictments concerning criminal networks operating in Sofia. Two **case files** were selected on the basis that they contained sufficient evidence of the use of legitimate businesses to facilitate criminal activities.

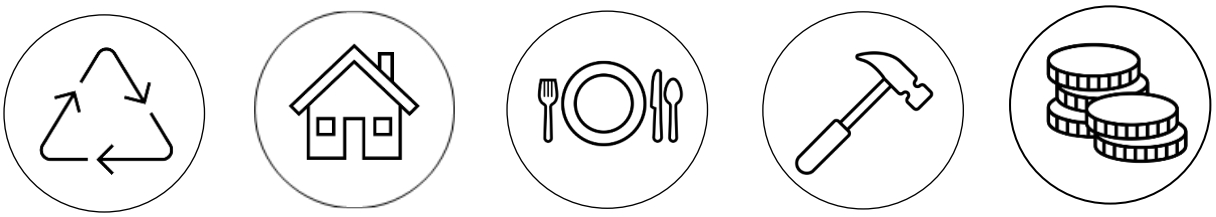
11.1.3 Critical remarks

Several methodological limitations should be acknowledged. The principal challenge concerned the **level of detail** that law enforcement officers were willing to disclose about specific investigations in Sofia, reflecting the sensitivity of ongoing and past criminal cases. Although access was ultimately granted to eight case files by the City Prosecutor's Office, only two were selected for in-depth analysis, as they provided sufficient evidence of the use of legitimate businesses by criminal networks. These cases concerned the nightlife economy and drug distribution, and the non-bank financial services sector, involving drug distribution and predatory lending. Although the waste management sector was also identified as particularly vulnerable, the third case study was reconstructed through in-depth interviews and an extensive review of media sources, as no relevant prosecution files were available.

The indictments obtained also revealed certain limitations regarding the level of detail. The case files focused primarily on the predicate offences, whilst considerably less attention was paid to the **financial aspects** of the criminal operations. It is common practice within the Bulgarian Prosecutor's Office to initiate separate money laundering investigations, which are assigned to a different Public Prosecutor from the one handling the predicate offence. Furthermore, the Public Prosecutor's Office's case management system does not allow for the identification or cross-referencing of related money laundering investigations. Although the Public Prosecutor's Office has been designated as one of the national Asset Recovery Offices in Bulgaria, most asset recovery activities are carried out by the Commission for Illegal Asset Forfeiture (CIAF). Asset tracing activities carried out by CIAF are initiated following notification from the Public Prosecutor's Office that pre-trial proceedings have been launched. However, pre-trial proceedings and asset recovery procedures then proceed in parallel, with no systematic exchange of information between the two institutions. This **institutional fragmentation**, together with the separation of investigations into distinct operational silos, hinders the identification and consolidation of all related case files, thereby limiting a comprehensive understanding of both the *modus operandi* and the financial architecture of individual criminal networks.

11.1.4 Identification of vulnerable (sub)sectors

Many subsectors of Bulgaria's legal economy, and particularly in Sofia, are affected by criminal use. As sectors ranging from construction to car dealerships are affected, very few economic sectors in Bulgaria are unexposed to this phenomenon. In Bulgaria, the shadow economy, widespread use of cash, and legislative loopholes create fertile conditions for these activities, particularly following economic crises that increase demand for illicit financing. Initial desk research identified five economic (sub)sectors particularly vulnerable to criminal use: **waste collection** and disposal, **real estate** (fraud), **nightlife economy** (drug distribution), **construction** (money laundering), and **payday lending** (drug distribution, extortion, and loansharking). Of these (sub)sectors, three have been selected for in-depth case study research.



11.2 Case Tango: The Hammers

Case Tango concerns a criminal network, known as 'The Hammers', which operated in Sofia and systematically infiltrated and exploited legitimate businesses, particularly a company in the **nightlife and entertainment sector** (see Annex 7.T). Many network members had links to the 'Levski Sofia Zapad' football supporters' faction and maintained a hierarchical structure comprising more than thirty members involved in large-scale drug trafficking and distribution (cocaine, amphetamines, cannabis, heroin), as well as violence, extortion, robberies, and intimidation. The company under control of the network managed some of the largest nightclubs in Sofia. They were used as distribution hubs for narcotics and provided access to large and affluent customer bases, limited oversight, and opportunities to launder illicit proceeds through legitimate income. High-ranking network members owned or controlled various businesses in the hospitality sector, thereby creating favourable conditions for criminal use and enabling the laundering of illegal proceeds.

Overall, Case Tango illustrates the structured exploitation of the nightlife sector to facilitate **drug distribution**, **launder illicit proceeds**, and reinforce the network's broader operations. The network exhibited clear functional differentiation, including leaders, regional managers, dealers, warehouse staff, cashiers, and a 'punishment unit' (referred to as 'The Hammers'). Members used code words, controlled regional territories, and handled proceeds through a well-defined weekly accounting system. From 2008 onwards, law enforcement authorities intervened, leading to indictments, arrests, and the seizure of drugs, money, and digital evidence, although the network's leader managed to evade extradition. Judicial proceedings continued until 2020.

11.3 Case Uniform: Quick Credits

Case Uniform concerns a criminal network operating in Sofia that infiltrated the **non-bank financial lending sector** through a franchise office operating under the "Quick Credits" brand (see Annex 7.U).[38] The network set up a formally registered company that provided quick consumer loans, serving as a façade for systematic criminal activities combining illegal lending, extortion, violence, and money laundering. The franchise offices therefore operated as dual-use structures, simultaneously carrying out legitimate lending activities while also serving as operational hubs for criminal enforcement. By exploiting regulatory loopholes in the payday loan market, the network targeted financially vulnerable individuals with high-interest loans enforced through intimidation and escalating violence.

The criminal network employed a clearly **structured escalation model** for debt collection, with initial repayment reminders followed by persistent harassment, threats, and physical visits to the debtors' homes. When these measures proved ineffective, the network escalated to systematic violence, including beatings, abduction, psychological abuse, and threats of rape, arson, or murder. The consistency of methods across multiple offices indicates coordinated operational practices aimed at maximising financial gain while discouraging victim cooperation with law enforcement. Overall, Case Uniform illustrates the systematic criminal exploitation of the non-bank lending sector to generate illicit profits, launder proceeds, and sustain organised criminal activities under the guise of legitimate economic operations.

11.4 Case Victor: Lords of the Dust

Case Victor concerns a large-scale **illegal construction waste dumping scheme** operating within Sofia's construction sector, commonly referred to as the "Lords of the Dust" network (see Annex 7.V). At its centre was a construction-sector entrepreneur who owned several legally registered companies providing excavation, transport, and waste disposal services. Through these legitimate business structures, he coordinated a parallel system for disposing excavated soil and construction waste outside the authorised municipal framework. The network's *modus operandi* followed a recurring cycle embedded within legitimate economic activity: waste was collected under valid commercial contracts and documented as destined for lawful disposal but was diverted during transport to illegal dumping sites. False administrative justifications, such as land levelling or terrain stabilisation, were used to conceal these activities. Sustained by Sofia's construction boom, weak enforcement, and legislative gaps limiting criminal liability, the scheme operated for several years, causing significant environmental damage, market distortion, and a loss of public trust in municipal oversight.

[38] "Quick Credits" is a pseudonym used to refer to the brand. Any resemblance to actual, existing names is unintended and purely coincidental.

11.5 Financial investigations in Bulgaria: key challenges and recommendations

11.5.1 Challenges in financial investigations in Bulgaria

The three cases analysed reveal systemic deficiencies in financial investigation practices that have enabled criminal networks to operate with impunity for extended periods. These deficiencies have facilitated the activities of the criminal networks in each case, allowing them to cause significant harm to Sofia and its citizens, while generating substantial illicit profits. Interviews with law enforcement officials and analysis of case files indicate that the financial dimensions of criminal operations receive **insufficient attention** during investigations, limiting both prosecutorial success and asset recovery.

The most significant structural impediment is the **functional fragmentation** between predicate offence investigations and money laundering inquiries within Bulgaria's prosecutorial system. Separate prosecutors handle each track, without an integrated case management system to identify related financial investigations. In addition, financial investigations concerning asset tracing and seizure fall under the jurisdiction of Bulgaria's Commission for Illegal Asset Forfeiture (CIAF). This is one of several entities involved in the process, alongside the National Investigation Service, the financial investigation unit of the General Directorate for Combatting Organised Crime (GDCOC), and the Financial Intelligence Directorate (FID) within the State Agency for National Security (SANS) (FID-SANS), among others. As a result, evidence of financial flows uncovered during investigations into drug trafficking, extortion, or environmental crime remains disconnected from parallel efforts to trace and recovered laundered proceeds. The files examined focused almost entirely on the predicate offences (i.e., violence, extortion, and illegal dumping), while financial elements were treated as **secondary considerations**, if considered at all.

Furthermore, interviews revealed a **reluctance** to pursue complex financial inquiries requiring forensic accounting expertise or the analysis of multiple corporate structures. Case Uniform provides a useful example. Despite clear indicators that payments to personal identification numbers (Uniform Civil Numbers; EGNs) of individual employees represented off-the-books- financial flows, investigators remained focused on the violence charges rather than systematically mapping the network's financial infrastructure. Resource constraints further compound these issues. Both national and regional investigative units lack dedicated financial intelligence analysts, forensic accountants, and specialised training in profit tracing. Moreover, reliance on administrative penalties rather than criminal asset forfeiture may further reduce incentives to conduct thorough financial investigations.

11.5.2 Recommendations for improving financial investigations in Bulgaria

Recommendation 1 – Enhance multi-agency cooperation

The first step towards strengthening financial investigations to counter criminal enterprises should be the establishment of joint investigative teams comprising criminal investigators, financial intelligence analysts, and tax authorities from the outset of a case. Case Tango demonstrates the value of seizing financial records and digital devices during searches. However, such evidence requires systematic analysis by specialists capable of reconstructing cash flows and tracing asset movements – capabilities beyond those of most investigative units. Some steps have already been taken to improve coordination between different agencies involved. The Ministry of the Interior has recently announced the creation of a specialised operational group responsible for analysing and combating money laundering. The task force will comprise officials from the National Revenue Agency, Customs, the National Agency for National Security, the Public Prosecutor's Office, and other relevant institutions, and will be based in the General Directorate of National Police. Although progress has been delayed by Bulgaria's ongoing political instability, this represents a step in the right direction (Kitanova, 2025).

Recommendation 2 – Strengthen the analysis of financial transactions and corporate structures

Increasing these capacities would enable law enforcement authorities to apply a more comprehensive follow-the-money approach. Financial investigations should therefore be prioritised as a parallel track to traditional evidence gathering. For example, in Case Victor, investigators could have sought bank records from the transport companies at an early stage to document discrepancies between fees charged to construction clients and actual disposal costs. Similarly, **payment data** could have been requested from Easypay and other financial service providers involved in Case Uniform's payday loan scheme to reconstruct complete transaction histories.

This financial transaction analysis infrastructure should be complemented by stronger capacity to analyse **corporate structures**. Developing investigative protocols for tracing complex ownership structures would enable LEAs to pursue a more intelligence-led approach and reduce the ability of criminal networks to adapt to investigative pressure. Case Uniform provides a clear example, revealing overlapping ownership between the primary business and related entities controlled by family members of the criminal network's leadership. This contributed to the network's resilience. Systematic beneficial ownership analysis could help uncover the network's true controllers and facilitate the identification of assets.

Recommendation 3 – Strengthen the use of criminal asset seizure

Following the implementation of the aforementioned recommendations, the next step for Sofia's law enforcement authorities should be to develop their capacity and focus on parallel financial investigations. The administrative sanctions currently used against unlawful practices such as debt entrapment, coercive debt collection, and illegal waste dumping have proven insufficiently deterrent for these criminal networks. The potential profits generated by these schemes substantially outweigh the costs associated with such sanctions. To ensure that crime does not pay, a fundamental shift in the approach to sanctioning may therefore be required, moving from fines-based administrative sanctions towards **criminal asset seizure** targeting the proceeds, infrastructure, and assets of crime. For example, vehicles used for illegal dumpling could be seized and repurposed by municipalities, while properties

used for nightclubs or payday lending could potentially be converted for community use. Such an approach would significantly increase the costs of engaging in criminal activities and could therefore provide an additional deterrent to potential offenders.

11.6 Summary of research findings: Sofia

The analysis demonstrates how high-risk criminal networks exploit structural vulnerabilities within Sofia's legitimate economy to generate profits, evade regulatory oversight, and establish themselves within mainstream commercial sectors. Across the cases, several overarching patterns emerge that illustrate the broader dynamics of criminal use of Sofia's economy. First, and perhaps most notably, **regulatory gaps** and weak enforcement mechanisms provided significant opportunities for criminal exploitation in all three cases. Whether through exceptions in consumer credit legislation, inadequate municipal inspection capacity, or limited oversight of nightlife establishments, each case demonstrates how criminal networks in Sofia identify and exploit specific vulnerabilities within regulatory frameworks. Furthermore, Sofia's economic structure, characterised by extensive subcontracting chains and fragmented responsibilities across multiple actors, systematically obscures accountability.

Another significant facilitating factor across all three cases was the central role of legitimate business structures in providing operational infrastructure and concealing criminal activities. In each case, companies were deliberately established or used for criminal purposes. Although formally registered and operating under legitimate business activities, these entities functioned as vehicles for systematic criminality. The assets of transport companies, nightclubs, and payday loan offices served as **dual-use infrastructure**, enabling illicit operations while maintaining a façade of legitimacy. Moreover, the organisational structure of the criminal activity often mirrored that of the legitimate business, with key criminal figures occupying managerial roles and other members holding corresponding operational positions. This integration allowed criminal proceeds to circulate through seemingly legitimate commercial channels, complicating detection and prosecution while facilitating the incorporation of illicit profits into the legitimate financial system.

Furthermore, all three cases provide insight into how criminal **networks adapt to law enforcement pressure**. Following the dismantling of the organisation of 'The Hammers', the nightlife business model persisted through a restructured ownership model. The network involved in Case Victor adapted quickly to new leadership within the Municipal Inspectorate by exploiting legal loopholes to evade administrative sanctions. Similarly, the fast-credit franchisee involved in Case Uniform could potentially have continued its operations at other locations by exploiting its decentralised, horizontal structure, as only a limited number of individuals involved in the scheme have been affected by law enforcement investigations.

Addressing the criminal use of Sofia's legitimate economy requires comprehensive reforms. First, although the loopholes in consumer credit legislation have been closed, **proactive enforcement** and **sanctioning** of non-compliant companies remain necessary. This should be complemented by licensing requirements, including mandatory criminal background checks and beneficial ownership transparency for payday loan and other fast-credit operators, waste transport companies, and nightlife establishments. In the waste disposal sector, a more specific measure would be the introduction of weight-based GPS tracking for construction waste transport, enabling real-time monitoring of disposal compliance.

Independent **oversight mechanisms** should also be established for municipal inspection services. These could include random integrity testing, mandatory rotation of personnel in positions particularly vulnerable to corruption, and financial disclosure requirements. Such measures could be complemented by protected reporting channels (i.e., 'whistleblowing') within municipal structures for individuals who observe criminal activity.

Finally, an **integrated case management** system should enable prosecutors to link predicate offence investigations with parallel financial investigations, asset tracing, and money laundering inquiries. Greater information-sharing between municipal authorities, law enforcement, regulatory agencies (such as the Commission for Consumer Protection), and financial intelligence units would further strengthen cross-sectoral coordination and facilitate the identification of early warning indicators spanning multiple sectors.

STOCKHOLM

EMPIRICAL RESULTS

12.1 Introduction

12.1.1 Background and context

Although the term 'criminal infiltration' is gaining traction, it is not yet widely used in Sweden. Numerous reports by government agencies address organised crime and the abuse of the legal economy by criminal networks, but these are generally broad in scope and lack detailed empirical evidence (see, for example: Ekobrottsmyndigheten, 2025; Gunnarson, 2023; Korsell, 2018; NOA, 2025; Rostami & Mondani, 2024). A related concept in Sweden, '**companies used as crime tools**', captures certain forms of infiltration, particularly criminal cover-ups. This typically refers to short- or medium-term schemes involving MTIC fraud, credit fraud, and the use of companies as subcontractors or as vehicles for money laundering in illicit labour schemes (Brå, 2016, 2025). Reports provide greater detail for specific schemes and sectors, particularly those involving labour-related crime (see, for example: Case X-Ray; Fair Play Bygg, 2025; SOU, 2023). More broadly, 'criminal infiltration' in the Swedish context often refers to the use of facilitators to gain access to the legal economy, although this appears to be even less common than criminal cover-ups (Brå, 2024, 2025). Similarly, the criminal abuse of legitimate business services may be interpreted as involving facilitators or insiders, yet such practices are rarely described as infiltration. Instead, the term 'enabling activities' is more commonly used.

Operational law enforcement agencies and researchers face several **challenges** in studying criminal infiltration and the use of companies by criminal networks. A key challenge is the fact that register-based studies both underestimate and overestimate the involvement of criminal networks. On the one hand, not all members of a criminal network use their businesses for criminal networks. On the other hand, many companies used for criminal activities are not registered in the names of known offenders but instead are held by nominees or strawmen.

The scale of criminal infiltration in Stockholm is difficult to assess. As a hidden phenomenon, no local or regional estimates are available. However, national-level analyses provide illustrative evidence for a limited number of sectors. In 2024, for instance, Rostami & Mondani (2024) published a report, commissioned by Stockholm's Chamber of Commerce, on the use of companies by criminal networks. The report highlights the **systematic risks** posed by the increasing infiltration of criminal elements into the legal economy, particularly through its potential to undermine the legitimacy of a welfare system founded on high levels of trust and social capital. The study analyses data covering the period 1995-2016, including 12,768 individuals identified by the Swedish Police Authority as being involved in organised crime during that period. Of these, 4,311 (34%) had corporate involvement, for example as company board members. Although the authors do not establish whether these companies were used for criminal purposes or whether the corporate involvement occurred before, during, or after the individuals' involvement in organised crime, the findings demonstrate a clear association between criminal entrepreneurship and legitimate companies.

A more extensive and systematic analysis of the use of **companies as 'crime tools'** by organised crime was published by Brå (2025), including 56,000 individuals involved in, or associated with, organised crime. One fifth had been registered as a company representative at least once between 2020 and 2023. Collectively, they were involved in approximately 23,000 companies, representing 1.7% of all companies in Sweden. The study identified several notable differences between these companies and the wider Swedish business population. First, a larger proportion were limited companies (80% compared with 65% nationally). Second, individuals linked to criminal networks generally served as company representatives for relatively short periods. Third, these companies were considerably more likely to enter bankruptcy and to have outstanding debts to the state.

In Brå's (2025) study, the sectoral classification of these companies was more frequently unknown: sectoral data were missing for 12% of these companies, compared with only 0.5% of all companies in Sweden. Among the companies for which sectoral information is available, most are concentrated in trade, including the repair of motor vehicles and motorcycles. Construction, real estate, hotels and restaurants, and transport and storage are also overrepresented compared with the wider Swedish business population. By contrast, companies operating in the legal, financial, scientific, and technical sectors are relatively less common.

The **sectors most vulnerable** to criminal infiltration in Sweden are broadly similar to those identified in other European countries. Sectors commonly highlighted in both the MORE and ARIEL studies include cash-intensive businesses, such as restaurants, bars, and hairdressers, as well as the construction, welfare and social services, and waste sectors. Among the 38 infiltration cases collected in the MORE project, the construction sector accounted for the largest number (nine cases), followed by import companies (six cases), and the social services and healthcare sectors (five cases) (Savona & Riccardi, 2018).[39] Tax fraud, welfare fraud, and credit fraud were among the most frequently identified offences.

12.1.2 Data and methodology

The economic (sub)sectors were selected based on the published reports outlined above (see Section 12.1.1), complemented by meetings and interviews with members of a '**reference group**' established for this purpose, comprising representatives from the municipality, the Swedish Police Authority, the Economic Crime Authority, the National Tax Agency, the Company Registration Office, and the Prosecution Authority. During an initial meeting, the group discussed the sectors considered most relevant for Stockholm in relation to the criminal use of the legal economy. Based on these discussions, suitable **case files** were subsequently identified through contacts with relevant contact persons, investigators, prosecutors, and inspectors. The case files comprised recent, preliminary investigations by LEAs involving the use of companies by criminal networks in Stockholm, with a particular focus on cases investigated by the Economic Crime Authority.[40]

[39] Healthcare in Sweden is largely tax-funded and organised by regional authorities, while social services, including care homes for various groups, are organised by local authorities. Although service provision is predominantly public, private providers – often profit-driven limited companies – increasingly operate within the publicly funded system under public regulation.
[40] In Sweden, court judgements are publicly available and can be accessed through judicial databases or requested directly from the courts, provided that the suspect's social security number or the relevant case file number is known.

The files were shared digitally and included materials such as interrogation records, wiretaps, chat messages extracted from suspects' smartphones, transaction records, company data, and searches of suspects' premises. For Case Whiskey, additional information was provided on decisions by the Health and Social Care Inspectorate, as well as data from civil courts concerning the foreclosure of companies. As the case files contain only information used in the investigation of the suspected offences, **interviews** were also conducted to clarify certain findings and address gaps in the available information concerning the three selected sectors, their vulnerabilities, and the criminal groups or networks involved in or associated with the cases. The insights provided by the interviewees and members of the reference group therefore complemented the analysis of the written case files.

12.1.3 Critical remarks

First, it should be noted that Sweden does not have a specific **criminal offence** addressing the criminal use of legitimate businesses. Instead, the applicable criminal classification depends on how the company is used. Where a company is used to conceal the transport or storage of illicit goods, the offence is generally classified in relation to the goods concerned. Where a company is used for money laundering, the conduct may be classified as gross money laundering or, more commonly, commercial money laundering (see Case X-Ray). Tax fraud and accounting offences may also apply (see Case Whiskey and Case Yankee). In the latter case, it may be sufficient to establish that accounting records are missing or contain inaccurate information. The applicable penalties are comparable to those for fraud and money laundering.

Second, the **organisational landscape** among Swedish authorities shapes the available knowledge on criminal networks and the criminal use of companies. Membership of a criminal network is not, in itself, a criminal offence in Sweden. To establish an aggravated offence, prosecutors must primarily demonstrate that the offence was committed in a systematic or organised manner. Consequently, there is no particular need for investigators to examine connections with criminal networks. Police intelligence units may have substantial knowledge of these networks, but often have limited evidence that can be used in criminal proceedings. Police investigations tend to focus on specific individuals, rather than on the companies through which criminal activities may be facilitated. By contrast, the Economic Crime Authority and tax crime investigators within the National Tax Agency focus primarily on companies and economic crime phenomena rather than on individual actors. Where the objective is to establish that a tax or accounting offence has been committed, there is little need to investigate the individuals behind the conduct beyond identifying the suspects responsible for the offences.

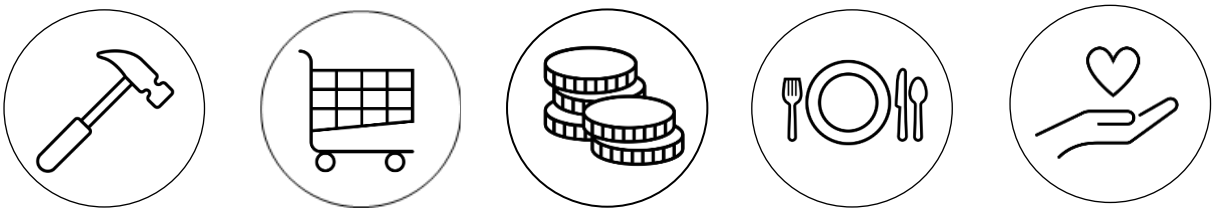
Third, the **relevance of the economic sector** varies across different forms of criminal company use. In some cases, the sector is important for the criminal set-up, whereas in others it is of limited relevance. This is particularly the case for the use of companies to issue or use fake invoices for moving money and for money laundering, where the main consideration is often to identify a suitable company that minimises the risk of detection. By contrast, more specialised forms of company use can be found in sectors subject to specific licensing requirements and regulatory oversight. One finding from the recent report on company use, supported by discussions with the reference group, is that many sectors are perceived as potential risk sectors (Brå, 2025). There is also at least anecdotal evidence that criminal networks operate companies across multiple sectors. Consequently, when controls are strengthened in one sector, some networks may be able to shift their activities to another, related sector (Brå, 2022).

12.1.4 Identification of vulnerable (sub)sectors

To identify potentially vulnerable sectors, the previous studies outlined above were used to narrow down the range of relevant sectors (see Section 12.1.1). As these studies were based on national-level analyses, the **situation in Stockholm** was subsequently discussed with the reference group to assess their relevance in the local context. Several sectors and subsectors were identified:

- Care and accommodation services, including residential care homes for older people;
- Sectors in which the municipality procures services from private companies (which includes most of the sectors listed below);
- Maintenance of parks and other public green spaces;
- Various subsectors within the construction industry;
- Waste disposal;
- Cleaning services;
- Real estate, including companies that own suburban shopping centres and, in some cases, the surrounding residential properties;
- Restaurants;
- Health centres;
- Market trading and wholesale businesses, including fruit and vegetable wholesalers;
- Financial services;
- Education, particularly private schools.

Subsequently, the reference group was asked to identify known cases in the sectors listed above. Based on their input, together with findings from other research projects (e.g., Brå, 2025; Savona & Berlusconi, 2015; Savona & Riccardi, 2018), four sectors appeared to have a higher prevalence of criminal use than most others: **construction**, **market trading and wholesale businesses** (e.g., fruit and vegetable wholesalers), **financial services**, and **restaurants**. At the national level, authorities primarily identify the **welfare sector** as vulnerable to criminal use. This sector was therefore added to the selection.



The sectors were subsequently assessed based on the potential harm associated with criminal activities, the extent to which the municipality may be affected (e.g., through the procurement of services), and the types of offences involving companies in each sector. To ensure variation in the types of criminal use, the following three sectors were selected:

- **Care and accommodation services** – Cases in this sector have involved particularly serious and specific harms. The sector is vulnerable to criminal use due to low barriers to entry, flexible working hours, and the relative ease of falsifying working hours and salary payments. These vulnerabilities also apply to other subsectors of the welfare sector (NUC, 2025).

- **Construction** – Construction is a recognised risk sector for criminal networks, with numerous relevant court cases, municipal procurement of construction services, and several ongoing infrastructure projects in Stockholm. Cases typically involve substantial sums of money and may include worker exploitation. Construction companies have also been targeted for the theft of explosives subsequently used by criminal networks, with serious consequences for third parties.
- **Market trading and wholesale businesses** – The municipality can act on certain suspicions, particularly through the enforcement of food safety legislation. The subsector is also part of a broader economic sector in which the police have raised concerns about the presence of criminal networks.

12.2 Case Whiskey: Children in the Care of Criminals[41]

Case Whiskey concerns a criminal network centred on four long-standing male friends, at least one of whom was involved in a criminal group (see Annex 8.W). Together or separately, they have established a number of companies, mainly private consultancy firms, that facilitated the placement of children in foster care, often in residential facilities presented as foster homes. Their business model was straightforward: they facilitated the **placement and care of vulnerable and/or high-risk children**, charged municipalities premium rates, and minimised expenditure on their care. While this business model is not in itself illegal, it has been associated with the employment of individuals with criminal backgrounds, neglect of children, various tax and accounting offences, breaches of contractual obligations towards municipalities, and the use of children in criminal activities. In effect, municipalities – and the welfare state more broadly – pay companies linked to criminal actors to provide care for vulnerable children, including children who are themselves heavily involved in crime.

12.3 Case X-Ray: Construction and Cash Compensation[42]

Case X-Ray concerns a criminal network whose members were connected primarily through a common language, Russian, despite originating from different Eastern European countries (see Annex 8.X). At its core were three long-standing male friends who involved others in operating a **cash compensation scheme** through multiple limited companies. The network was involved in money laundering and provided services to client companies, primarily in the construction sector, using undeclared workers. These services were provided both to members of the wider network and to external clients. The network also operated an underground banking (or 'hawala') service through which refugees and migrants could transfer, for example, money as support to a conflict zone. In addition, it provided currency exchange, cryptocurrency purchases, and services for moving cash into and out of bank accounts. This combination of financial services was reported to have attracted clients from drug-trafficking networks.

[41] The main sources of information for the analysis of Case Whiskey were case files and interviews with a municipal investigator, police analysts, and an individual working with inspections. Media reports were also used to corroborate information from the interviews and provide additional details.

[42] Case X-Ray was primarily documented through an extensive preliminary investigation and a court judgement, supplemented by a limited number of interviews and research reports on criminality in the construction sector.

12.4 Case Yankee: Money, Meat, and MTIC

Case Yankee concerns a criminal network centred on two individuals and their business associates (see Annex 8.Y). Many, although not all, originated from the same Middle Eastern country and had previously conducted business with one another. The two key individuals used two companies to carry out a **'Missing Trader Intra-Community' (MTIC) fraud** involving meat, as well as credit fraud against a major Swedish bank. The other business associates were involved in the MTIC fraud to varying degrees, either knowingly or unknowingly. As part of the MTIC fraud, one company imported meat from within the EU without correctly declaring or paying VAT. It then sold the meat to the second company, which gained a significant competitive advantage by avoiding VAT. The second company subsequently sold the meat to large food retailers and restaurants. Several actors had direct or indirect links to a criminal group, while one of the two key individuals had previously operated several similar MTIC frauds. Although the basic structure is straightforward, the case itself is more complex, involving numerous actors as well as conflicts and confusion.

12.5 Financial investigations in Sweden: key challenges and recommendations

12.5.1 Challenges in financial investigations in Sweden

One challenge, raised by the reference group, concerns the **lack of clarity** surrounding the term 'financial investigation'. It may refer to anything from tracing bank accounts and analysing company records to the more systematic analysis of financial data. Moreover, a financial investigation is generally initiated only when a prosecutor considers it necessary. For example, when a member of a criminal network is suspected of assault, a prosecutor may not initiate a financial investigation, even though this could reveal important information for mapping the wider network. The assault, for instance, may be linked to debts or loans within the criminal environment, but such connections may remain unknown to the investigators.

Financial investigations are neither the sole nor the primary solution to addressing criminal networks. They cannot, on their own, dismantle such networks. However, when financial components are incorporated into criminal network mapping, they can support the prioritisation of networks and individuals for both financial and criminal investigations. Several pieces of **information-sharing** legislation have been introduced recently, indicating a willingness to improve information exchange, and many authorities have begun to make use of these provisions. Nevertheless, some interviewees noted that authorities tend to interpret information-sharing legislation conservatively, meaning that new provisions may take time to become fully embedded in practice.

Technical challenges also remain. Two members of the reference group highlighted difficulties in incorporating financial data into law enforcement databases and conducting searches across these datasets. Compiling the relevant information often requires substantial manual effort, particularly when information is shared between law enforcement authorities, as there is no shared intelligence register for financial information relating to criminal networks. Similarly, collecting and coordinating financial information on the same network across different authorities or departments has proved

challenging in practice. Consequently, even where substantial amounts of public data are available, it can remain difficult to use this information efficiently.

Interviewees noted that certain types of transactions are particularly difficult to trace, including **cross-border transactions**, especially those involving countries outside the EU. While information can be obtained within the EU, this may still be administratively challenging when accounts belong to non-Swedish citizens. Effective use of these mechanisms requires prosecutors to know how to proceed and what assistance is available from their EU counterparts. Moreover, the technical systems used to request and receive information do not always meet operational needs. Europol can provide valuable support, but not all prosecutors and investigators are aware of this possibility. **Cryptocurrency transactions** are also considered particularly challenging to trace, especially when the relevant assets or wallets cannot initially be identified. Interviewees further described the difficulty of managing large volumes of transaction data and identifying the transactions most relevant to an investigation. At the same time, specialised expertise remains limited: according to at least one interviewee, case analysts and personnel with accounting expertise are scarce within the law enforcement system. This is consistent with findings from previous studies (Brå, 2019, 2021).

12.5.2 Recommendations for improving financial investigations in Sweden[43]

Drawing on the cases, interviews, and discussions with the reference group and other experts, several recommendations emerge:

- **Restrict access to companies**, particularly those with a credible track record. This could be achieved, for example, by requiring licences for company brokers or by making it easier and faster for individuals to liquidate their own companies.
- **Make identity misuse more difficult**, particularly where individuals are incorrectly registered in the population registry. The use of biometric data for identification purposes could be an important tool in this regard.
- Develop registers enabling investigative authorities to **identify major shareholders and beneficial owners** of companies. This would make it more difficult for organisers to conceal their involvement behind strawmen. Access to information on powers of attorney for bank transactions would also facilitate law enforcement and financial investigations.
- Increase awareness among procurement actors of **indicators of strawman arrangements**.
- **Accelerate the bankruptcy process** for companies used solely for illicit purposes and combine this with bans on business activity for the actors involved.
- Develop stronger mechanisms for **monitoring procured welfare services**, particularly regarding what constitutes a suitable provider and how quality should be assessed. Municipalities, regions, and inspection agencies have already begun collaborating in this area.

[43] Many of these recommendations are aligned with Brå's report on the criminal use of companies (Brå, 2025).

- Establish a **shared intelligence database** for law enforcement authorities on criminal networks and serious forms of economic crime. It is also difficult to identify data on denied or revoked permits and registrations, particularly when it is unclear which authority holds the relevant information. While legitimate actors operating within a single sector are often subject to the same supervisory authority, criminal networks that shift between sectors to evade controls can exploit this fragmentation to their advantage. Administrative measures against companies can be implemented relatively quickly, but may leave little trace when the individuals behind the company establish a new one.
- Strengthen the capacity to conduct **financial investigations in medium-sized cases**, which are often too small for multi-agency cooperation but too complex for a single authority to handle effectively. In larger multi-agency investigations, differences in objectives, organisational cultures, terminology, and working practices should be addressed at an early stage. Reference group members also highlighted the difficulty of finding time to evaluate large cases involving staff from different agencies, creating a risk that important lessons are not captured and that mistakes and inefficiencies are repeated.

12.6 Summary of research findings: Stockholm

All three cases analysed involve loosely organised networks led by entrepreneurs, in which personal contacts play an important role and shape the businesses and services provided. Although the actors have contacts with more traditional criminal groups, they operate primarily as individuals and entrepreneurs, drawing on competitive advantages within their respective sectors. The cases also illustrate **different motivations** among the actors involved. While some become increasingly involved in the criminal environment, others seek to help children or fellow nationals, or to develop legitimate businesses and distance themselves from criminal activities.

The **Swedish law enforcement system** is structured in ways that affect the understanding of organised crime. While the Swedish Police focuses on mapping criminal networks and key actors within them, the Economic Crime Authority and the National Tax Agency focus their mapping on phenomena and companies responsible for large-scale tax offences, without always identifying links to criminal networks. These approaches can be combined through multi-agency collaboration. However, the criminal environment is highly fluid, with alliances and company structures constantly changing. According to interviewees, both competition and cooperation are important dynamics within criminal networks, although their relative importance varies. In traditional criminal markets, particularly drug trafficking, competition is described as highly significant. In economic crime, by contrast, there is greater scope for new actors to enter the market, making cooperation between networks more common. For highly sought-after services, such as those provided by strategic insiders, competing networks may even purchase services from the same actors.

The cases illustrate, and interviewees confirmed, that a variety of criminal networks make use of legitimate businesses. A general risk identified in Swedish authorities is that greater emphasis is placed on providing services to individuals and businesses and facilitating transactions than on ensuring that **adequate controls and checks** are in place to identify criminal actors within these systems. At the same time, two somewhat competing tendencies can be observed in Sweden. On the one hand, efforts are made to simplify procedures for businesses through reduced controls and increased digitalisation. On

the other hand, efforts are aimed at strengthening controls and assigning a greater crime-prevention role to public authorities. Some authorities maintain registers based on organisational numbers rather than individuals. However, companies can be changed relatively easily.

Moreover, the extent to which relevant authorities can conduct checks varies, both because of differences in the **legislation** governing their powers and because of differences in the **resources** and expertise available to them. In Case Whiskey, for example, the network avoided permit requirements and reduced the likelihood of inspections by presenting the establishments as family homes rather than HVB-homes ("Homes for Care or Residence"). Cases X-Ray and Yankee, meanwhile, occurred in sectors subject to at least some controls and forms of supervision. Nevertheless, the actors were able to blend in with legitimate businesses, at least temporarily. Actors in all three cases had previously committed similar offences through other companies. The cases therefore illustrate how quickly criminal actors can change companies once they are detected by different control systems.

The analysis of the case studies further suggests that individuals connected to or directly involved in criminal networks establish or acquire legitimate businesses for their own benefit, either as seemingly legitimate source of income and/or to support their criminal activities. However, particularly in Cases Whiskey and X-Ray, the analysis suggests that these businesses may also have **unintended positive effects for the criminal world** as a whole. The involvement of criminal actors in legitimate businesses creates opportunities for other criminal networks, which can exploit these businesses and their services in various ways. In Case Whiskey, young people were placed in a criminal environment and, rather than being distanced from it, acquired new skills. Some were even recruited, not only by the network that placed the child or owned the home. In Case X-Ray, other criminal networks made use of services provided by the Russian-speaking criminal milieu. This is less evident in Case Yankee, although information in the case file indicates that other criminal networks became involved in collecting debts from one of the financiers.

Furthermore, the analysis demonstrates that legitimate businesses also serve to **conceal criminal activities** in plain sight. In all three cases, the level of sophistication is low, and it appears to be only a matter of time before the companies are detected. In some sectors, particularly as illustrated by Case Whiskey, control systems rely on warning signs emerging from the businesses themselves, a strategy that can be effective in identifying more overtly criminal actors. However, through a steady flow of new companies, sometimes with a credible history, as well as the use of strawmen and false identities, key actors can remain concealed from authorities, banks, and other institutions. At the same time, they can exploit the benefits provided by society and participate in publicly procured services.

Another challenge identified in the analysis is that **multi-agency collaboration** often requires time to build trust and establish a shared understanding of what information can and should be shared. In the construction sector, the problems are well recognised by the actors involved, and information sharing is already well established. In the foster care sector, by contrast, information sharing remains more challenging. The Police Authority and Health and Social Care Inspectorate (IVO) are reportedly developing closer cooperation, but this collaboration is still at an early stage compared with that in the construction sector. In the food sector, the relevant inspecting authority varies depending on where in the supply chain the food is handled, from import and distribution to restaurants, complicating efforts to establish collaboration.

UTRECHT

EMPIRICAL RESULTS

13.1 Introduction

13.1.1 Background and context

The Netherlands has long occupied a **strategic position** within European organised crime networks, due to its highly developed transport infrastructure, open economy, and international trade connections. The country plays a central role in several illicit markets, most notably drug trafficking. Large volumes of cocaine enter Europe through Dutch ports and logistics hubs, while the Netherlands also functions as a production, transit, and distribution centre for synthetic drugs (Europol, 2022). The Netherlands' position within European organised crime is further reinforced by the role of its **seaports**, particularly the Port of Rotterdam, which, together with Antwerp and Hamburg/Bremerhaven, constitutes one of the most targeted port clusters for criminal use of the legal economy in the EU. According to Europol (2023a), the sheer volume of maritime container traffic handled by these ports creates structural vulnerabilities that are systematically exploited by organised crime groups.

For several decades, organised crime has been a persistent subject of political, administrative, and academic attention in the Netherlands. Studies have examined the nature, scale, and evolution of organised criminal networks, providing periodic assessments of developments in organised crime at the national level. These studies consistently demonstrate that organised crime is dynamic and adaptive, increasingly **exploiting legitimate infrastructures**, institutions, and processes (Strategisch Kenniscentrum Ondermijnende Criminaliteit, 2026). More recent research has further advanced this understanding by highlighting how criminal collaboration structures exploit organisational, procedural, and human vulnerabilities within both public and private settings (Kruisbergen et al., 2019; Strategisch Kenniscentrum Ondermijnende Criminaliteit, 2026).

Thus, over time, our understanding of organised crime has evolved. Whereas earlier research focused primarily on criminal groups and their illicit activities, it has become increasingly evident that organised crime also operates through **legitimate structures and institutions**. Criminal networks do not merely exist alongside the legitimate economy; they actively engage with it, depend on it, and in some cases reshape it to serve their interests. Businesses are not simply vehicles through which criminal proceeds can be concealed or laundered; they can also provide mechanisms for access, influence, and resilience.

13.1.2 Data and methodology

The identification of vulnerable economic (sub)sectors in Utrecht and the selection of case studies followed a multi-stage process that combined consultations with local partners, analysis of available documentation, and efforts to access judicial and police records. The first phase involved close **collaboration with the Utrecht representative** within the PREVENT consortium, who works for the Municipality of Utrecht. This partner provided, in addition to access to respondents, relevant documents relating to the criminal use of the legitimate economy, both with a regional and national scope. The Municipality of Utrecht works with prioritised sectors based on indicators such as crime concentration. In consultation with the municipal representative, five sectors were identified as particularly vulnerable. These sectors aligned with municipal priorities, demonstrated evidence of criminal use in documented cases, or were assessed internally as posing significant levels of harm.

In a second phase, the research team sought access to **non-public case files** in order to analyse specific cases of criminal use of the legitimate economy. Additional efforts were made to obtain information from the analytical divisions of the police. These units were unable to provide case-specific or sector-specific intelligence beyond the general regional threat assessment, which outlines broad trends but does not contain details on ongoing individual cases.

Consequently, the study relied heavily on publicly available data on the identified sectors, interviews, and public judicial files for the development of the case studies. To select specific cases within the identified sectors, the research team and the municipality applied **three criteria**:

- The presence of a financial component or financial investigation;
- The involvement of a company operating within the relevant (sub)sector;
- The availability of a case outcome, such as a verdict or other procedural resolution, meaning that the case was no longer subject to a fully active investigation.[44]

Ultimately, three of the five sectors were selected for **case studies**. The analysis is based primarily on publicly available information and a limited number of expert interviews. For each case, two professionals directly involved in the case or sector were interviewed. This reliance increases the risk of incomplete or inaccurate information, particularly where interviewees were required to recall financial figures or reconstruct events from memory. Although information was cross-checked across multiple sources wherever possible, the absence of case files and supporting documentation inevitably limits the precision of the analysis. Furthermore, the third case study relied exclusively on publicly available sources, as no respondents directly involved in the case were available or remained employed at the relevant institution.

13.1.3 Critical remarks

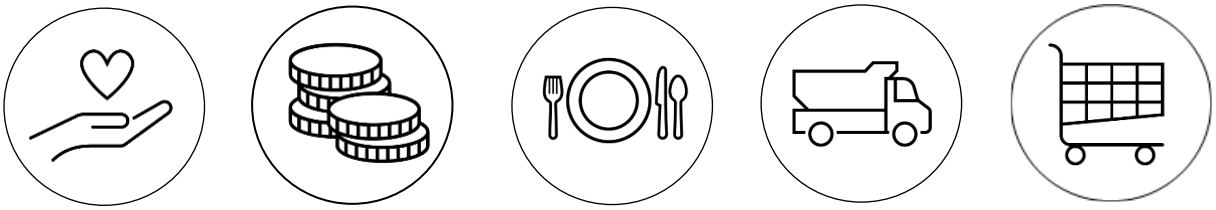
A structural critical remark in assessing the criminal misuse of businesses, both in the region of Utrecht and more broadly in the Netherlands, is not only limited capacity but also how that capacity is allocated. Although the Netherlands has a relatively strong institutional framework and access to administrative, fiscal, and financial data, these resources are not consistently translated into a thorough understanding of the financial dimensions of criminal misuse. Consequently, enforcement efforts tend to **focus on visible offences** or individual actors, while more complex forms of criminal misuse embedded in seemingly legitimate business activities remain under-investigated. This limitation is also reflected in the available data, as court records provide only limited information on the businesses underpinning criminal networks.

[44] This criterion was applied to ensure that interviews could be conducted and relevant information could be shared. However, for the first sector, an illustrative example is included despite the fact that the investigation remains ongoing or that the case has not yet been brought before the court. This example was retained because administrative sanctions have been imposed and certain aspects of the case have already been established.

A further critical remark concerns how the **financial dimensions** of criminal cases are reflected in judicial proceedings. The financial figures reported in court records and criminal investigations are typically based on conservative, evidentially substantiated estimates, deliberately restricted to amounts that investigators and prosecutors can prove beyond reasonable doubt. While this approach is both necessary and appropriate in a legal context, it has important implications for research relying on these records. In practice, documented criminal proceeds often represent the minimum amount that can be proven rather than the full extent of illicit earnings. For example, in Case Alfa-Alfa, the investigation focused on assets supported by sufficient evidence, while broader or longer-term financial flows may have remained outside its scope (cf. *infra*). Consequently, the financial reconstructions presented in judicial records, interviews, and publicly available sources are likely to underestimate the true scale of criminal profits. The financial dimensions discussed in this chapter should therefore be interpreted as conservative **lower-bound estimates**, shaped by the evidential requirements of criminal proceedings, rather than comprehensive assessments of criminal proceeds.

13.1.4 Identification of vulnerable (sub)sectors

In consultation with local authorities, five economic (sub)sectors were identified as particularly vulnerable to criminal use of the legitimate economy in Utrecht. The **healthcare sector**, financial services providers (with a particular focus on the **gold trade**), **hospitality**, **courier services**, and the **automotive sector** were selected. These five sectors reflect a diverse range of opportunity structures and forms of criminal use of the legitimate economy. While all five were identified as particularly vulnerable in Utrecht, three were selected for in-depth case study analysis: financial service providers (with a focus on the gold trade), the healthcare sector, and the automotive sector. It is important to note, however, that no single sector dominates in Utrecht. Rather, criminal use has been identified across a wide range of economic activities.



First, the **healthcare sector** was selected because of its long-standing prioritisation by the Municipality of Utrecht and the availability of a relatively strong evidence base. National and local analyses consistently indicate structural vulnerabilities, including fragmented oversight, trust-based funding mechanisms, and the ease with which healthcare providers can be established (IKZ, 2024). In Utrecht, several cases have demonstrated the resulting harms, including large-scale fraud, money laundering, the exploitation of vulnerable individuals, and substantial financial losses to public institutions (van der Torre & Jongepier, 2021).

Second, **financial services providers**, with a particular focus on the gold trade, were included due to their recognised role as facilitators of money laundering and value transfer. The national prioritisation of the gold trade has generated increased signals (NSOC, 2023), and local information indicates that a small number of businesses may play a disproportionate role in facilitating transactions for multiple criminal networks.

Third, the **hospitality sector** was identified as relevant due to its recurrent association with organised crime in Utrecht, particularly in relation to violence, intimidation, and public order disturbances. Although financial investigations of hospitality businesses are often constrained by limited capacity, the sector repeatedly emerges as an environment in which criminal networks interact, exert influence, and become visibly embedded.

Fourth, **courier services** were selected due to their rapid growth in Utrecht and emerging indications of links to organised crime based on internal municipal reports. The sector's operational characteristics, including decentralised structures, subcontracting chains, low entry barriers, and limited oversight, create opportunities for criminal use, such as cash-based compensation arrangements, labour exploitation, and the movement of illicit goods.

Lastly, the **automotive sector** has been prioritised in Utrecht for an extended period due to persistent indicators of criminal activity, including links to organised crime, violence, and financial offences. The sector provides services that are directly relevant to criminal networks. Local interventions, such as licensing requirements, highlight both the sector's vulnerability (Gemeente Utrecht, 2022). In 2018, the Municipality of Utrecht, the police, the Tax Administration, and Customs conducted an operation targeting seventeen companies on an industrial estate, primarily within the automotive sector. The action followed numerous verified signals of potential links to criminal activity, including nighttime operations, intimidation, a closed business culture, and a shooting incident at one of the premises. A police official noted that the automotive sector is both vulnerable to criminal exploitation and highly specialised, making it attractive for criminal exploitation (Tieleman, 2018). Among other uses, the sector has been exploited for ram-raid and ATM bombings. In 2020, a location in Utrecht was identified where expertise for such activities was being developed (Gemeente Utrecht, 2021). Subsequently, a licensing requirement for the automotive sector was introduced at the same industrial estate in 2022. Over the preceding five years, police registrations in the area were 40% higher than average, and incidents at the location were up to three times more likely to be linked to organised crime (Gemeente Utrecht, 2022).

13.2 Case Zulu: The Gold Trading Landscape

Rather than focusing on a single, detailed case study, Case Zulu examines the **gold trading and jewellery sector** as a whole, highlighting how legitimate businesses operating within this sector may be used for criminal purposes (see Annex 9.Z). In recent years, the gold trading sector in the region of the Middle Netherlands has attracted increasing attention from LEAs and local authorities due to concerns that it may be used for money laundering and other forms of financial crime. These concerns are not limited to isolated incidents; rather, the sector includes both legitimate and non-compliant actors, and its structural characteristics may create vulnerabilities that can be exploited for criminal purposes. In particular, the handling of high-value goods, the prevalence of cash-based transactions, and the ability to convert value into different forms can collectively facilitate money laundering activities.

An **illustrative example** reported in the media demonstrates how jewellers may potentially become involved in the conversion and movement of illicit financial flows (Politie, 2025). At the end of 2024, an individual was arrested after exchanging cryptocurrency for a substantial amount of cash at a jeweller's shop, prompting the Utrecht Police to initiate a criminal investigation. Subsequent joint inspections identified regulatory breaches, including failures to properly maintain the Digital Trader's Register (in Dutch: *Digitaal Opkopersregister*; DOR), an important instrument for preventing money laundering within the gold trade. The jeweller was subsequently suspected of facilitating money laundering through the conversion of cryptocurrency into cash and *vice versa*. A police raid was conducted, together with a search of a residential property associated with the owner. During these searches, a significant amount of cash and cryptocurrency was found.

Other cases involving gold traders at the national level further illustrate how the sector may be exploited for suspected **money laundering activities**. In one reported example, a gold dealer was intercepted by customs while transporting substantial quantities of scrap gold and cash without adequate documentation (FIU Nederland, 2022). The dealer claimed that the gold was intended for melting and reprocessing abroad before being returned to the legitimate market. Based on a combination of suspicious transactions, insufficient documentation, and prior intelligence signals, authorities identified potential money laundering concerns, resulting in a search of the business premises and the seizure of gold and cash assets.

13.3 Case Alfa-Alfa (AA): Fraudulent Healthcare

Case Alfa-Alfa (AA) concerns a healthcare company in Utrecht that operated between 2014 and 2018 and systematically defrauded publicly funded care schemes (see Annex 9.AA). Managed by three brothers, the organisation presented itself as a legitimate provider of home and day care. In reality, however, it served as a vehicle for **large-scale healthcare fraud**, facilitated by access to a vulnerable client base and deficiencies in sectoral oversight. The criminal network associated with the company primarily comprised family members, individuals from their social circle, and numerous clients receiving personal care budgets (in Dutch: *Persoonsgebonden Budget*; PGB). Many clients knowingly participated by sharing part of their allocated care budgets in exchange for little or poor-quality care.

Case Alfa-Alfa (AA) demonstrates how criminal networks exploit **structural vulnerabilities** in the Dutch healthcare system, including fragmented oversight, limited screening of new providers, and the ease of transferring clients or dissolving companies. The investigation was initiated following reports from the Financial Intelligence Unit (FIU) and criminal intelligence indicating extensive cash exchanges between the provider and its clients. Surveillance, wiretaps, and camera monitoring uncovered distribution lists detailing pre-arranged allocations of care funds, demonstrating the scheme's systematic nature. The trial took place between February and November 2019. Since then, several personal care budget holders have also been prosecuted, with some proceedings still ongoing in 2025. Similar large-scale healthcare fraud schemes employing comparable *modus operandi* remain active in Utrecht.

13.4 Case Bravo-Bravo (BB): From Showroom to Shadow

Case Bravo-Bravo (BB) concerns the criminal use of a **car-related business** in the Middle-Netherlands Police Unit, whose owner (C1_BB) became involved in organised drug-related crime and the laundering of criminal proceeds through vehicles and luxury goods (see Annex 9.BB). The criminal network operated between December 2019 and March 2021 and involved multiple actors coordinating the transport, financing, logistics, and distribution of **narcotics**, involving at least one hundred kilograms of cocaine. Communication within the network took place via encrypted communication services such as SkyECC. The laundering of assets and falsification of business records occurred between 2021 and 2023, resulting in a conviction of C1_BB in 2025. In November 2022, authorities seized approximately EUR 286,000 in cash, six luxury watches, several cars, and a motorcycle identified as criminal proceeds.

13.5 Financial investigations in the Netherlands: key challenges and recommendations

13.5.1 Challenges in financial investigations in the Netherlands

Financial investigations are increasingly prioritised across all crime phenomena and play a central role in understanding and disrupting organised crime embedded in the legal economy in the Netherlands. At the same time, the analysis highlights several structural challenges. A key issue is the partial and delayed **visibility of financial flows**. Although financial data can be traced over time, investigations are often reconstructive, taking place only after criminal proceeds have already been spent, reinvested, or transferred across jurisdictions. In the Dutch context, this challenge is particularly pronounced given the extensive financial and administrative data available, which is not always effectively integrated or analysed across institutions. Fragmentation between municipalities, police, and tax authorities further limits the ability to develop a comprehensive financial picture, while cross-border elements, such as foreign investments, add further jurisdictional and administrative barriers.

At the same time, the cases highlight that financial investigations offer distinct **advantages** beyond traditional criminal investigations. By focusing on financial irregularities, authorities can identify patterns across different types of crime and actors. Financial analyses can reveal connections and *modus operandi* within criminal networks, as observed in Case Alfa-Alfa, thereby providing entry points for intervention even where direct evidence of criminal activity is limited. In this sense, financial investigations are particularly valuable where criminal activities are embedded within legitimate structures.

13.5.2 Recommendations for improving financial investigations in the Netherlands

Recommendation 1 – Strengthen the analytical capacity of financial investigations

The primary recommendation is to strengthen the analytical capacity of financial investigations, not only by increasing resources but also by enhancing expertise. In addition, further efforts are needed to improve data-sharing and cooperation among relevant actors, both within the Netherlands and internationally. While legal safeguards remain essential, reducing unnecessary **administrative barriers** could significantly enhance the speed and effectiveness of financial investigations. This is particularly relevant when tracing financial flows in the context of international cooperation.

Recommendation 2 – Strengthen the proactive use of financial intelligence

Another recommendation, formulated by one of the respondents, is to move towards a more proactive use of financial intelligence. Rather than primarily supporting ongoing investigations, financial data could be used more systematically to identify patterns of the criminal use of the legitimate economy, detect emerging risks, and prioritise interventions. This would require a shift from case-driven to **intelligence-driven approaches**, in which financial analysis plays a central role in determining enforcement priorities. Financial-economic considerations should therefore not be treated as a separate category that may or may not be prioritised, but rather as an integrated component of the broader understanding of the criminal landscape. To achieve this, financial investigations need to be structurally embedded within broader strategies, supported by sufficient capacity and effective coordination between organisations to match the adaptability of criminal networks.

13.6 Summary of research findings: Utrecht

The cases of criminal use in Utrecht demonstrate that the relationship between crime and the legitimate economy is not incidental or opportunistic, but rather **structural and purposeful**. In these cases, businesses form an integral part of criminal activities and are primarily used to gain access to the financial system and legitimise criminal proceeds. Across the three sectors analyses – financial service providers, with a focus on gold trading, healthcare, and the automotive sector – the legitimate business does not function merely as a passive vehicle for laundering proceeds. Rather, it provides an enabling environment that facilitates the access, transformation, and concealment of criminal value. At the same time, the cases suggest that sector-specific vulnerabilities may be less important than recurring overarching mechanisms that transcend individual sectors. What appears more consistent, however, are the underlying business models of criminal use, which exploit gaps in oversight and rely on fragmented regulatory responsibilities.

An important insight from the cases is that the criminal use of a legitimate business is not necessarily confined to a single network or activity. Instead, certain businesses can evolve into shared infrastructures that serve multiple criminal actors. This is particularly evident in the gold trading sector (Case Zulu), where businesses may function as service providers for different criminal clients seeking to launder money through a combination of cash transactions, TBML, or potentially cryptocurrency conversions. This suggests that parts of the legitimate economy can take on characteristics of a **'crime-as-a-service'** model, functioning as underground banking systems in which access to the financial system or value transfer is outsourced to specialised actors. Such arrangements reduce the need for individual criminal networks to develop their own infrastructures, allowing them instead to rely on established business environments that are already adapted to minimise detection. Consequently, this dynamic complicates traditional law enforcement approaches focused on dismantling individual networks, as the underlying facilitating structures may remain intact and continue to serve new actors.

Furthermore, the cases also highlight the **role of social structures** in enabling the criminal use of businesses. This is particularly evident in Case Alfa-Alfa, where a social network based on family ties and shared backgrounds played a crucial role in the recruitment, coordination, and protection of criminal activities. In this case, fraud was not only committed by providers but also sustained through the active or passive involvement of clients and their social environment. This blurs the distinction between offenders and beneficiaries and creates a system in which criminal behaviour is normalised and collectively maintained. These dynamics suggest that the criminal use of the legitimate economy should, in some cases, be understood within their broader social context. Criminal activities may therefore be shielded and sustained not only through the concealment of financial flows, but also through social protection and the normalisation of criminal behaviour within social networks.

Ultimately, the **limited visibility of financial flows** emerges as a structural challenge rather than a methodological limitation. The report repeatedly shows that the financial dimension of criminal activity is only partially captured in both investigations and available data. Judicial records reflect conservative estimates, focusing on provable amounts rather than the full scope of illicit gains, while cross-border elements and fragmented information further limit the available knowledge. As a result, enforcement efforts risk focusing on individual cases or visible irregularities, while the systemic nature of criminal use remains insufficiently addressed.

CONCLUSION AND DISCUSSION

14.1 Conclusion: general research findings

14.1.1 General conclusions

The comparative analysis of the 28 case studies across Antwerp, Brussels, Caserta, Frankfurt, Paris, Madrid, Sofia, Stockholm, and Utrecht demonstrates that the **legitimate economy** is not merely a backdrop to organised crime, but an **indispensable environment** in which criminal networks operate. Across the jurisdictions examined, criminal actors were found to rely extensively on legitimate businesses, legal market structures, and lawful economic activities to sustain, support, conceal, and expand their criminal operations. The case studies therefore suggest that the relationship between organised crime and the legitimate economy is structural rather than incidental, with criminal networks increasingly embedding themselves within legitimate markets.

Despite the considerable diversity of the cases examined, several **recurring patterns** emerged. The cases covered a broad spectrum of economic sectors and criminal activities, ranging from drug trafficking and fraud to money laundering and other forms of organised crime. Criminal networks differed substantially in terms of their composition, internal organisation, scale, and geographical reach. Nevertheless, similar mechanisms were identified across cases and jurisdictions, suggesting that the criminal use of the legitimate economy is driven by a relatively stable set of underlying processes.

A key finding concerns the **multifunctional role** of legitimate businesses within criminal business models. Across the cases, businesses were used not only to facilitate criminal activities and launder illicit proceeds, but also to create an appearance of legitimacy, provide access to financial infrastructure, obscure beneficial ownership, and establish a presence within legitimate markets. In many instances, companies simultaneously engaged in genuine economic activities while serving criminal purposes. The distinction between legal and illegal economic activity was therefore increasingly blurred, with lawful and unlawful practices often becoming intertwined within the same organisational structures. Rather than functioning as purely criminal enterprises, many businesses operated as hybrid or 'dual-use' structures in which legitimate and illicit activities co-existed (cf. *infra*).

The findings further confirm the **motivations** (or 'drivers') previously identified in the literature for the infiltration of legitimate businesses by criminal networks. All major motivations identified by the Transcrime MORE project were reflected in the analysed cases, including profit maximisation, the laundering of illicit proceeds, the concealment of illicit trade, the facilitation of fraud and other criminal activities, and the pursuit of social, political, or territorial influence (Savona & Riccardi, 2018). While financial gain emerged as the dominant 'driver' across most cases, several examples also demonstrated how legitimate businesses can contribute to broader forms of criminal governance, particularly by strengthening social legitimacy, sustaining (electoral) influence within local communities, and facilitating access to public and administrative structures. Certain cases, particularly in Italy, demonstrate, for example, that criminal networks seek to establish comprehensive territorial control over both legitimate and illicit businesses.

14.1.2 Vulnerable sectors and underlying opportunity structures

The case studies identified several **economic sectors** that featured prominently in the criminal use of the legitimate economy. Construction, transport and logistics, hospitality, and real estate emerged as the most prevalent sectors, while recurring examples were also found in gambling, healthcare, and environmental services (see Figure 2). However, the findings suggest that vulnerability should not be understood primarily as a sector-specific characteristic. While certain sectors may offer attractive opportunities due to factors such as cash intensity, administrative complexity, low barriers to entry, fragmented oversight, or opaque subcontracting arrangements, similar mechanisms were observed across highly diverse economic activities. The recurring feature across the cases was therefore not necessarily the sector itself, but the opportunities and functions it provided to criminal actors.

The analysis thus indicates that **cross-sectoral** (or sector-transcending) **vulnerabilities** may be more important than the characteristics of individual sectors. Criminal networks frequently exploited opportunities associated with weak verification procedures, limited transparency, gaps in supervision, and the possibility of creating credible legitimate cover. Consequently, the choice of sector appeared to have been driven less by the intrinsic nature of a particular industry than by the practical opportunities it offered to minimise detection risks and maximise operational flexibility. The evidence therefore suggests that vulnerability is not confined to a limited number of traditionally identified 'high-risk' sectors. Rather, very few sectors appear entirely unexposed to criminal use, and virtually any area of the legitimate economy may become vulnerable when suitable opportunities, regulatory gaps, or facilitating conditions are present.

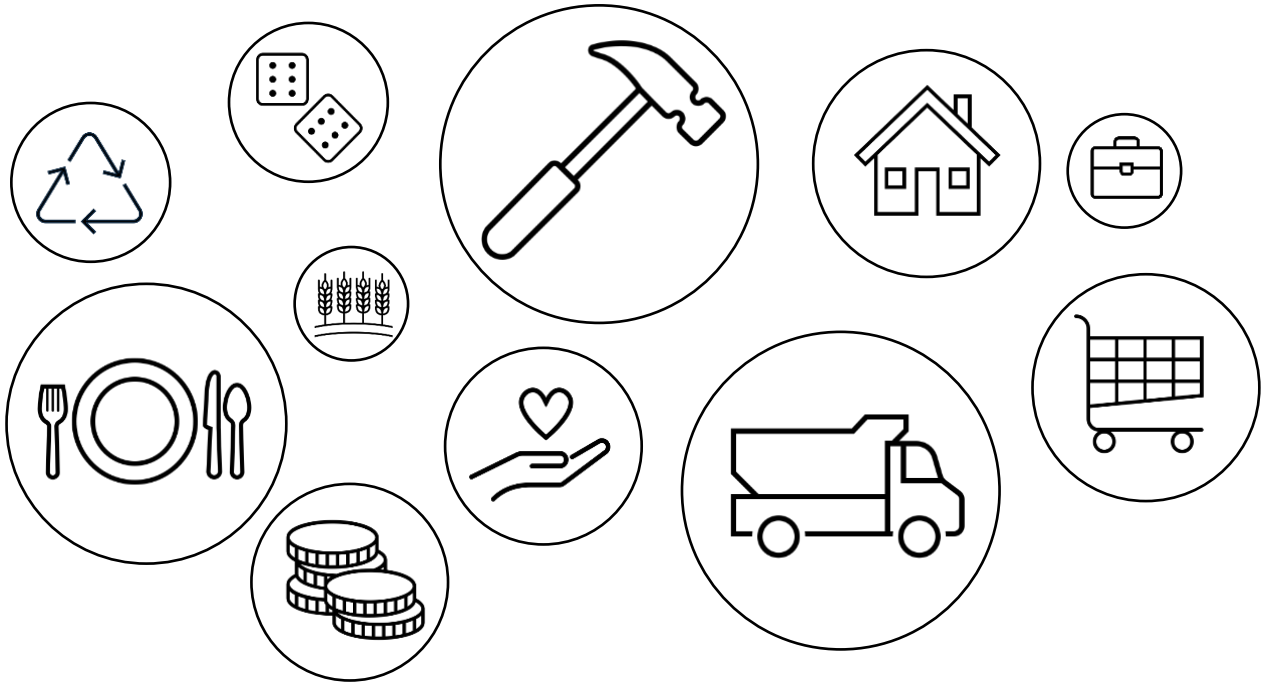


Figure 2
Most prevalent economic sectors identified across the case studies (with size indicating frequency of occurrence)

The findings further illustrate that criminal networks rarely restrict themselves to a single sector. Several cases revealed complex corporate 'ecosystems' consisting of multiple interconnected businesses operating across different economic domains and sectors. Such **'spiderweb structures'** enabled criminal actors to combine different functions within a broader organisational framework. This suggests that analytical attention should extend beyond individual sectors towards the combination of vulnerabilities and opportunities across the legitimate economy that can facilitate criminal use (see Section 14.2).

14.1.3 Recurring patterns throughout the criminal process

Although the distinction between different phases of the crime script can be regarded as an analytical simplification rather than a direct reflection of reality (see Section 14.2), the comparative analysis nevertheless identifies several recurring patterns throughout the criminal process.

Stage 1: Preparation

During the preparation phase, criminal networks consistently exploited legal and regulatory **vulnerabilities** at both the sectoral and business levels. Low barriers to market entry, cash-intensive business models, administrative complexity, and fragmented supervision frequently created opportunities for the criminal use of the legitimate economy. At the level of individual enterprises, legal structures such as (private) limited companies and limited partnerships appeared particularly attractive due to their flexibility and relatively limited transparency requirements.

Stage 2: Pre-activity or enabling conditions

During the pre-activity phase, legitimate businesses were either established directly by criminal actors or acquired and subsequently infiltrated. The use of straw persons, nominee directors, and figureheads emerged as a recurring strategy for concealing beneficial ownership and distancing key actors from criminal activities. Many cases additionally highlighted the important role of **facilitators** and intermediaries, including accountants, lawyers, notaries, consultants, and logistics specialists. Their involvement ranged from the provision of legitimate professional services to active and intentional participation in criminal schemes. In some instances, cooperation also appeared to have been facilitated through intimidation or coercion.

Stage 3: Activity

The activity phase revealed a wide variety of methods through which criminal networks used, managed, and exploited legitimate businesses. Although the specific *modus operandi* differed considerably across cases, sectors, and jurisdictions, several recurring patterns emerged from the comparative analysis. Most notably, **money laundering** constituted a central function of many of the businesses involved. Criminal proceeds were integrated into the legal economy through a diverse range of laundering techniques, including trade-based money laundering schemes, the strategic manipulation of financial transactions and business revenues, and the use of complex corporate structures. Across multiple cases, fictitious invoices and artificially created revenue streams were used to disguise the origin of illicit funds. Examples included the creation of fictitious restaurant bookings, fabricated rental income, and fraudulent employment arrangements. In addition, several cases highlighted the use of cash compensation schemes and alternative value transfer mechanisms to conceal financial flows and circumvent formal controls. Furthermore, the case studies also revealed a range of more context-specific laundering methods. Criminal proceeds were, for example, invested in

luxury goods or laundered through practices such as 'house flipping', whereby properties were rapidly bought and resold in order to integrate illicit funds into apparently legitimate financial transactions. While the specific techniques varied, the cases demonstrate the ability of criminal actors to adapt existing commercial practices and legal business structures.

A particularly notable finding concerns the emergence of specialised laundering services operating within the broader criminal landscape. Several cases revealed how criminal networks used legitimate business structures and financial infrastructures not only to launder their own proceeds, but also to provide money-laundering services to other criminal actors. In these instances, the networks functioned as specialised service providers, thereby occupying a facilitating role within the wider criminal economy. This finding suggests that parts of the legitimate economy can increasingly display characteristics of a **'crime-as-a-service'** model. Such arrangements reduce the need for individual networks to develop their own laundering infrastructures and, at the same time, complicate law enforcement responses.

Beyond money laundering, the analysis demonstrated a broader convergence between licit and illicit economic activities, as legitimate businesses were rarely used exclusively for criminal purposes. Instead, many companies continued to conduct **genuine economic activities** while simultaneously facilitating criminal operations. In certain cases, most notably in Italy, evidence points to the active governance of the legitimate economy. This illustrates how legitimate enterprises can function as 'dual-use' structures, combining lawful and illicit commercial activities. Furthermore, across the case studies, businesses were repeatedly used to facilitate a broad range of criminal activities, including drug production and trafficking, fiscal and social fraud, VAT fraud, the smuggling of illicit goods, and acts involving violence, intimidation, and coercion. These findings are consistent with previous research demonstrating that legitimate businesses frequently function as enabling structures for organised crime (Janssens et al., 2023; Savona & Riccardi, 2018).

Finally, the findings underscore the highly **adaptive nature of criminal networks**. The methods identified across the cases should therefore not be interpreted as fixed or static. Criminal actors continuously adjust their strategies and operational techniques in response to changing regulatory environments, law enforcement practices, and technological developments. As a result, the criminal use of the legitimate economy should be understood as a dynamic process characterised by ongoing innovation and adaptation. The resilience and flexibility of these networks imply that successful disruption efforts may generate displacement effects rather than permanently eliminating criminal opportunities. This dynamic was captured by one Belgian respondent:

> "*They will always look for another route. You can make it difficult for them, that is true, but then we must also be aware that an alternative will emerge, and that we will probably again need some time to detect that system*."[45] [R8_BE]

[45] Original quotation in Dutch: "Ze gaan altijd een andere weg zoeken. Je kunt het hen moeilijk maken, dat is waar. Maar dan moeten we er ons ook wel van bewust zijn dat er een alternatief gaat komen, en dat we terug waarschijnlijk een tijd nodig gaan hebben om dat systeem te detecteren."

Stage 4: Post-activity or post-conditions

The case studies also identified a range of recurring '**indicators'** associated with the criminal use of legitimate businesses (i.e., 'red flags'), including unusual cash transactions, the use of straw persons, missing tax filings, incomplete accounting records, complex corporate structures, and vague or unverifiable invoicing arrangements. While none of these indicators are necessarily indicative of criminal activity when considered in isolation, their recurrent presence across cases underscores their potential value as signals for risk assessment, monitoring, and the prioritisation of investigative efforts.

At the time of analysis, several investigations and judicial proceedings remained ongoing, whereas a number of cases had already resulted in the identification, prosecution, and/or conviction of multiple network members. Nevertheless, across the analysed cases, law enforcement authorities frequently encountered **significant challenges** during both operational interventions and subsequent (financial) investigations. These difficulties were often associated with the complexity of the criminal networks involved, including the use of intermediaries and layered organisational structures. In addition, the transnational nature of organised crime, with activities spanning multiple jurisdictions, posed further obstacles for investigators (cf. *infra*).

14.1.4 Financial characteristics of criminal networks

The financial analysis demonstrated that criminal networks rely on highly diverse funding structures, payment mechanisms, and revenue models. In many cases, initial investments originated from proceeds generated through earlier criminal activities, particularly drug trafficking and fraud. Cash remained a prominent financing mechanism, despite ongoing efforts to increase financial transparency. The analysis further showed that criminal enterprises incur significant operational costs associated with maintaining the appearance of legitimate business activities. These included company formation and acquisition costs, administrative expenses, payments to facilitators and straw persons, falsified documentation, logistical expenditures, (encrypted) communication infrastructure, and other investments necessary to sustain criminal operations. Such findings reinforce the observation that organised crime increasingly operates according to entrepreneurial and **business-oriented principles**, combining illicit profit generation with sophisticated forms of economic management.

14.1.5 Harms associated with the criminal use of legitimate businesses

Across the 28 case studies, harms associated with the criminal use of legitimate businesses were identified at several levels: individuals, other businesses, public institutions, the physical environment, and the wider social environment. Although the nature and severity of these harms varied between cases, several recurring patterns can be observed.

Harm to individuals

Across cases, individuals are primarily harmed through labour precarity, exposure to coercion and intimidation, and, where violence occurs, physical risk and psychological trauma. Undeclared or otherwise informal employment arrangements recurrently deprive workers of enforceable rights and social protection, including social security coverage, pension accrual, and protection in cases of non-payment. They may also increase workers' dependency on employers and thereby heighten their vulnerability to exploitation. In addition, workers may be exposed to unsafe or otherwise inadequate working conditions where businesses do not comply with relevant employment and safety standards.

These risks can be particularly pronounced among vulnerable groups, including individuals experiencing addiction or financial difficulties, as well as people who are dependent on care. Their circumstances may make them more susceptible to exploitation and coercion. In some cases, children were also involved in or affected by the criminal use of businesses. More broadly, threats, intimidation, and violence associated with criminal activity can expose both employees and other individuals connected to the business to physical and psychological harm.

Harms to other businesses

The predominant harm to other businesses is the distortion of fair competition. Legitimate businesses may be placed at a structural competitive disadvantage when other businesses evade taxes and social contributions, circumvent regulatory requirements, manipulate the system, or use criminal proceeds to finance their activities. Access to illicit capital and the ability to avoid costs that compliant businesses are required to bear can allow criminally involved businesses to offer lower prices or otherwise operate under conditions that are not available to legitimate competitors. This undermines fair market principles and may contribute to the displacement of compliant businesses.

In addition to these direct competitive effects, criminal use of legitimate businesses can generate reputational and operational spillovers. Legitimate businesses may suffer reputational damage when criminal activity becomes associated with their sector, while commercial relationships, transactions, shipments, or subcontracting arrangements may become subject to additional scrutiny or disruption when they are exploited by criminal networks. These effects can impose additional costs and undermine confidence between businesses within the sector.

Harm to public institutions

Public institutions are harmed primarily through material financial losses. Tax evasion and the non-payment of social contributions reduce public revenues and therefore diminish the resources available for public expenditure. Across several cases, substantial amounts of public money were lost through fraudulent or otherwise illicit practices. At the same time, investigating and responding to criminal use of legitimate businesses can require considerable financial and human resources from law enforcement, supervisory authorities, and other public institutions. This creates an additional burden on public institutions beyond the direct financial losses caused by the underlying criminal activity.

A further harm concerns institutional credibility and public trust. Where criminal schemes are able to operate for extended periods without detection, or where public financial or regulatory systems are themselves exploited, this may undermine public confidence in the effectiveness of oversight and enforcement mechanisms. More broadly, the perception that businesses can operate outside established rules without consequence may erode trust in public institutions and, in some cases, in the criminal justice system.

Harms to the physical environment

Not all case studies provided direct evidence of harm to the physical environment. Nevertheless, several cases indicate that the criminal use of legitimate businesses can create or exacerbate physical and environmental risks. These may arise, for example, where business premises are used for illicit activities that carry risks of fire or explosion, potentially endangering surrounding properties and infrastructure. Criminal use may also be associated with physical deterioration or damage to business premises where properties are neglected or used for illicit purposes. Depending on the nature of the

criminal activity, environmental harm may also arise through the improper disposal or dumping of waste and other practices used to facilitate or conceal illicit activities.

Harms to the social environment

At the level of the wider social environment, recurring harms include the normalisation of illegality, increased fear and insecurity, and the erosion of trust in businesses, markets, and public institutions. The visible presence of criminal activity within otherwise legitimate commercial settings may blur the distinction between legitimate and illegitimate economic activity and contribute to the perception that criminal practices are embedded within the local economy. Where such practices become sufficiently widespread or socially tolerated, they may contribute to the normalisation of illegality within the legitimate economy.

Violence, threats, intimidation, and other forms of criminal activity can further undermine perceptions of public order and safety, particularly among residents and other local stakeholders. They may contribute to an increased sense of insecurity and, in some contexts, create wider risks to public health, for example where legitimate business premises are used in connection with drug production or trafficking. Intimidation may also discourage individuals from reporting criminal activity or acting as whistleblowers, thereby further limiting informal and formal mechanisms of social control.

Finally, the criminal use of businesses can undermine confidence in regulatory, supervisory, and judicial processes. Where criminal activity is perceived to persist despite existing oversight mechanisms, this may weaken confidence in the ability of public institutions to maintain a fair and secure economic environment. In some contexts, public exposure of criminal activity may also carry a risk of broader stigmatisation if criminal practices become associated in public discourse with particular sectors or communities.

14.2 Limitations of the study

Several methodological and substantive limitations should be considered when interpreting the findings presented in this report. Although the comparative analysis provides valuable insights into the ways in which criminal networks use the legitimate economy, the findings are best understood as illustrative of broader patterns and mechanisms, rather than as universally generalisable conclusions.

Limitation 1 – Unequal access to investigative and judicial data

A first limitation concerns access to primary data. The quality and depth of the case studies varied across jurisdictions, partly due to differences in access to judicial and law enforcement information. In some instances, law enforcement authorities appeared reluctant to share data or provide concrete information on specific criminal networks operating within their jurisdiction. Furthermore, while some research teams were granted access to extensive judicial case files, others relied predominantly on expert interviews, publicly available court records, intelligence reports, or open-source information. Consequently, the **empirical basis differs between cases** and countries, affecting the level of detail that could be obtained regarding criminal structures, financial flows, operational costs, revenues, and organisational processes. Moreover, judicial and police files do not provide a complete representation of criminal activity, but rather reflect investigative priorities and strategic decisions made by law enforcement agencies and prosecutors.

Limitation 2 – Subjectivity in the identification of vulnerable (sub)sectors

A second limitation relates to the selection and identification of vulnerable economic (sub)sectors. The sectors examined in the study were identified through a combination of case analyses and consultations with local stakeholders. As a result, the designation of certain sectors as particularly vulnerable is informed, at least in part, by the perspectives, experiences, institutional responsibilities, and priorities of the actors consulted. Vulnerability should therefore not be understood as an entirely objective or inherent characteristic of a sector, but rather as a concept that is, to some extent, socially and **institutionally constructed**. Authorities operating in different contexts may identify different sectors as particularly vulnerable or problematic, depending on local circumstances, available intelligence, regulatory frameworks, and prevailing policy priorities. Accordingly, the findings should be interpreted as indicative patterns of perceived and observed vulnerability, rather than as establishing a definitive 'hierarchy' of vulnerable economic (sub)sectors.

Limitation 3 – Limits of a sector-based perspective

Related to the previous limitation, the study highlights a broader conceptual challenge associated with a predominantly sector-based approach. While certain economic (sub)sectors recurred across the cases analysed, the findings suggest that criminal networks are often less dependent on specific sectors as such than on the opportunities and functions that businesses can provide (cf. *supra*). Similar mechanisms of criminal use were observed across sectors that differ substantially in terms of their economic activities and organisational characteristics. As one Belgian respondent noted:

> *"(…) It doesn't matter what the sector is underneath. It's a modus operandi. You can set parameters on the companies. (…) But if you just focus on sectors, you'll always end up with the same ones: hospitality, service provision, and so on."*[46] [R1_BE]

Consequently, a focus on economic (sub)sectors may risk obscuring the broader structural vulnerabilities and cross-sectoral mechanisms that enable or facilitate the criminal use of the legal economy. The findings therefore point towards a more nuanced understanding of vulnerability, in which sector-specific characteristics are considered alongside organisational, regulatory, and administrative opportunity structures.

Limitation 4 – Focus on local-level case studies

A fourth limitation stems from the study's emphasis on local contexts. The research design intentionally focused on city-level case studies in order to capture local manifestations of criminal use and generate context-sensitive insights. While this approach constitutes an important strength of the study, it also entails certain limitations. Criminal networks frequently operate across regional, national, and international boundaries, whereas the case studies necessarily concentrated on specific cities and jurisdictions. As a result, certain **transnational dimensions** of criminal activities, including international financial flows, foreign business interests, and links to actors and networks operating beyond the jurisdictions under investigation (e.g., South American drug cartels), may have remained only partially visible. The local focus therefore provides an important, context-sensitive perspective on criminal ecosystems, but cannot fully capture their broader (transnational) dimensions.

[46] Original quotation in Dutch: "Het maakt niet uit wat de sector is die eronder zit. Het is een *modus operandi*. Je kunt wel parameters trekken op de vennootschappen. (…) Maar gewoon puur focussen op sectoren? Dan gaat het altijd op dezelfde dingen uitkomen. Dan gaat het altijd op de horeca uitkomen, op dienstverlenende sectoren, enzovoort."

Furthermore, comparability across jurisdictions is inherently constrained by differences in legal frameworks, regulatory structures, investigative practices, data availability, and criminal justice procedures. The cases examined in this study are embedded in distinct local and national contexts, which shape both the opportunities available to criminal actors and the responses of relevant authorities. Consequently, observed similarities should not necessarily be interpreted as evidence of identical underlying dynamics, while observed differences may, at least in part, reflect contextual variations rather than substantive differences in the criminal phenomena.

Limitation 5 – Analytical constraints of Crime Scripting

An additional methodological limitation concerns the use of Crime Scripting as an analytical framework. Although this approach proved valuable for structuring the comparative analysis and identifying recurring patterns across different stages of the criminal process, the distinction between these phases should be understood as an **analytical construct** rather than as a precise representation of how criminal activities unfold in practice. In reality, such activities often develop through fluid, overlapping, and iterative processes. Organised criminal operations do not necessarily follow clearly delineated stages, and networks may move between different activities or 'revisit' earlier stages in response to changing opportunities or enforcement pressures. Moreover, crime scripts provide a representation of criminal processes at a particular point in time and may therefore not fully capture the adaptive and evolving nature of organised crime.

Limitation 6 – Inherent complexity of criminal networks

Finally, several substantive limitations arise from the inherent complexity of criminal networks themselves. Due to the clandestine nature of serious organised crime, criminal networks often remain largely below the radar of law enforcement agencies, making it inherently difficult to assess their size, scale, and overall scope (Hulme et al., 2021). The available evidence therefore often provided only **partial visibility** into internal decision-making processes, power relations, financial arrangements, and organisational hierarchies. In many cases, the relative importance of individual actors could only be inferred from their prominence in investigative files, creating a potential risk of selection bias. Similarly, the role of facilitators, professional intermediaries, and associated businesses could not always be established with certainty.

A related limitation concerns the **estimation of criminal proceeds**. The financial figures presented in this report should generally be regarded as conservative estimates, as they are often based on amounts that could be substantiated through the available evidence and may therefore represent only a minimum proven amount rather than the full extent of criminal earnings. Taken together, these limitations suggest that the observable elements of criminal networks – and the financial proceeds that can be documented – are unlikely to provide a complete representation of their actual structure, scale, or operational reality.

14.3 Implications and recommendations for policy and practice

The findings of this study demonstrate that organised crime and the legitimate economy are closely interconnected. Effective responses therefore require approaches that extend beyond traditional crime-control strategies and address the financial, administrative, regulatory, and economic dimensions of criminal activity. Alongside the context-specific recommendations for each city and country examined, as discussed earlier in the report, the findings also point to several broader implications that emerge across the jurisdictions studied.

Recommendation 1 – Prioritise the financial dimension of organised crime

A first recommendation is to place greater emphasis on the financial dimensions of organised crime. Across the case studies, financial gain emerged as the principal driver of the criminal use of legitimate businesses. Nevertheless, financial investigations often receive less attention and lower priority than investigations focusing on drug trafficking, violence, or other more visible manifestations of organised crime. The analysis indicates that **financial investigations** should not be treated as secondary to other investigative activities, but rather integrated as a parallel and complementary investigative track from the outset. Following financial flows can provide valuable insights into the broader organisational structure of criminal networks and may help identify facilitators and supporting infrastructures.

Recommendation 2 – Strengthen and modernise financial investigative capacities

Relatedly, the analysis highlights the need to strengthen and modernise financial investigative capacities. Although 'traditional' investigative tools remain indispensable in the fight against organised crime, they are often insufficient to uncover and dismantle the increasingly complex financial structures through which criminal networks operate. The findings highlight the considerable adaptability of criminal actors, who continuously adjust their methods in response to regulatory changes, technological developments, and enforcement efforts. Consequently, greater investment is needed in specialised financial investigation capabilities. This includes strengthening **expertise** in emerging technologies and financial instruments, such as cryptocurrencies, digital payment systems, and other alternative value-transfer mechanisms. Alongside continuous professional training, specialised investigative techniques, such as communication interception and covert observation, should be more systematically integrated in financial investigations.

Recommendation 3 – Increase scrutiny of cash-intensive business environments

The findings further underline the importance of maintaining attention to cash-intensive economic activities. Although digital payment systems have become increasingly widespread, cash continues to play a significant role in many of the cases analysed, particularly in relation to money laundering and the concealment of criminal proceeds. Economic sectors in which substantial cash transactions remain common may therefore warrant enhanced scrutiny. Policymakers should consider whether existing regulatory frameworks provide adequate safeguards against abuse and whether additional measures could further reduce opportunities for the concealment of illicit financial flows.

Recommendation 4 – Strengthen the administrative approach

A further recommendation concerns strengthening administrative approaches to organised crime. The case studies indicate that criminal justice interventions alone may not always be sufficient to disrupt the broader infrastructures that sustain criminal business models. Administrative measures, including licensing procedures, permit systems, inspections, and regulatory interventions, can provide additional opportunities to identify and disrupt the criminal use of legitimate businesses. In this regard, administrative authorities and local governments may play an important complementary role alongside law enforcement and judicial actors.

Recommendation 5 – Strengthen asset recovery, seizure, and confiscation mechanisms

The findings also highlight the importance of asset seizure, confiscation, and asset recovery measures. Given the fundamentally profit-driven nature of organised crime, interventions targeting illicit gains may help to weaken the economic foundations of criminal activity. Depriving criminal actors of their assets may reduce the attractiveness of using legitimate businesses for criminal purposes and potentially disrupt the cost-benefit calculations that underpin many criminal enterprises. Strengthening asset recovery mechanisms and their consistent application across jurisdictions may therefore contribute to more effective disruption of the economic foundations of organised crime.

Recommendation 6 – Enhance European and international cooperation

Given the transnational nature of many of the cases analysed, enhanced international cooperation is particularly important. Criminal networks often operate across multiple jurisdictions, while legal frameworks, regulatory requirements, and investigative powers may vary considerably across countries. Such differences can create opportunities for regulatory arbitrage and may, in some cases, hinder timely cooperation between competent authorities. Greater alignment of relevant legal and regulatory frameworks at the European level, alongside more efficient mechanisms for intelligence sharing, information exchange, and joint investigations, could strengthen the collective capacity to address the criminal use of the legitimate economy.

Recommendation 7 – Promote multidisciplinary information sharing and joint action

Finally, the findings highlight the value of multidisciplinary approaches. The complexity of contemporary criminal business models requires expertise, information, and investigative powers that are often distributed across multiple institutions. Closer cooperation between law enforcement agencies, financial intelligence units, prosecutors, tax authorities, customs services, regulatory inspectors, supervisory bodies, financial institutions, and local administrations is therefore essential. Enhanced information sharing, greater interoperability between databases, and the development of multidisciplinary investigative structures could help reduce fragmentation and improve the identification of links between criminal actors, businesses, and financial flows.

Overall, the findings indicate that approaches focused solely on criminal prosecution are unlikely to be sufficient. The increasing integration of organised crime into legitimate economic structures calls for a **comprehensive, multidimensional response** that combines criminal, financial, administrative, regulatory, and preventive measures. An integrated approach of this kind may enhance the capacity of relevant authorities to identify, disrupt, and prevent the criminal use of the legitimate economy.

BIBLIOGRAPHY

References

Alexandrova-Zorina, L. (2023). Imperiets barn. *Volante.* https://volante.se/bocker/imperiets-barn/

Alexandrova-Zorina, L. (2025). De livegnas land: Den undre världen som bygger Sverige. *Volante*. https://volante.se/bocker/de-livegnas-land/

Algemene Directie Veiligheid & Preventie. (n.d.). *Brochure ARIEC Antwerpen.* Retrieved from https://www.besafe.be/sites/default/files/2023-04/Brochure%20ARIEC%20Antwerpen.pdf

Anderson, A. (1995). *Organised crime, mafia and governments*. Cambridge University Press.

Anti-Corruption Fund [ACF]. (2024, August 5). *Lords of the Dust: Who are the Patrons of a Parallel Construction Waste Removal Scheme in Sofia?* Retrieved from https://acf.bg/en/vlastelinite-na-prastta-koi-sa-pokrov/

Bezlov, T., & Gounev, P., Petrunov, G., Tzenkov, E., & Tzvetkova, M. (2007). *Organized crime in Bulgaria: Markets and trends.* Center for the Study of Democracy (CSD). https://csd.eu/fileadmin/user_upload/publications_library/files/2007/2007_01_ENG_Organized_Crime_in_Bulgaria.pdf

BNT News. (2023, July 4). *90% of fast loan firms in Bulgaria violate the rights of customers*. Bulgarian National Television: News. Retrieved from https://bntnews.bg/news/90-of-fast-loan-firms-in-bulgaria-violate-the-rights-of-customers-1305097news.html

Boelens, M., & Groothuis, S. (2020). *Weerbare boeren in een kwetsbaar gebied: Over drugscriminaliteit en ondermijnende effecten daarvan op boeren en tuinders*. Zuidelijke Land- en Tuinbouworganisatie (ZLTO); Aanjaagteam Ondermijning (ATO). https://open.overheid.nl/documenten/ronl-970c5dd4-5bc2-4720-ae93-399d44a40d77/pdf

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017; Georganiseerde criminaliteit*. Politie Nederland, Dienst Landelijke Informatieorganisatie. https://www.politie.nl/binaries/content/assets/politie/onderwerpen/nationaal-dreigingsbeeld/2017/71fc2512-2641-42b2-ac16-2c6e36bc1ada.pdf

Booth, R. (2018, April 18). NHS workers top list of those applying for payday loans. *The Guardian*. https://www.theguardian.com/money/2018/apr/18/nhs-workers-top-list-of-those-applying-for-payday-loans

Bruinsma, G., & Bernasco, W. (2004). Criminal groups and transnational illegal markets. *Crime, Law and Social Change, 41*(1), 79-94. https://doi.org/10.1023/B:CRIS.0000015283.13923.aa

Brussels Hoofdstedelijk Gewest. (n.d.). *Licenties, vergunningen en toegang tot het beroep*. Retrieved from https://be.brussels/nl/ondernemen-innoveren/ondernemen-brussel/licenties-vergunningen-en-toegang-tot-het-beroep#main

Brussels Instituut voor Statistiek en Analyse [BISA]. (2026). *Ondernemingen*. Retrieved May 12, 2026, from https://bisa.brussels/themas/economie/ondernemingen

Brå (2022). *Välfärdsbrott mot kommuner och regioner. Fel och oegentligheter bland företag och föreningar.* Brottsförebyggande Rådet. https://bra.se/download/18.366598ab19270941a1c3b2b/1729259835797/2022%201%20Valf%C3%A4rdsbrottslighet%20mot%20kommuner%20och%20regioner.pdf

Brå. (2011). *Storskaliga skattebrott - En kartläggning av skattebrottslingens kostnader*. Brottsförebyggande Rådet. https://bra.se/download/18.24d9e8f019301e61bb7370a/1731086557312/2011_storskaliga_skattebrott.pdf

Brå. (2016). *Kriminell infiltration av företag; Rapport 2016:10*. Brottsförebyggande Rådet. http://bra.se/download/18.660677dc19301da04632739/1730989788238/2016_10_Kriminell%20infiltration%20av%20f%C3%B6retag.pdf

Brå. (2019). *Penningtvättsbrott: En uppföljning av lagens tillämpning*. Brottsförebyggande Rådet. https://bra.se/download/18.1537f1c6192bd251bfc3af2/1730202793067/2019_17_Penningtvattsbrott.pdf

Brå. (2021). *Finansiering av terrorism: En studie av motåtgärder*. Brottsförebyggande Rådet. https://bra.se/download/18.1537f1c6192bd251bfc1137/1729842834318/2021_6_Finansiering_av_terrorism.pdf

Brå. (2023). *Barn och unga i kriminella nätverk: En studie av inträde, brott, villkor och utträde.* Brottsförebyggande Rådet. https://bra.se/download/18.3808406a192bd2f0b723548/1730213224915/2023_13-Barn-och-unga-i-kriminella-natverk.pdf

Brå. (2024). *Möjliggörare för kriminella nätverk. Om möjliggörare i kommunal, statlig och privat sektor; Rapport 2024:2*. Brottsförebyggande Rådet. https://bra.se/download/18.3ad2ec4c19329a0a7e599c1/1732088255882/2024_2_Mojliggorare-for-kriminella-natverk.pdf

Brå. (2025). *Företag som brottsverktyg. Upplägg, systemsårbarheter och kopplingar till den kriminella miljön; Rapport 2025:20*. Brottsförebyggande Rådet. https://bra.se/download/18.51af66dd19afd01636541b6/1765461166378/2025_20_F%C3%B6retag%20som%20brottsverktyg.pdf

Bulgarian National Bank (2025a). *Статистика на банкнотите и монетите в левове [Statistics on Banknotes and Coins in Levs].* https://www.bnb.bg/NotesAndCoins/NACStatisticsNC/index.htm?toLang=_EN

Bulgarian National Bank. (2025b, December 23). *2025: Парични, депозитни и кредитни показатели [2025: Monetary, Deposit and Credit Indicators].* https://www.bnb.bg/AboutUs/PressOffice/POStatisticalPressReleases/POPRSMonetarySurvey/index.htm?toLang=_EN

Bundeskriminalamt [BKA]. (2025). *Bundeslagebild Organisierte Kriminalität 2024*. BKA. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2024.html?nn=27988

Bäuerle, M. (2025). hessenDATA in rechtssoziologischer Perspektive – Rechtsstaatliche Aspekte der automatisierten Datenanalyse durch die hessischen Polizeibehörden. In M. Bäuerle, K. Denker, C. Geminn, & B. Schöndorf-Haubold (Eds.), *Big Data und KI bei der Polizei: Das Palantir-Urteil in der interdisziplinären Diskussion* (pp. 213–224). Campus Verlag.

Campana, P. (2016). Explaining criminal networks: Strategies and potential pitfalls. *Methodological Innovations, 9*, 1-10. https://doi.org/10.1177/2059799115622748

Capital. (2026, January 14). *Годината преди еврото постави 3-годишен рекорд по сделки с жилища и земи [The year before the euro set a 3-year record for housing and land transactions].* Retrieved from https://www.capital.bg/biznes/imoti/2026/01/14/4872408_godinata_predi_evroto_postavi_3-godishen_rekord_po/

Center for the Study of Democracy [CSD]. (2020). *Bulgarian Organised Crime Threat Assessment 2020*. https://csd.eu/publications/publication/bulgarian-organised-crime-threat-assessment-2020/

Centraal Bureau voor de Statistiek [CBS]. (2026a, 1 June). *AZW Dashboard.* Retrieved from https://www.cbs.nl/nl-nl/dossier/arbeidsmarkt-zorg-en-welzijn/azw-dashboard

Centraal Bureau voor de Statistiek [CBS]. (2026b, 20 April). Vestigingen van bedrijven; bedrijfstak, regio. *CBS StatLine*. Retrieved from https://opendata.cbs.nl/#/CBS/nl/dataset/81578NED/table?ts=1781170344230

Centrum voor Criminaliteitspreventie en Veiligheid [CCV]. (2026, 4 February). *Digitaal Opkopers Register (DOR).* Retrieved from https://hetccv.nl/themas/high-impact-crimes/heling/digitaal-opkopers-register-dor/

Chiu, Y., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *British Journal of Criminology*, *51*(2), 355–374. https://doi.org/10.1093/bjc/azr005

Colman, C. (2018). Naar een geïntegreerde aanpak van de invoer en doorvoer van cocaïne via de haven via Antwerpen. *Panopticon, 39*(2), 130–140.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R.V. Clarke (Ed.), *Crime Prevention Studies* (pp. 151-196). Criminal Justice Press.

CTIF-CFI. (2019). *26ste activiteitenverslag; 2019*. https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/2019.pdf

CTIF-CFI. (2021a). *Activiteitenverslag 2021*. https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/CFI_JAARVERSLAG_2021-DEF.pdf

CTIF-CFI. (2021b, January 6). *Use of the corporate structure of a partnership (société en nom collectif or SNC).* Retrieved from https://www.ctif-cfi.be/index.php/en/previous-warnings/203-use-of-snc

CTIF-CFI. (2022). *Activiteitenverslag 2022*. https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/JV2022NL.pdf

CTIF-CFI. (2023). *Samenvatting van de Nationale risicoanalyse witwassen van geld (Update 09/2023)*. https://www.ctif-cfi.be/images/documents/Dutch/NRA_2023_Samenvatting_ML.pdf

CTIF-CFI. (2024a). *Activiteitenverslag 2024*. https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/CTIF-CFI_JV24_NL_2024.pdf

CTIF-CFI. (2024b). *Vademecum: Typologieën van schema's voor het witwassen van geld vastgesteld door de CFI*. https://www.ctif-cfi.be/images/documents/Dutch/Vademecum_witwassen_van_geld.pdf

De Schutter, A. (2024). Drugsgeweld in België: Intimidatie, reputatie en de onderwereld. Vlaams Vredesinstituut. https://vlaamsvredesinstituut.eu/wp-content/uploads/2024/12/20241203-VVI-rapport-drugsgeweld_BE_-web.pdf

Degen, W. (2026a, 28 March). Ein "Unternehmer" der speziellen Art. Ein Albaner und seine Komplizen stehen in Wiesbaden vor Gericht. Es geht um bandenmäßigen. Drogenhandel. Der 32-Jährige "Ridi" organisierte die Einfuhr am Frankfurter Flughafen. *Wiesbadener Kurier*, p. 13.

Degen, W. (2026b, 27 April). Wenn bei "Ridi" das Interesse erwacht. Wie eine albanische Bande die Schwachstelle der menschlichen Gier bei Frachtfirma-Mitarbeitern genutzt hat. Einblicke gibt ein Drogenprozess am Landgericht Wiesbaden. *Wiesbadener Kurier*, p. 11.

Denislova, V. & Minkov, V. (2025, April 11). *Неформалната икономика в България: 34.6% сиво [The Informal Economy in Bulgaria: 34.6% In the Shadows]*. Capital. https://www.capital.bg/politika_i_ikonomika/ikonomika/2025/04/11/4768068_neformalnata_ikonomika_v_bulgartiia_346_sivo/

Deutsche Bundesbank. (2025, April 22). *Current opinions on the role of cash in German society. Monthly Report – April 2025*. Retrieved from https://publikationen.bundesbank.de/publikationen-en/reports-studies/monthly-reports/monthly-report-april-2025-954672?article=current-opinions-on-the-role-of-cash-in-german-society-954666

Dimitrova, R., & Toteva, E. (2026, January 22). *Share of Housing Transactions with Buyers' Own Funds in Sofia Increase by End 2025.* Bulgarian News Agency. https://www.bta.bg/en/news/economy/1048737-share-of-housing-transactions-with-buyers-own-funds-in-sofia-increase-by-end-20

Direzione Investigativa Antimafia [DIA]. (2024). *Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia: Primo semestre 2024.* Ministero dell'Intern.

Ekobrottsmyndigheten. (2020). *Ekobrottsmyndighetens lägesbild om ekonomisk brottslighet i Sverige.* Ekobrottsmyndigheten; Swedish Economic Crime Authority. https://www.ekobrottsmyndigheten.se/wp-content/uploads/2021/10/ekobrottsmyndighetens-lagesbild-om-ekonomisk-brottslighet-i-sverige-2020-webb.pdf?_gl=1*pm6csw*_up*MQ..*_ga*MTQ4MTYxMjI1Ny4xNzc3MTIyMDk4*_ga_76KDTL233E*czE3NzcxMjIwOTgkbzEkZzAkdDE3NzcxMjIwOTgkajYwJGwwJGgw

Ekobrottsmyndigheten. (2025). *Ekonomisk brottslighet: Ekobrottsmyndighetens Lägesbild 2025*. Ekobrottsmyndigheten; Swedish Economic Crime Authority. https://www.ekobrottsmyndigheten.se/wp-content/uploads/se/2025/05/ebm-lagesbild-2025.pdf?_gl=1*1aqwe2l*_up*MQ..*_ga*MTYxNDg1MTI5Ny4xNzg0MzAwODEz*_ga_76KDTL233E*czE3ODQzMDA4MTMkbzEkZzAkdDE3ODQzMDA4MTMkajYwJGwwJGgw

European Commission. (2023a). *Communication from the Commission to the European Parliament and the Council on the EU Roadmap to fight drug trafficking and organised crime (COM/2023/641 Final).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0641

European Commission. (2023b). *Study on the effectiveness of policies to tackle undeclared work (VT/2021/0380) – Final report.* Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/94ca6bed-2c25-11ee-95a2-01aa75ed71a1/language-en

European Court of Auditors. (2015). *Tackling intra-Community VAT fraud: More action needed.* (Special Report No. 24/2015). https://www.eca.europa.eu/lists/ecadocuments/sr15_24/sr_vat_fraud_en.pdf

European Crime Prevention Network [EUCPN]. (2018). *CONFINE: Towards operational cooperation on local administrative financial investigations in the fight against human trafficking.* https://eucpn.org/sites/default/files/document/files/confine_manual_eng.pdf

European Monitoring Centre for Drugs and Drug Addiction [EMCDDA], & Europol. (2024). *EU drug markets analysis: key insights for policy and practice*. Publications Office of the European Union.

European Network on the Administrative Approach [EENA]. (2020). *3rd EU Handbook on the administrative approach in the European Union*. EENA. https://administrativeapproach.eu/sites/default/files/publication/files/2005_Third%20Handbook%20EU_ENG_LR_1.pdf

European Parliament. (2010, 30 September). *Waste crisis in Campania: Time to reduce, re-use and recycle*. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20100927IPR83723/waste-crisis-in-campania-time-to-reduce-re-use-and-recycle

Europol. (2016). *Does crime still pay? Criminal asset recovery in the EU. Survey of statistical information 2010-2014.* European Police Office. https://www.europol.europa.eu/cms/sites/default/files/documents/criminal_asset_recovery_in_the_eu_web_version.pdf

Europol. (2021). *European Union Serious and Organised Crime Threat Assessment. A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime.* Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Europol. (2022, 4 May). *EU Drug Markets Report: Latest analyses of Europe's drug markets by Europol and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)*. Retrieved from https://www.europol.europa.eu/publications-events/publications/eu-drug-markets-report

Europol. (2023a, 5 April). *Criminal networks in EU ports: Risks and challenges for Law Enforcement. Focus on the misappropriation of container reference codes in the ports of Antwerp, Hamburg and Rotterdam.* Retrieved from https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement

Europol. (2023b). *European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime.* Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf

Europol. (2024a). *Decoding the EU's most threatening criminal networks.* Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks

Europol. (2024b). *Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures.* Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/leveraging-legitimacy-how-eu%E2%80%99s-most-threatening-criminal-networks-abuse-legal-business-structures

Europol. (2025). *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Europol. (2026). *Decoding the EU's most threatening criminal networks - Issue 2: The blueprint of criminal opportunism*. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/Blueprint-of-criminal-opportunism.pdf

Eurostat. (2023, January 6). *Statistics explained. Glossary: Economic activity.* Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Economic_activity#:~:text=An%20economic%20activity%20takes%20place,products%20(goods%20or%20services)

Evans, C. (2021, August 28). Online loans: 'I went from loaning £150 to owing £6,000 in months.' *BBC News*. https://www.bbc.com/news/uk-wales-58341915

Fair Play Bygg. (2025). *Årsrapport 2025*. https://fairplaybyggoslo.no/wp-content/uploads/2026/03/HM37626-Fair-Play-Bygg-arsrapport-2025-nett.pdf

Federale Politie. (2020, June 11). *KALI-team neemt inboedel van restaurant in beslag in Borgerhout.* Retrieved from https://www.politie.be/5998/nl/nieuws/kali-team-neemt-inboedel-van-restaurant-in-beslag-in-borgerhout

Federale Politie. (2024, January 25). *Diefstallen van paardenzadels – Eigenaars gezocht*. Retrieved from https://www.politie.be/opsporingen/nl/opsporingen/gezochte-eigenaars/diefstallen-van-paardenzadels-eigenaars-gezocht

Fernstädt, H. (1987). Organisierte Kriminalität – Auswirkung auf die Wirtschaft? In H.D. Schwind, G. Steinhilper, & E. Kube (Eds.), *Organisierte Kriminalität. Beiträge zu einer Fachtagung deer Deutschen Kriminologischen Gesellschaft und zur Verleihung der Beccaria-Medaille 1986* (pp. 55-60). Kriminalistik-Verlag.

Financial Action Task Force [FATF]. (2006). *Trade Based Money Laundering*. FATF; OECD. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf

Financial Action Task Force [FATF]. (2026). *Targeted Report on Stablecoins and Unhosted Wallets; Peer-to-Peer Transactions.* FATF; OECD. www.fatf-gafi.org/content/fatf-gafi/en/publications/virtualassets/targeted-report-stablecoins-unhosted-wallets

Financial Intelligence Unit Nederland. (2022, 14 July). *The gold dealer*. Retrieved from https://www.fiu-nederland.nl/en/knowledge_base/the-gold-dealer/

Fiscale Inlichtingen- en Opsporingsdienst [FIOD]. (2023, 20 June). *Miljoenenfraude in autobranche*. Retrieved from https://www.fiod.nl/miljoenenfraude-in-autobranche/

FOD Economie. (2024, 17 April). *Wettelijke beperkingen op betalingen met cash geld*. Retrieved from https://economie.fgov.be/nl/publicaties/wettelijke-beperkingen-op

Frankfurt Airport (n.d.). *Facts and Figures*. Retrieved from https://b2b.frankfurt-airport.com/en/cargo-hub/at-one-glance.html

Fyrk, J. (2020). *Svartjobbsfabriken*. Verbal Förlag.

Gemeente Utrecht. (2021, 16 September). *Utrechts offensief bestrijdt ontwrichtende effecten drugscriminaliteit.* Retrieved from https://www.utrecht.nl/nieuws/nieuwsbericht-gemeente-utrecht/utrechts offensief-bestrijdt-ontwrichtende-effecten-drugscriminaliteit

Gemeente Utrecht. (2022, 24 February). *Veiliger bedrijventerrein door vergunningplicht autobranche Nieuw Overvecht*. Retrieved from https://www.utrecht.nl/nieuws/nieuwsbericht-gemeente-utrecht/veiliger-bedrijventerrein-door-vergunningplicht-autobranche-nieuw-overvecht

Gemmer, K. (1983). Organisierte Kriminalität in der Bundesrepublik? *Archiv für Kriminologie, 171*(1), 1-8.

Gemmer, K. (1992). Frankfurt am Main – Die deutsche Hauptstadt des Verbrechens? *Archiv für Kriminologie, 190*(3-4), 65-71.

Georgiev, G., Petrova, V., & Tsabala, K. (2023). *Breaking the code: Tackling the interlocking nexus of Russian and Chinese disinformation and illicit financial flows in Southeast Europe*. Center for the Study of Democracy [CSD]. https://csd.eu/publications/publication/breaking-the-code/

Georgieva, T. (2025, January 31). *Комисията за защита на потребителите е установила 1147 неравноправни клаузи в 357 договора за бързи кредити [The Consumer Protection Commission has identified 1,147 unfair clauses in 357 payday loan contracts].* Banker.bg. Retrieved from https://banker.bg/2025/01/31/barzi-krediti/

GlasNews.bg. (2026, January 23). *Кои са задържаните в бандата за бързи кредити, лихварство и изнудване в София СНИМКИ [Who are the detainees in the gang for quick loans, usury and extortion in Sofia? PHOTOS].* Retrieved from https://glasnews.bg/krimi/koi-sa-zadarzhanite-bandata-barzi-krediti-lihvarstvo-i-589672/

Global Initiative Against Transnational Organized Crime [GI-TOC]. (2025a). *Criminal networks*. Retrieved from https://ocindex.net/crime/criminal-networks

Global Initiative Against Transnational Organized Crime [GI-TOC]. (2025b). *The Global Organized Crime Index: Criminality in Belgium.* https://ocindex.net/assets/downloads/2025/english/ocindex_profile_belgium_2025.pdf

Goranova, K. (2018, April 13). *Икономика след полунощ [Economy after mindnight]*.Capital. https://www.capital.bg/politika_i_ikonomika/bulgaria/2018/04/13/3162013_ikonomika_sled_polunosht/

Greenfield, V.A., & Paoli, L. (2022). *Assessing the Harms of Crime: A New Framework for Criminal Policy*. Oxford University Press.

Greenfield, V.A., Nuñez-Neto, B., Mitch, I., Chang, J., & Rosas, E. (2019). *Human smuggling and associated revenues: What do or can we know about routes from central America to the United States?* Homeland Security Operational Analysis Center [HSOAC]; RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2852/RAND_RR2852.pdf

Gunnarson, C. (2023). *Den sårbara staten: En forskningsöversikt om hur organiserad brottslighet påverkar stat och kommun*. SNS Förlag. https://cms-production.sns.se/app/uploads/2023/11/den-sarbara-staten.pdf

Hendrickx, K. (2024, February 7). *Bingokasten op café: 'Vaak spelen ze vier of vijf uur aan een stuk'*. BRUZZ. https://www.bruzz.be/actua/samenleving/bingokasten-op-cafe-vaak-spelen-ze-vier-vijf-uur-aan-een-stuk-2024-02-07

Hessisches Ministerium der Finanzen. (2025, 9 December). *Gegen Finanzkriminalität. Wie Hessens neues Gemeinsames Finanzermittlungszentrum Organisierte Kriminalität austrocknet*. Retrieved from https://finanzen.hessen.de/presse/wie-hessens-neues-gemeinsames-finanzermittlungszentrum-organisierte-kriminalitaet-austrocknet

Hessisches Ministerium für Wirtschaft, Energie, Verkehr, Wohnen und Ländlichen Raum [HMWVW]. (n.d.). *Viel beschäftigte Branche. Logistik in Hessen*. Retrieved from https://wirtschaft.hessen.de/wirtschaft/logistik

Hessisches Statistisches Landesamt. (2025, 23 October). *Pendlerpotenzial 2024: 62 Prozent der Hessinnen und Hessen nicht an ihrem Arbeitsort wohnhaft.* Retrieved from https://statistik.hessen.de/presse/pendlerpotenzial-der-hessinnen-und-hessen-2024

Het Nieuwsblad. (2019, May 28). *Celstraffen tot vier jaar voor heling van 28 gestolen luxewagens*. Retrieved from https://www.nieuwsblad.be/regio/antwerpen/regio-antwerpen/antwerpen/celstraffen-tot-vier-jaar-voor-heling-van-28-gestolen-luxewagens/57238209.html?utm_campaign=share&utm_medium=referral&utm_source=hyperlink

Houwen, J. (2023, October 11). Vier verdachten in cel na diefstallen van dure zadels over heel het land: buit bedraagt enkele honderdduizenden euro's. *Het Nieuwsblad*. https://www.nieuwsblad.be/regio/oost-vlaanderen/regio-gent/destelbergen/vier-verdachten-in-cel-na-diefstallen-van-dure-zadels-over-heel-het-land-buit-bedraagt-enkele-honderdduizenden-euro-s/54925710.html?utm_campaign=share&utm_medium=referral&utm_source=hyperlink

Hulme, S., Disley, E., & Blondes, E.L. (2021). *Mapping the risk of serious and organised crime infiltrating legitimate businesses: Technical annexes.* European Commission (Directorate-General for Migration and Home Affairs); Centre for the Study of Democracy (CSD); EY; Government Transparency Institute (GTI); Optimity Advisors; RAND Europe. https://op.europa.eu/en/publication-detail/-/publication/bd3cb673-879d-11eb-ac4c-01aa75ed71a1/language-en#

Informatieknooppunt Zorgfraude [IKZ]. (2024). *Rapport: Signalen fraude in de zorg 2023*. https://open.overheid.nl/documenten/e4c5f4ed-fc97-4013-a810-fe4cd8b665b1/file

Iskandar, K. (2025, 30 April). Polizei und Palantir. Eine Software, die fast alles weiß. *Frankfurter Allgemeine Zeitung [FAZ.NET]*. Retrieved from https://www.faz.net/aktuell/rhein-main/region-und-hessen/palantir-und-polizei-hessendata-als-vorbild-fuer-ganz-deutschland-110438575.html

Istituto Nazionale di Statistica [ISTAT]. (2024). Preliminary estimate of agricultural economic accounts | Year 2024. https://www.istat.it/wp-content/uploads/2025/01/Report_Preliminary_estimate_of_agricultural_economy_trend_2024.pdf

Istituto Nazionale Previdenza Sociale [INPS]. (2024). *Campania: Rendiconto Sociale Regionale 2024.* Comitato Regionale Campania; Direzione Regionale Campania; Il Consiglio di Indirizzo e Vigilanza. https://www.inps.it/content/dam/inps-site/pdf/dati-analisi-bilanci/rendiconti-sociali/2024/RSR_CAMPANIA_2024.pdf

Janssens, J., Wittevrongel, F., & Smet, T. (2023). *Risicoanalyse van Ondermijnende Criminaliteit - Criminalité Déstabilisante in Belgische economische sectoren (RISK OCD).* Institute for International Research on Criminal Policy (IRCP), Algemene Directie Veiligheid & Preventie, FOD Binnenlandse Zaken. http://hdl.handle.net/1854/LU-01HGZA764PH0PVYCMSXG99VBKC

Jeppson, H. (2024). *Arbetslivskriminalitet – Ett hot mot god produktionstillväxt*. Ansvar Säkerhet.

Kansspelcommissie. (n.d.-a). *Legale kansspelen: Cafés online.* Retrieved February 10, 2026, from https://gamingcommission.paddlecms.net/node/288

Kansspelcommissie. (n.d.-b). *Operatoren: Vergunningen*. Retrieved February 10, 2026, from https://www.gamingcommission.be/nl/operatoren/vergunningen

Kitanova, D. (2025, December 23). Митов обяви Task Force срещу изпирането на пари (ВИДЕО) [Mitov announced a Task Force against money laundering (VIDEO)]. *ActualNo.com.* https://www.actualno.com/politics/mitov-objavi-task-force-sreshtu-izpiraneto-na-pari-video-news_2536092.html

Kleemans, E.R., Brienen, M.E.I., & van de Bunt, H.G. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. Boom Juridische Uitgevers. https://repository.wodc.nl/bitstream/handle/20.500.12832/1143/ob198-volledige-tekst_tcm28-75039.pdf?sequence=2&isAllowed=y

Klima, N., Vander Beken, T., & Van Daele, S. (2009). Vulnerabilität der Wirtschaft für Organisierte Kriminalität: Vulnerabilitätsstudien zur Prävention am Beispiel der Abfallentsorgungsindustrie. *Kriminalistik, 63*(1), 28–35.

Kojouharov, A., & Rusev, A. (2016). Sharks in sheep's clothing – Modalities of predatory and illegal lending in Bulgaria. In G. Antonopoulos (Ed.), *Illegal Entrepreneurship, Organised Crime and Social control*. Springer International Publishing.

Koning, V. (2024). *Regio in Beeld; Midden-Utrecht, 2024-2025*. UWV Arbeidsmarktinformatie en -advies. https://www.uwv.nl/assets-kai/files/f324eef7-8078-4a32-b5a4-9ee983117199/Regio_in_Beeld_2024-2025_Midden-Utrecht.pdf

Korsell, L. (2018). Regulating Organized Crime. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 158-177. https://doi.org/10.1177/0002716218782654

Kostov, K. (2025, August 19). *Домакинствата дължат рекордни суми към компаниите за бързи кредити [Households owe record amounts to payday loan companies].* Darik Business Review. Retrieved from https://dbr.bg/domakinstvata-dalzat-rekordni-sumi-kam-kompaniite-za-barzi-krediti

Kruisbergen, E.W., Roks, R.A., & Kleemans, E.R. (2019). *Georganiseerde criminaliteit in Nederland: Daders, verwevenheid en opsporing*. Wetenschappelijk Onderzoek- en Documentatiecentrum [WODC]. https://repository.wodc.nl/server/api/core/bitstreams/ba33581c-a44c-4131-a3e5-1964e9d1ed84/content

Kruisbergen, E.W., van de Bunt, H.G., & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Wetenschappelijk Onderzoek- en Documentatiecentrum [WODC]. https://research.vu.nl/ws/portalfiles/portal/710011/O_B306%20Volledige%20tekst.pdf

Kruize, P., & Gruter, P. (2020). *Criminele gebouwen: De faciliterende rol van woningen & bedrijfsruimten bij ondermijnende criminaliteit in Nederland en vier EU-landen*. Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). http://repository.wodc.nl/bitstream/handle/20.500.12832/3027/3092-criminele-gebouwen-volledige-tekst.pdf?sequence=1&isAllowed=y

Lam, J., van der Wal, R., & Kop, N. (2018). *Sluipend gif: Een onderzoek naar ondermijnende criminaliteit.* Boom.

Landelijk Informatie en Expertise Centrum [LIEC]. (2019, October 21). *Landelijk beeld van ondermijnende criminaliteit.* https://www.riec.nl/documenten/rapporten/2019/10/21/landelijk-beeld

Leefmilieu Brussel. (2025, November 4). *Socio-economische ontwikkeling*. Retrieved from https://leefmilieu.brussels/burgers/documentatie-en-tools/leefmilieu-stand-van-zaken/socio-economische-ontwikkeling

Lefevere, F. (2020, December 16). "10 tot 15 procent van overheidssteun coronacrisis wordt misbruikt", en de overheid controleert tot nog toe amper. *VRT NWS.* https://vrtnws.be/p.43eN3mVvo

Levi, M., Shentov, O., & Todorov, B. (2015). *Financing of organised crime*. Center for the Study of Democracy (CSD).

Listflix. (n.d.). *Branchenstatistik: Restaurants in Deutschland*. Retrieved from https://listflix.de/statistik/restaurants/

Livsmedelsverket. (2025). *L-2025 nr. 21: Livsmedelsbedrägeri och dess samhällskostnader*. Livsmedelsverket Rapportserie. https://www.livsmedelsverket.se/4af599/globalassets/publikationsdatabas/rapporter/2025/l-2025-nr-21---livsmedelsbedrageri-och-dess-samhallskostnader_.pdf

McDowell, J., & Novis, G. (2001). The consequences of money laundering and financial crime. *Economic Perspectives, 6*(2), 6-8.

Mediapool. (2017, August 17). *Валери Симеонов: Маджо, Радо Слънцето, Маргините клатят държавата чрез туризма [Valeri Simeonov: Maggio, Rado the Sun, Marginites shake the state through tourism]*. Retrieved from https://www.mediapool.bg/valeri-simeonov-madzho-rado-slantseto-marginite-klatyat-darzhavata-chrez-turizma-news268060.html

Morselli, C. (2009). *Inside Criminal Networks*. Springer.

National Statistical Institute. (2025). *Building permits issued for construction of new buildings.* https://www.nsi.bg/en/statistical-data/414/927

Nationale Samenwerking tegen Ondermijnende Criminaliteit [NSOC]. (2023). *Kennisdocument: Verschijningsvormen van malafide goudhandel.* https://www.amlc.nl/wp-content/uploads/2025/01/Verschijningsvormen-van-malafide-goudhandel.pdf

Nationella Operativa Avdelningen [NOA]. (2023). *Miljöbrott Kunskapsunderlag om avfallsbrottslighet till Sveriges tillsynsmyndigheter – Erfarenheter från 2021-2022.* Polismyndigheten; NOA.

Nationella Operativa Avdelningen [NOA]. (2024a). *Myndighetsgemensam rapport om välfärdsbrottslighet inom vård och omsorg*. Polismyndigheten; NOA. https://polisen.se/contentassets/1ad30b09cd7d42bb8330f56188e0c70a/myndighetsgemensam-rapport-om-valfardsbrottslighet-inom-vard-och-omsorg.pdf/download/?v=c1f8559db14136de7c59717903eb9401

Nationella Operativa Avdelningen [NOA]. (2024b). *SIS och HVB-hem: Studie avseende kopplingar till den grovt organiserade brottsligheten.* Swedish National Police Authority; NOA. https://mebybehandlingshem.se/wp-content/uploads/2024/09/SIS-och-HVB-hem-studie-avseende-kopplingar-till-den-grovt-organiserade-brottsligheten-240718.pdf

Nationella Operativa Avdelningen [NOA]. (2025). *Myndighetsgemensam lägesbild organiserad brottslighet 2025*. Polismyndigheten; NOA. https://polisen.se/481be867c6e3ed5c58fd8b73f3dd0c75/siteassets/dokument/organiserad_brottslighet/myndighetsgemensam-lagesbild---organiserad-brottslighet-2025.pdf

Nationellt Underrättelsecentrum [NUC]. (2025). *Delanalys 1: Tecken på missbruk av Försäkringskassans förmåner hos den organiserade brottsligheten och hur den verkar inom assistansersättning.* https://www.forsakringskassan.se/download/18.7e6aef2f19650784573525/1747638970024/tecken-pa-missbruk-av-forsakringskassans-formaner-hos-den-organiserade-brottsligheten-delanalys-1.pdf

Nationellt Underrättelsecentrum [NUC]. (2025). *Delanalys 1: Tecken på missbruk av Försäkringskassans förmåner hos den organiserade brottsligheten och hur den verkar inom assistansersättning.* Försäkringskassan. https://www.forsakringskassan.se/download/18.7e6aef2f19650784573525/1747638970024/tecken-pa-missbruk-av-forsakringskassans-formaner-hos-den-organiserade-brottsligheten-delanalys-1.pdf

Nederlandse Vereniging van Banken [NVB]. (2024, 6 September). *Sector Standaard verduidelijkt bankieren voor ondernemers in de automotive sector.* Retrieved from https://www.nvb.nl/nieuws/sector-standaard-verduidelijkt-bankieren-voor-ondernemers-in-de-automotive-sector/

Paoli, L. (2003). *Mafia brotherhoods: Organized crime, Italian style*. Oxford University Press.

Paoli, L. (2004). Italian organised crime: Mafia associations and criminal enterprises. *Global Crime, 6*(1), 19-31. https://doi.org/10.1080/1744057042000297954

Paoli, L. (2020). What makes mafias different? *Crime and Justice, 49*(9), 141-222. https://doi.org/10.1086/708826

Patiëntenfederatie Nederland. (n.d.). *Zorgaanbieders in Utrecht*. Retrieved from https://www.zorgkaartnederland.nl/utrecht

Pinotti, P. (2015). The Economic Costs of Organised Crime: Evidence from Southern Italy. *The Economic Journal, 125*(586), 203-232. https://doi.org/10.2139/ssrn.2057979

Politie. (2025, 4 July). *Geld en crypto aangetroffen bij onderzoek naar juwelier Kanaalstraat*. Retrieved from https://www.politie.nl/nieuws/2025/juli/4/03-geld-en-crypto-aangetroffen-bij-onderzoek-naar-juwelier-kanaalstraat.html

Porrazzo, E. (2025). *Rapporto Rifiuti Urbani – Edizione 2025*. L'Istituto Superiore per la Protezione e la Ricerca Ambientale (ISPRA). https://www.isprambiente.gov.it/files2025/pubblicazioni/rapporti/rapportorifiutiurbani_ed-2025_n419_versioneintegrale.pdf

Port of Antwerp-Bruges. (n.d.). *Wereldhaven*. Retrieved from https://www.portofantwerpbruges.com/nl/onze-haven/wereldhaven

PVO Oost-Nederland. (2022). *Witwassen en heling in de metaalhandel: Waarop letten?* Retrieved from https://www.pvo-oostnederland.nl/nieuws/witwassen-en-heling-in-de-metaalhandel-waarop-letten/

Raets, S., & Janssens, J. (2019). Financing of trafficking in human beings in Belgium. In O. Shentov, A. Rusev, & G. Antonopoulos (Eds.), *Financing of organised crime: Human trafficking in focus* (pp. 129-160). Center for the Study of Democracy (CSD).

Rijksoverheid. (2024, March 14). *Handreiking voor kwetsbare branches in de strijd tegen georganiseerde, ondermijnende criminaliteit.* Ministerie van Justitie en Veiligheid; Ministerie van Economische Zaken en Klimaat. https://open.overheid.nl/documenten/df1d92dd-bd18-4d8e-a1f0-0922d387b4f1/file

Rijksoverheid. (n.d.). *Persoonsgebonden budget (pgb).* Retrieved from https://www.rijksoverheid.nl/onderwerpen/persoonsgebonden-budget-pgb

Rostami, A., & Mondani, H. (2024). *Kriminella entreprenörer: En studie av den organiserade brottslighetens kopplingar till näringslivet.* Stockholms Handelskammare. https://stockholmshandelskammare.se/wp-content/uploads/2024/01/kriminella-entreprenorer--en-studie-av-den-organiserade-brottslighetens-kopplingar-till-naringslivet.pdf

Rusev, A., Faion, M., Bezlov, T., & Sabev, M. (2026). *Dirty streams: Organised crime, corruption and control over municipal waste services.* Center for the Study of Democracy [CSD]. https://csd.eu/fileadmin/user_upload/publications_library/files/2026_02/Dirty-Streams-en-web.pdf

Safe News (2024, October 18). *Рекетьорите от „Пас Кредит“ измъчвали жертвите си със средства подобни за инквизиция [The Pass Credit racketeers tortured their victims with inquisition-like means].* Retrieved from https://safenews.bg/reketorite-ot-pas-kredit-izmachvali-zhertvite-si-sas-sredstva-podobni-za-inkvizicziya/

Savona, E.U. (2010). Infiltration of the public construction industry by Italian organised crime. In K. Bullock, R.V. Clarke, & N. Tilley (Eds.), *Situational Prevention of Organised Crimes* (pp. 130-150). Willan Publishing.

Savona, E.U., & Berlusconi, G. (2015). *Organized crime infiltration of legitimate businesses in Europe: A pilot project in five European countries – Final report of project ARIEL – Assessing the risk of the infiltration of organized crime in EU MSs legimitate economies: a pilot project in 5 EU countries*. Transcrime – Università degli Studi di Trento.

Savona, E.U., & Riccardi, M. (2015). *From illegal markets to legitimate businesses: The portfolio of organised crime in Europe. Final report of Project OCP – Organised Crime Portfolio.* Transcrime – Università degli Studi di Trento.

Savona, E.U., & Riccardi, M. (2018). *Mapping the risk of Serious and Organised Crime infiltration in European Businesses – Final report of the MORE Project.* Transcrime – Università Cattolica del Sacro Cuore.

Schouten, A. (2025, 10 September). Burgemeester Dijksma sluit pand in Lombok na inval bij goudhandel. *Algemeen Dagblad*. https://www.ad.nl/utrecht/burgemeester-dijksma-sluit-pand-in-lombok-na-inval-bij-goudhandel~a253536a/

Servizio Analisi Criminale. (2023). *Le interdittive antimafia 2021-2022.* Ministero dell' Interno, Dipartimento Della Publica Sicurezza, Direzione Centrale della Polizia Criminale.

Shentov, O., Rusev, A., & Antonopoulos, G. A. (2018). *Financing of organised crime: Human trafficking in focus*. Center for the Study of Democracy (CSD).

Snaphaan, T., & van Ruitenburg, T. (2024). Financial crime scripting: An analytical method to generate, organise and systematise knowledge on the financial aspects of profit-driven crime. *European Journal on Criminal Policy and Research*, *31*(4), 695-715. http://doi.org/10.1007/s10610-023-09571-9

Snaphaan, T., Verhoeven, S., Van Bergen, K., & Van Ruitenburg, T. (2025). Compensatie als witwastechniek: Het 'Cash Compensatie Model' ontrafeld. In T. Snaphaan, A. Verhage, M. Hoekstra & W. Huisman (Eds.), *De financiële kant van criminaliteit* (Cahiers Politiestudies, nr. 76) (pp. 101-130). Gompel & Svacina.

Snaphaan, T., Kostense, M., & van Ruitenburg, T. (2024). Financial crime scripting: Een verdieping van crime scripting voor de analyse van winstgedreven criminaliteit. In T. Snaphaan & P. Klerks (Eds.), *Crime scripting: Een methode voor wetenschap en praktijk* (pp. 123-141). Boom.

Soudijn, M., & Akse, T. (2012). *Witwassen: Criminaliteitsbeeldanalyse 2012.* Korps Landelijke Politiediensten [KLPD] – Dienst Nationale Recherche. https://www.researchgate.net/profile/Melvin_Soudijn2/publication/261362765_Witwassen_Criminaliteitsbeeldanalyse_2012/links/00b7d534045b668301000000/Witwassen-Criminaliteitsbeeldanalyse-2012.pdf

Spapens, A. C. M., Peters, M., & Van Daele, D. (2015). *Administrative approaches to crime. Administrative measures based on regulatory legislation to prevent and tackle (serious and organized) crime. Legal possibilities and practical applications in 10 EU Member States*. Tilburg University, Catholic University of Leuven, Dutch Ministry of Security and Justice.

Spapens, A., Blatter, I., Mouris, M., Jaspaert, E., Colman, C., & Van Nimwegen, S. (2024). *Grensoverschrijdende samenwerking tegen ondermijnende criminaliteit in het Belgisch-Nederlandse grensgebied: 2018-2023.* Tilburg University; Universiteit Gent; Nationale Politie. https://research.tilburguniversity.edu/en/publications/7e3d478f-d997-4a84-859b-e30bc0819b67

Stad Antwerpen. (2025). *Rapport economie: District Antwerpen*. Antwerpen: Stad in Cijfers. Retrieved from https://stadincijfers.antwerpen.be/Mosaic/rapport-economie/

Stad Antwerpen. (n.d.). *Horecabeleidsplan*. Retrieved on May 5, 2026 from https://www.antwerpen.be/info/horecabeleidsplan

Stadt Frankfurt am Main (n.d.). *Lebenslagenkarten und Stadtteilprofile*. Retrieved from https://frankfurt.de/service-und-rathaus/verwaltung/aemter-und-institutionen/jugend--und-sozialamt/unsere-inhalte/armut/lebenslagenkarten-und-stadtteilprofile

Stanchev, S. (2024, November 2). *Среднощна полицейска акция в София: Открити са наркотици и райски газ [Midnight police raid in Sofia: Drugs and laughing gas found].* BTV Novinite. https://btvnovinite.bg/predavania/tazi-sabota-i-nedelia/srednoshtna-policejska-akcija-v-sofija-otkriti-sa-narkotici-i-rajski-gaz.html

Statens Offentliga Utredningar [SOU]. (2023). *Arbetslivskriminalitet – Arbetet i Sverige; En bedömning av omfattningen; Lärdomar från Danmark och Finland*. Elanders Sverige AB. https://www.regeringen.se/contentassets/c9ca41d6a6d449b494d399b42bc0d7c8/arbetslivskriminalitet--arbetet-i-sverige-en-bedomning-av-omfattningen-lardomar-fran-danmark-och-finland-sou-20238.pdf

Statens Offentliga Utredningar [SOU]. (2025). *Hem för barn och unga: För en trygg, säker och meningsfull vård. Betänkande av Utredningen om HVB för barn och unga.* Elanders Sverige AB. https://www.regeringen.se/contentassets/58f9f98580c34e3d911b4cdeefdd8b1d/hem-for-barn-och-unga-sou-202584.pdf

Statista. (n.d.). *Gesamtbruttowertschöpfung in den Metropolenregionen in Deutschland in den Jahren 2020 bis 2022*. Retrieved from https://de.statista.com/statistik/daten/studie/1491367/umfrage/bruttowertschoepfung-in-den-metropolregionen-in-deutschland/

Stoykova, P. (2023, October 30). *The housing market in Sofia in 2023 – New market report*. Bulgarian Properties. https://www.bulgarianproperties.com/Property_news/sofia-housing-market-review_9547.html

Strategisch Kenniscentrum Ondermijnende Criminaliteit. (2026). *Criminele inmenging: Corruptie, bedreiging en infiltratie door georganiseerde criminaliteit in Nederland*. https://skc-oc.nl/wp-content/uploads/2026/03/260311_Themastudie-Criminele-Inmenging.pdf

Sørensen, K.E. (2021). 'Front' or 'straw men' directors: A missing element in the effort to prevent the abuse of companies? *European Company and Financial Law Review, 18*(5), 749-772. https://doi.org/10.1515/ecfr-2021-0028

te Pest, M., Nieuwdorp, S., Smeets, B., & van Wijnen, E. (2012). *Verwevenheid van onder- en bovenwereld bij georganiseerde criminaliteit. Een overzichtsstudie: Aard en oorzaken.* Regionaal Informatie en Expertise Centrum (RIEC) Zuid-West Nederland; Openbaar Ministerie. https://www.yumpu.com/nl/document/read/19839788/verwevenheid-van-onder-en-bovenwereld-bij-riecs/1

ten Dam, N. (2021, 30 March). Risico-indicatoren Cash Integration in de automotive sector. *Anti Money Laundering Centre*. Retrieved from https://www.amlc.nl/risico-indicatoren-cash-integration-in-de-automotive-sector/

Tieleman, Y. (2018, 4 December). Politie en gemeente doen inval bij 17 autobedrijven in Utrecht Overvecht. *Algemeen Dagblad*. Retrieved from https://www.ad.nl/utrecht/politie-en-gemeente-doen-inval-bij-17 autobedrijven-in-utrecht-overvecht~acb2d93c/

Top, P., & van der Torre, E. (2024). *Ondermijning*. Boom.

Tops, P., & Van der Torre, E. J. (2024). Ondermijning: Over de praktische betekenis van een analytisch begrip. Boom bestuurskunde.

TREND – Research Centre (2023). *НАГЛАСИ СРЕД ПОТРЕБИТЕЛИТЕ: НА БЪРЗИ КРЕДИТИ [Consumer Attitudes: On Fast Credits].* Association for Responsible Non-Bank Lending [AONK].

Trifonov Law Office. (2012, August 13). *Payday Loans License for Short Term Loans Direct Lenders in Bulgaria.* Retrieved from https://businessimmigrationbulgaria.com/loans/

Trippen, S., Engelhardt, A.K., Hischemöller, M., Heinola, M., Holzmaier, A., Quirin, L., & Remlein, L. (2021). *Die volkswirtschaftliche Bedeutung der Bau- und Immobilienwirtschaft in FrankfurtRheinMain.* PERFORM Zukunftsregion FrankfurtRheinMain; Chamber of Commerce and Industry Darmstadt.

Unioncamere, & InfoCamere. (2025). *Analiso del dato: Movimprese*. Retrieved from https://www.infocamere.it/movimprese

UtrechtZorg. (n.d.). *Aantal werknemers per kwartaal*. Retrieved from https://utrechtzorg.arbeidsmarktinbeeld.nl/content/states/index/36752?frame=True&cmsComp%20onentId=28407&cmsPageId=857&chartHeight=Height_150&applicableCMSFilters=64&applicable%20CMSFilters=42

Van den Wyngaert, C., Vandromme, S. & Traest, P. (2019). *Strafrecht en strafprocesrecht in hoofdlijnen.* Gompel & Svacina.

van der Torre, E., & Jongepier, T. (2021). *Een quick scan naar (de aanpak van) zorgfraude in Utrecht*. LokaleZaken. https://utrecht.bestuurlijkeinformatie.nl/Document/View/c20f6ba6-ee28-4ddb-84fa-c28530a39e65

van der Veen, H.C.J., & Heuts, L.F. (2024). National Risk Assessment Witwassen 2023. Wetenschappelijk Onderzoek- en Documentatiecentrum [WODC]. https://open.overheid.nl/documenten/dpc-57df777dcc8eb70a11d5f2e8faedf623a4fd153f/pdf

van der Veen, H.C.J., & Heuts, L.F. (2017). *National Risk Assessment on Money Laundering for the Netherlands.* Wetenschappelijk Onderzoek- en Documentatiecentrum [WODC]. https://repository.wodc.nl/server/api/core/bitstreams/b3869ec0-d3ac-453e-999e-5bda45bb0e41/content

Van Maele, P. (2023, January 14). *Hoe de drugsmaffia haar fortuin witwast.* De Standaard. https://www.standaard.be/nieuws/hoe-de-drugsmaffia-haar-fortuin-witwast/47500006.html

van Santvoord, V. D., & van Ruitenburg, T. (2022). Financial crime scripting: Introducing a financial perspective to the Dutch cocaine trade. *The Police Journal, 96*(2), 374-389. https://doi.org/10.1177/0032258X221083449

Varese, F. (2010). What is organised crime? In F. Varese (Ed.), *Organized Crime: Critical Concepts in Criminology* (pp. 1-33). Routledge.

Veiligheidsalliantie Rotterdam. (n.d.). *Automotivebranche*. Retrieved from https://veiligheidsalliantie.nl/kennisbank/ondermijning/automotive/

Vlaamse Overheid. (n.d.-a). *Bedrijfsbeheer en beroepsbekwaamheid*. Retrieved from https://www.vlaanderen.be/starten-met-een-onderneming/bedrijfsbeheer-en-beroepsbekwaamheid

Vlaamse Overheid. (n.d.-b). *Een vennootschap oprichten*. Retrieved from https://www.vlaanderen.be/economie-en-ondernemen/een-eigen-zaak-starten/starten-met-een-onderneming/een-vennootschap-oprichten

VLAIO. (n.d.). *Overbruggingslening*. Retrieved from https://www.vlaio.be/nl/subsidies-financiering/overbruggingslening

Wittevrongel, F., & De Jaeger, T. (2024). Het spanningsveld tussen het vrij ondernemerschap en het criminele ondernemerschap in België: een eerste blik op enkele opportuniteiten voor, en recente initiatieven tegen, malafide ondernemers. *Panopticon, 45*(4), 305-350. http://hdl.handle.net/1854/LU-01J0T7XFNHDMS3PAFWE684VN4P

Държавна агенция Национална сигурност [State Agency for National Security] (SANS). (2022). *Резюме на Националната оценка на риска от изпиране на пари и финансиране на тероризъм [Summary of the National Money Laundering and Terrorist Financing Risk Assessment]*.

Столичната общинска агенция за приватизация и инвестиции [Sofia Municipal Agency for Privatisation and Investments; InvestSofia]. (2025). *2024 София бизнес дестинация [2024 Sofia Business Destination].* СОАПИ [SOAPI]. Retrieved from https://investsofia.com/3d-flip-book/sofia-business-destination-2024/

ANNEXES

ANNEX 1

ANTWERP

DETAILED CASE STUDIES

Annex 1.A – Case Alfa: Laundering Cocaine Profits in Antwerp

1. Criminal network involved in Case Alfa

The criminal network at the centre of Case Alfa was involved in the systematic laundering of illicit proceeds derived from the large-scale importation of cocaine through the Port of Antwerp. Its organisation was designed to conceal identities and the origin of assets, and to shield ongoing criminal activities from external scrutiny. Based on the judicial files, at least 54 persons have been linked to the network. An individual was considered a member if the records revealed an evidentiary link to the network's criminal activities. This also included facilitators, 'guards', and intermediaries who used encrypted telephony, but whose roles could be precisely identified. Table 2 provides an overview of the core **members of this network**.

Table 2
Overview of the core members of the criminal network involved in Case Alfa (Antwerp)

Member	Role	Gender	Born between	Nationality
C2_A	Leader (after C1_A's death)	Male	1974-1993	Moroccan
C3_A	Co-leader; Cocaine extractions	Male	1974-1993	Belgian
C4_A	Key launderer; Financial advisor	Male	1954-1973	Dutch
C5_A	Support tasks	Male	1974-1993	Belgian
C6_A	External contacts; Meeting facilitator	Male	1934-1953	Dutch
C7_A	Facilitator; Fake payslips; Prospection of foreign acquisitions	Male	1954-1973	Dutch
C8_A	Errand runner and guard for C2_A	Male	1974-1993	Belgian
C9_A	Facilitator – Unofficial accountant; Advisor of LTD2_A and LTD3_A	Male	1954-1973	Belgian
C10_A	Beneficiary and strawperson of LTD2_A	Female	1974-1993	Belgian
C11_A	Leader of another criminal network	Male	1974-1993	Albanian
C12_A	Prospection of foreign acquisitions	Male	1974-1993	Russian
C13_A	Cocaine shipments from South America	Male	1954-1973	Dutch

As individual characteristics are not known for all members of the networks, no definitive statements can be drawn about the network's demographic composition. However, the judicial files allowed to infer information about the structure and organisation of the network. Following the death of the network's initial leader (C1_A) in 2018, decision-making was concentrated within a small core group, supported by trusted advisors and informal financial facilitators. The judicial files revealed a **layered structure**, consisting of a leadership group (C2_A; C3_A) that coordinated the import and distribution of cocaine, a laundering 'back office' (C4_A) that provided financial advice and cover stories, and a broader circle of associates and service providers who were mobilised as needed.

Aside from a few family ties, the network seems to be held together primarily by opportunistic relationships. Moreover, the judicial files revealed links to other criminal networks: at least two members (C11_A; C18_A) had ties to networks involved in cocaine import and money laundering.[47] On top of that, since some members primarily used the network to create the appearance of being formally employed through fictitious labour ties, its money laundering infrastructure also served other criminals seeking to launder illicit funds and obtain legal status (i.e., crime-as-a-service).

2. Legitimate businesses involved in Case Alfa

An analysis of the judicial files related to Case Alfa revealed the involvement of several legally registered companies, most of which located in Belgium, but also one in the Netherlands and one in the United Arab Emirates (UAE). Based on the files, **nine legitimate businesses** were identified. The majority of these are private limited companies (LTD). Table 3 provides an overview of the companies involved.

Table 3
Overview of the businesses involved in Case Alfa (Antwerp)

Company	Economic sector	Status in 2025	Location
LTD1_A	Hospitality and car rental	Inactive – Bankrupt in 2020	Antwerp, Belgium
LTD2_A	Hospitality and car rental	Active – Voluntary dissolution in 2022	Antwerp, Belgium
LTD3_A	Hospitality and car rental	Active	Antwerp, Belgium
LTD4_A	Oil and gas industry	Active	Breda, The Netherlands
LTD5_A	Oil and gas industry	Unknown	Dubai, UAE
LTD6_A	Construction	Inactive – Bankrupt in 2019	Limburg, Belgium
LTD7_A	Construction	Active	Limburg, Belgium
PLC1_A	Services	Active	Liège, Belgium
GP1_A	Services	Active	Antwerp, Belgium

With the exception of LTD4_A and LTD5_A, the businesses under investigation were characterised by highly local or regional activities, holding little significance within their respective sectors or markets. Most of the entities qualified as **small enterprises**, often employing less than twenty individuals. Their ownership and management structures consistently demonstrated close connections to the criminal network, with several entrepreneurs simultaneously occupying leadership positions within the network. LTD1_A, LTD2_A and LTD3_A were the core business entities, while the other companies were used to a lesser extent by the network. Nevertheless, all of the businesses involved combined the conduct of legitimate business operations with the facilitation of criminal activities.

[47] Within that other network, C11_A appears to have played a leading role and to have been involved in various international investigations into cocaine trafficking and money laundering.

- **LTD1_A** was established in 2009 in Antwerp as a private limited company operating in the hospitality sector, specifically in the restaurant industry. Later, its corporate purpose was formally extended to include, among others, activities related to the purchase, sale, and rental of vehicles with or without a driver. The company continued to operate until its liquidation in 2020. Since its very inception, LTD1_A has been closely linked to the criminal network; the company's executives being part of that network.
- **LTD2_A**, founded in 2016 in Antwerp, has been registered as a combination of a brasserie and retail, wholesale, and brokerage services of vehicles. The company was established by members of the criminal network. Following C1_A's death in 2018, C10_A took over the responsibility of directorship, a position she continues to hold to this day.
- **LTD3_A** was founded in 2010, located in Antwerp. In 2015, this business was acquired by members of the criminal network, with C1_A, C2_A, and C3_A appointed as directors. The firm's activities encompass a diverse range of commercial activities, including cafés, full-service restaurants, catering services, and vehicle wholesale.
- **LTD4_A** constitutes a Dutch-registered company directed by C7_A and specialised in project execution within the oil and gas industry. This company had a subsidiary in Dubai (**LTD5_A**).
- **LTD6_A** was originally established in 2003 in Belgian Limburg as a general partnership (GP) by C25_A and C27_A but was later reorganised into a private limited company. The company specialised in renovation activities. The business was declared bankrupt in 2019, bringing its operations to a definitive conclusion.
- **LTD7_A** was founded in 2012 by C24_A, C25_A and C26_A as a renovation firm in Limburg. Subsequent years witnessed a series of changes in managerial leadership: official records demonstrate a discrepancy regarding its current status. While judicial documents indicate bankruptcy in 2019, the Crossroads Bank for Enterprises (CBE) lists the company as still active with two other owners not mentioned in the judicial files.
- **PLC1_A** was established in 1998 in Liège and has operated continuously under the directorship of C7_A since its incorporation. The company specialises in providing management consultancy services.
- **GP1_A**, founded in 2017 in Antwerp under the directorship of C19_A, is centred around providing consultancy services in information technology.

3. Crime script based on Case Alfa

Motivation – Purpose

Within Case Alfa, the criminal use of legitimate businesses was primarily motivated by the aims of laundering the proceeds of drug trafficking and cleaning the network's reputation. The core members sought to convert the illicit earnings from large-scale cocaine imports and subsequent sales into seemingly legitimate revenues, thereby publicly presenting themselves as legitimate entrepreneurs. The legitimate businesses were primarily involved in the **money laundering** aspect of the criminal business model. They provided the corporate façade and the day-to-day commercial operations that allowed illicit proceeds to be integrated into the system and made to appear legitimate. Nevertheless,

their role was not limited to laundering proceeds. Evidence from phone taps shows that the hospitality sites of firms LTD2_A and LTD3_A also served as regular **meeting points** during the planning phase. At these restaurants, the network members discussed the acquisition of encrypted devices, the potential establishment of an import route through the Port of Ghent, and the exchange of information regarding container numbers and the cover loads relevant to the transport of cocaine.

Preparation

The network has selected economic sectors that combine **low barriers** to entry with opportunities to generate or manipulate revenue streams. Businesses within the hospitality industry, on the one hand, are cash-intensive and anonymous, produce large numbers of small transactions, and boost revenue by adding 'extra' covers or reservations. Staffing can also be flexible, which facilitates the manipulation of payroll records. Services related to the rental of vehicles and limousines, on the other hand, provide additional opportunities to fabricate service provision and cash income.

Pre-activity or enabling conditions

The criminal network relied on legitimate businesses that it had either **established itself or infiltrated** to create opportunities for money laundering. In all cases, however, lawful activities continued alongside the criminal use, such as restaurant operations and the rental of limousines. LTD1_A and LTD2_A were founded by members of the network, hence criminally owned from their inception, in sectors that lend themselves to money laundering. LTD3_A was subsequently acquired by members of the network. Although the judicial files did not specify exactly why this company was selected, they do describe a 'standard' takeover method coordinated by C4_A: network members approached the former managers and, where possible, finance directors to assess solvency and determine how easily the business could be transferred. The same *modus operandi* was used abroad.

The level of criminal use in LTD1_A, LTD2_A, and LTD3_A can be considered high. The leaders of the network occupied managerial positions and began artificially inflating daily revenues with illicit cash, creating fictitious payrolls, and shuffling assets. When LTD2_A was established, the network transferred LTD1_A's assets, including limousines, without any documentation. A few years later, these vehicles were sold to a dubious foreign buyer through fake invoices with inflated amounts, suggesting a form of **trade-based money laundering**. The other businesses mentioned (LTD4_A, LTD5_A, LTD6_A, LTD7_A, PLC1_A, GP1_A) were infiltrated primarily to generate false employment contracts and payslips. The owners were approached directly and accepted bags of cash, which weakens any claim that they were unaware of the criminal intent. However, the judicial files did not allow for any clear conclusions to be drawn as to whether coercion was involved.

Activity

Alongside legitimate commercial activities, the businesses were used as multifunctional tools for placing, layering, and integrating proceeds from cocaine trafficking. It is estimated that more than EUR 5 million in illicit assets were laundered between 2014 and 2020. However, not all companies were used with the same intensity. On a day-to-day basis, revenue at LTD2_A and LTD3_A was artificially inflated by entering **fictitious restaurant reservations** into the system in order to meet a daily cash target of around EUR 5,000. Shortfalls were covered with cash obtained through cocaine sales and deposited as business takings. The judicial investigation attributed at least EUR 290,000 (2014-2020) to this method of manipulating the declared revenues. Furthermore, more than EUR 50,000 in cash was

found to have been set aside for wages paid 'off the books' to *bona fide* employees at LTD2_A and LTD3_A, indicating systematic **fiscal and social fraud**.

Another common method of money laundering involved the limousine and car rental industry. Businesses were used to justify **fictitious rental income** without performance-based invoices. Trip sheets were forged by randomly selecting names from telephone directories and using them as the names of people who had supposedly rented the vehicles. These fictitious 'trips' were paid for with illicit drug money, to make the money appear legitimate. Through this scheme, approximately EUR 480,000 was laundered. At the same time, the network gave the impression of generating legitimate income through the **false employment** of network members and **cash compensation schemes**: C4_A received cash (derived from the sale of cocaine sales) from C2_A and C3_A and passed it on to the business owners, who then paid out fake monthly wages to the members of the criminal network.

Alongside these recurring laundering practices, the criminal network also used LTD2_A and LTD3_A for various one-off transactions. For instance, the **renovation of their premises** served to launder proceeds from cocaine trafficking: by inflating construction works and paying them almost exclusively in cash, illicit funds were disguised as legitimate renovation expenses.[48] To make the financial scheme appear credible, the network officially engaged a seemingly reputable architect, who provided architectural plans, invoices, and project documentation to create a convincing paper trail. During the renovation work, the network also significantly expanded its seating capacity in order to justify sudden increases in revenue.

Post-activity or post conditions

Between 2014 and 2020, the legitimate businesses involved were continuously used for criminal purposes, enabling the network to launder drug proceeds. During this period, there were certain indications of criminal use. For example, LTD1_A should technically have been dormant since its closure in 2016 but continued to receive more than EUR 500,000 in cash deposits. Banks also signalled numerous **red flags**, as a bank director noted that the usual ratio of cash to debit/credit cards – 40 percent cash and 60 percent cards, as in similar restaurants – was reversed here, with deposits often consisting exclusively of 50-euro bills in near-unused conditions. The law enforcement investigation into the criminal use of legitimate businesses by this network was launched following a referral from the Belgian FIU, after network members attempted to deposit EUR 750,000 in cash at a Belgian bank.

4. Financial profile of the criminal network involved in Case Alfa

Financing sources and start-up capital

The judicial investigation revealed that the start-up capital came primarily from **illegal sources**, derived from the large-scale importation of cocaine through the Port of Antwerp, and the sale thereof. These illegal streams were supplemented by a few legal streams that were, however, negligible. For example, the limousine and car rental service generated roughly EUR 60 per day. Lawful turnover in LTD1_A, LTD2_A, and LTD3_A cannot be reliably estimated because the cash registers were regularly topped up with illicit cash.

[48] Nevertheless, this investment was unusual, since the venues were initially only leased.

Payment methods and arrangements within the network

Transactions within the criminal network were predominantly **cash**-based. Sky ECC messages indicate that EUR 5 to 6 million in cash was stored in bags and was tracked by an internal administration system that recorded who withdrew money and when. For example, cash was used to pay network members in the form of vacuum-packed bundles carried in sports bags and packages hidden in vehicle compartments. Cross-border transfers relied on **underground banking**, where cash was handed over locally and transferred to Morocco for a fee of around 3 percent. Subsequently, family members or friends could withdraw the funds in Morocco and deposit them into local bank accounts. The fact that cash played such a dominant role is also evident from the way it was stored and the contingency arrangements that were made.[49] Moreover, **fictitious salaries** were paid through the companies' payrolls to create the appearance of legal income. Payment **in kind** was also commonplace: members received luxury cars and had their rent and utilities paid.[50] The criminal network purchased more than EUR 180,000 worth of luxury vehicles in cash for its members.

Costs of business operations

The network's operating costs included both expenses related to criminal activities and costs incurred to maintain the appearance of legitimate business operations.[51] Major expenses included the cash-heavy renovations at companies LTD2_A and LTD3_A. Moreover, day-to-day laundering required cash for till inflation, fictitious payroll, and cash payments to *bona fide* staff members. In addition, the network also incurred costs for compensation in kind. Through LTD2_A's cash register, prospecting trips abroad to identify companies for sale were financed. Other expenses included the wages of a straw director, payments to facilitators, legal fees, the production of false invoices, and forgery of payroll documents. Cash handling itself also generated costs, including underground banking fees, the rental of safe deposit boxes, vacuum sealers, packaging materials, modifications to vehicles, and premises for the concealment of cash. Furthermore, operational security required encrypted devices and their regular placement. To maintain a credible front, the companies also covered standard operating expenses, such as fuel, food and beverages for restaurants, and other daily necessities. They likewise paid administrative costs typical of legitimate businesses, including notary fees, licences, bank account maintenance costs, costs associated with changes to registered offices, insurance, and utilities.

Revenues and proceeds

Overall criminal proceeds were originating primarily from the importation and sale of cocaine. Based on the judicial investigation, it is estimated that the network possessed between EUR 5 to 6 million, and that an amount of over EUR 5 million was laundered between 2014 and 2020.

[49] Members of the network opened bank lockers in the names of relatives or friends and hid money there, whereas others buried cash in plastic bags underground. One member described setting aside EUR 20,000 together with a friend to ensure immediate access to legal counsel in the event of an arrest, plus EUR 150 per month for expenses at the prison canteen.

[50] For example, C4_A financed safe houses for several members by putting the lease and utility contracts in his own name and paying the annual rents and security deposits in cash to the landlords (> EUR 75,000).

[51] This section focuses exclusively on the costs related to the money laundering phase, as those associated with cocaine imports were not specified in the judicial files.

5. Harms caused by Case Alfa

Harms to individuals

Bona fide workers employed by LTD2_A and LTD3_A were frequently paid in cash and, in many cases, worked off the books. The absence of formal employment arrangements deprived them of basic labour protections, social security coverage, and pension entitlements, leaving them in a vulnerable and insecure position.

Harms to other businesses

By combining criminal proceeds with legitimate restaurant revenues and engaging in tax and social security fraud, the network reduced operating costs and gained an unfair competitive advantage. This distorted competition and disadvantaged law-abiding businesses in the hospitality and transport sectors.

Harms to public institutions

The network's tax and social security fraud resulted in lost public revenue and unpaid contributions, undermining the financial basis of public services. In addition, attempts to channel large amounts of unexplained cash through the National Bank of Belgium and the commercial banking sector sought to exploit financial infrastructure for money laundering purposes, thereby eroding trust in institutional integrity.

Harms to the social environment

Case Alfa demonstrates broader harm to the social environment. The use of a strawman and the provision of misleading employment documentation undermined confidence in judicial processes. Furthermore, efforts to launder criminal proceeds through financial institutions and evidence that imprisoned leaders continued to coordinate network activities contributed to perceptions of institutional weakness and reduced public trust in the effectiveness of the Belgian justice system.

Annex 1.B – Case Bravo: Infiltrating Antwerp's Logistics Chain

1. Criminal network involved in Case Bravo

The criminal network at the centre of Case Bravo was involved in the large-scale **importation and distribution of cocaine** through the Port of Antwerp. Judicial evidence from 2019 to 2021 points to repeated attempts of cocaine importation, including at least fourteen successful extractions and six failed operations. Seizures by the police and customs authorities indicated that these were substantial shipments, typically weighing more than 500 kilograms and sometimes nearly two tons. Alongside these import activities, the network **laundered the proceeds** through affiliated companies and relied on violence, or the threat thereof, to secure cooperation. Table 4 provides an overview of the core members of this network.

Table 4

Overview of the core members of the criminal network involved in Case Bravo (Antwerp)

Member	Role	Gender	Born between	Nationality
C1_B	Right-hand man of C2_B	Male	1974-1993	Belgian
C2_B	Key figure within the international drug trade; Drug lord with his own clan	Male	1974-1993	-
C3_B	Key figure within the international drug trade; Drug lord with his own clan	Male	1974-1993	-
C4_B	Facilitator; Corrupted employee of LTD1_B	Female	1974-1993	-
C5_B	Facilitator; Corrupted employee of LTD1_B	-	1974-1993	-
C6_B	Facilitator; Corrupted employee of LTD1_B	Female	1974-1993	-
C7_B	Facilitator; Shareholder of LTD6_B	Male	1954-1973	Belgian
C8_B	Girlfriend of C4_B	Female	1974-1993	Belgian
C9_B	Right-hand man of C2_B	Male	1974-1993	-
C10_B	Cash driver; Support tasks	Male	1974-1993	-

Although the exact size of the criminal network and the full scope of its broader associations remain unclear, the judicial files and open sources allowed to form a useful picture. The available information indicates that at least 38 individuals were involved, none of whom were minors. Many of those involved were already known to LEAs and had criminal records. This network turned out to have a **clear leadership structure** centred on C1_B and composed of a wide range of facilitators. Under this leadership, however, the network appeared to have operated largely opportunistically, seeking out actors who could assist with specific stages of the criminal process. Moreover, the network appeared to be operationally resilient: it regularly changed drivers, bank accounts, and licence plates, built in-house transport capacity, and repeatedly established or acquired new companies. It also adapted quickly to technological security upgrades at the Port of Antwerp.

The judicial files showed that C1_B is the central broker within the criminal network, acting on behalf of C2_B and C3_B, two notorious drug traffickers who play a major role in international cocaine trafficking and related violence. It turned out that C1_B played a key role in organising cocaine imports through the Port of Antwerp and in establishing import routes from South America. He also appeared to have controlled access to facilitators, owned several businesses, and provided services to other criminal networks. Both court documents and open sources portrayed him as the right-hand man of C2_B, and as a person known in criminal circles for using threats and violence against rivals and non-cooperators.

Furthermore, **facilitators** operating within logistics company LTD1_B played an important support role. Three employees (C4_B, C5_B, C6_B) acted as fixed facilitators for this criminal network. Working within LP1_B's container schedule system, they provided information about containers and seals, manipulated scheduling data, and disclosed PIN codes and delivery details related to container traffic through the Port of Antwerp. Other facilitators included corrupt truck drivers, cash couriers, and strawmen. To secure the cooperation of these individuals, the network relied on both corruption and intimidation. In addition, the judicial files point to connections with other criminal networks: counterparts in South America concealed cocaine at the point of origin and coordinated departures with the network's extraction window in Antwerp, and it also had ties to a Brussels-based network.

2. Legitimate businesses involved in Case Bravo

An analysis of the judicial files related to Case Bravo revealed a link between the aforementioned criminal network and **six legitimate businesses** located in Antwerp. These companies were involved to varying degrees in the different stages of the criminal process. Those that were mentioned only once in the case files have been excluded from this discussion due to a lack of information. Table 5 provides an overview of the most relevant companies involved.

Table 5
Overview of the businesses involved in Case Bravo (Antwerp)

Company	Economic sector	Status in November 2025
LTD1_B	Logistics	Active
LTD2_B	Hospitality	Inactive – Bankrupt in 2022
LTD3_B	Hospitality	Inactive – Bankrupt in 2020
LTD4_B	Hospitality and car retail	Active – Bankruptcy opened in 2024
LTD5_B	Wholesale	Unknown
LTD6_B	Services	Active

All of the companies mentioned in the judicial files were **private limited companies** (LTD). This preference for a particular legal form was also evident in the intercepted Sky ECC communications, which suggested that the economic activities of the companies associated with the network were essentially secondary to their legal structure (cf. *infra*).

- **LTD1_B**, a Flemish logistics company, offers a wide range of services, including container and port logistics and storage solutions for various industries such as retail, food, and petrochemicals. Its Antwerp port branch was infiltrated through the corruption of lorry drivers and employees who had access to container information.

- **LTD2_B** was founded in 2016 by C1_B as a hospitality business, based in Antwerp. For this company, however, no tax filings or annual accounts were found. The case files revealed that LTD2_B was involved in VAT fraud, money laundering, and the misuse of corporate assets. Although C1_B retained factual control, it appears that C6_B acted as a strawman. A bankruptcy case was opened in 2019 and closed in 2022.

- **LTD3_B** was established in 2013 in Antwerp and infiltrated by the network in 2015. Although the judicial files listed it as a food service establishment, the Crossroads Bank for Enterprises (CBE) revealed that the firm's stated corporate purpose was much broader. Among others, this included road haulage, gas and electricity distribution, highway construction, vegetable cultivation, and clothing retail. As it had never filed its mandatory annual accounts with the National Bank of Belgium, LTD3_B was removed from the registered in 2017. Bankruptcy proceedings were opened in 2018 and closed in 2020.

- **LTD4_B** was established by C1_B and two other parties in 2015 as a combination of a hospitality venue and a retailer of car and automotive components. Despite the initiation of bankruptcy proceedings in 2024, the company continues to operate in Antwerp.

- **LTD5_B**, an Antwerp business that presented itself as a legitimate wood importer, was set up by C1_B as a shell company and registered in the name of a strawman.[52] On paper, this business traded timber with a partner company in South America. By regularly shipping containers with full paperwork, the network had established a transport route under its own control, from origin to destination. Once this route had been labelled as 'low risk' by control services of the Port of Antwerp, the network could start using it to import cocaine.
- **LTD6_B**, a large company specialised in business and management consultancy, was established in 2012 in Antwerp.

3. Crime script based on Case Bravo

Motivation – Purpose

Within Case Bravo, the criminal use of legitimate businesses was primarily driven by the network's aim to generate **financial profit**. More specifically, the main motivation for infiltrating logistics company LTD1_B was to facilitate the import and storage of cocaine through the Port of Antwerp and to conceal criminal activities (using the 'switch method', cf. *infra*). Businesses in the hospitality industry, on the other hand, were used primarily to launder the illicit proceeds of cocaine sales. False invoices were used to disguise the actual nature of these sales, presenting them as legitimate business transactions of C1_B's company. However, these venues also served distribution purposes.

Background on the network's modus operandi

To understand the different phases of the crime script, a concise overview of the network's general *modus operandi* is provided here. In South America, criminal associates packed certain amounts of cocaine in sport bags and placed them in sea containers. The vessels then sailed to Antwerp, where, upon arrival, the network employed the well-known '**switch method**'.[53] Once the cocaine had been 'switched', complicit truck drivers transported the containers out of the port to a warehouse rented by the network, where the cocaine was being extracted. The driver then delivered the legitimate cargo, as specified in the paperwork, to the consignee.

Preparation

In the context of the 'preparation' phase, the criminal network focused on two areas. On the one hand, they looked for opportunities to gain access to insider information and operational control within the logistics chain of the Port of Antwerp. On the other hand, limited liability companies were established or acquired for the purpose of absorbing cash and generating documentary covers for future transactions.

[52] Although the case files did not contain any information regarding the date of LTD5_B's incorporation, intercepted encrypted communications indicate that it was established between 2019 and 2021.

[53] A switch container which, according to the documentation, is destined for a country within the EU, is placed next to a container originating from outside the EU (in this case, from South America) and containing cocaine. Subsequently, the extractors enter the premises and transfer the bags filled with cocaine to the switch container (Spapens et al., 2024).

Considering these objectives, the **logistics sector** was particularly attractive as port logistics companies have access to sensitive and time-critical information that can facilitate the importation of cocaine, including about container arrivals, container and seal identifiers, and delivery details. These opportunities were particularly evident in connection to LTD1_B, which operated inside the **Port of Antwerp**, the second largest port in Europe were container transport plays a major role (Port of Antwerp-Bruges, n.d.). The port's operational attractiveness is further increased by its open and relatively accessible nature, the reasonable possibility for bypassing the ANPR shield through taxis or rental cars, its location in two judicial districts, and its division over two shores. As a recognised logistics firm, LTD1_B also benefited from a legitimate reputation that reduced suspicions. Its large company size weakened peer oversight and social control, making it easier to dismiss minor scheduling changes as routine work. Its reliance on subcontracted transport firms further reduced control.

In addition, businesses in the **hospitality industry** were also infiltrated by the criminal network due to the sector's cash-intensive nature, steady flow of small transactions, low barriers to entry, fluid staffing and payroll arrangements, and significant potential for high revenues. Because of these characteristics, the hospitality sector was particularly suited for absorbing illicit cash and creating documentary covers. The car retail sector, too, offered attractive opportunities, as it is highly accessible and difficult for local authorities to monitor effectively.

More generally, however, the case files suggested that, for this criminal network, the economic sector itself was less important than the **legal form** of the businesses involved. Limited liability companies proved to be particularly attractive because they combine low start-up costs with a quick incorporation process, and control can be relatively easily transferred to a strawman who acts as a formal manager.

Pre-activity or enabling conditions

- **Logistics sector**
  The criminal network has infiltrated LTD1_B at the employee level. At least three employees (C4_B, C5_B, C6_B), all of whom were operators of the company's container planning system, became regular **facilitators**, as they had access to crucial information for the criminal business model. In addition, the network included several **lorry drivers** who worked for LTD1_B. They were bribed into cooperating, but it is unclear whether their initial cooperation was motivated solely by financial gain or whether they were also subjected to pressure. It is known that the collaborating drivers received a bribe of around EUR 50,000 per criminal operation. However, LTD1_B itself was (and still is) a *bona fide* company. Although port-adjacent logistics companies are generally aware that their employees may be targeted by criminal networks, the case files contained no evidence that LTD1_B was cognisant of the criminal activities in which any of its staff were involved. For that reason, the business was considered unwillingly complicit.
  In addition, the criminal network exploited the services of numerous other legitimate businesses without their knowledge. For example, particular containers belonging to companies that transported goods from South America to Antwerp were reportedly used for the international transportation of cocaine. Other companies' containers were deployed as switch containers and thus became an integral part of the network's criminal process.

- **Wholesale sector**
  After several shipments of cocaine had already been successfully extracted through the Port of Antwerp between 2019 and 2021, the criminal network gained confidence and sought to gain greater control over the entire import chain. Since its purpose was to establish a shipping line for **transporting timber** from South America to Antwerp and a façade of legitimacy was needed to do so, the network decided to found a private limited company (LTD5_B).

  The *modus operandi* used by the network to infiltrate LTD5_B is a well-known method in the criminal underworld, particularly in the context of drug trafficking, involving the **establishment** of a clean and predictable **trade route** before introducing illicit shipments. Officially, LTD5_B purchased timber in South America, which it then imported to Antwerp.[54] Over an extended period, the company transported only legitimate shipments, accompanied by complete documentation. When these consignments underwent customs scans and inspections, they consistently yielded negative results. As a result of repeated checks that revealed no irregularities, the trade route gradually acquired a low-risk profile. Once this status had been established, the network intended to use the route to transport cocaine, typically during periods of limited customs personnel availability. After importation, LTD5_B sold the timber at a profit, thereby maintaining the appearance of a legitimate and commercially viable business.

- **Hospitality industry and car retail sector**
  Alongside the acquisition of the existing company LTD3_B, C1_B deliberately established the businesses LTD2_B and LTD4_B with the purpose of using them as vehicles to gain **personal profit** and to facilitate the network's operations. The degree of criminal use in these companies can therefore be considered high. However, the case files contained no information regarding why these particular companies were selected or why they were established or acquired at those specific moments. Furthermore, the number of individuals employed in these companies remains uncertain, as well as their awareness of the illegitimate purposes of their workplace.

Activity

- **Logistics sector**
  A key element of the network's *modus operandi* regarding the criminal use of LTD1_B was the involvement of the regular **facilitators** C4_B, C5_B, and C6_B, who received instructions from C1_B, who was acting on behalf of C2_B and C3_B. To minimise the risk of detection by *bona fide* colleagues, C1_B provided these facilitators with encrypted laptops so they could carry out their tasks from home. Communication also took place regularly via encrypted devices.

  The operations proceeded as follows. First, C1_B informed the facilitators which of the incoming containers contained cocaine, after which they were tasked with identifying suitable 'switch containers' associated with LTD1_B. Steel containers were favoured because they were usually loaded to about one-third of their capacity, leaving space to transfer overfilled bags of cocaine without causing visible damage or leaving any traces on the legitimate cargo. After a switch container was selected, the facilitators removed it from the planning system of LTD1_B to prevent *bona fide* colleagues from assigning it to a legitimate driver. They then provided

[54] Timber was deliberately chosen as a cover, because effective detection often requires drilling into the wood.

C1_B with information on the switch container number, seal number, PIN code, and delivery address and created fictitious TAR codes.[55] Subsequently, transport assignments were given to complicit truck drivers: a corrupt lorry driver collected the container and transported it from the port to a warehouse that C1_B had rented under a straw person's name. The cocaine was extracted at the warehouse, after which the container was resealed with a cloned seal, and the driver delivered the remaining legitimate cargo to the intended recipient. As cooperation intensified, however, C1_B gained direct access to LTD1_B's computer systems via these facilitators, allowing him to manipulate the **container planning system** himself.

In addition, the judicial files documented cases of coercion when the facilitators hesitated or operations faltered. Following failed cocaine transports, intercepted messages included explicit threats of abduction, and C1_B threatened to physically assault a planner whom they believed would provide information to the police. These communications indicate that the network enforced compliance through corruption, intimidation, and threats of violence.

- **Wholesale sector**

  In its day-to-day operations, LTD5_B presented itself as an ordinary **timber wholesaler**. The company placed orders, received invoices, sold cover shipments to customers, and recorded payments. This created a consistent paper trail of legitimate commercial activity. Behind this façade, however, the same transport route and port access were intermittently used to transport cocaine hidden in shipping containers.

- **Hospitality industry and car retail sector**

  Through criminal business practices in the hospitality industry and car retail sector, the criminal network was able to commit VAT fraud and launder illicit proceeds.

  VAT fraud and money laundering through intra-Community vehicle acquisitions

  By using LTD2_B, the network was able to evade an estimated EUR 80,000 between 2016 and 2019. C1_B financed the purchase of second-hand vehicles in other EU Member States, mainly the Netherlands and Germany, using private funds and including more than EUR 130,000 in cash suspected to derive from cocaine trafficking. The remaining amount was paid in advance via bank transfer. The vehicles were purchased under LTD2_B's name and VAT number, allowing VAT-exempt **intra-Community acquisitions**.[56] C1_B subsequently resold the vehicles in Belgium, receiving payments partly by bank transfer to a personal account and partly in cash. These transactions were omitted from LTD2_B's accounts, and the VAT due was not declared. Judicial records identified at least twelve vehicles involved in this scheme combining cash payments, transfers to a private bank account and the misuse of the company's VAT number, thereby constituting VAT fraud and money laundering.

[55] Truck Appointment Reference (TAR) codes are pre-advice access codes or reservations to collect containers from the quay.
[56] An intra-Community acquisition refers to the purchase of goods by a VAT-liable person in one EU Member State, with the goods being transported from another EU Member State to the purchaser's Member State (European Court of Auditors, 2015). In principle, the supplier does not charge domestic VAT; however, the purchaser must report the acquisition and declare the VAT due in their own Member State while, in most cases, deducting it as input VAT at the same time.

Money laundering via hospitality accounts

LTD2_B and LTD3_B were used to launder drug trafficking proceeds by mixing illicit cash with legitimate **hospitality revenues** and depositing these funds into the companies' bank accounts. By combining lawful and unlawful sources of income, the illicit funds were funnelled into the financial system as legitimate business revenues. Moreover, LTD2_B was formally managed by a strawman; despite the official transfer of authority, C1_B remained the *de facto* manager of the company. In addition, C6_B received a salary from LTD2_B for fictitious employment.

TBML through fictitious invoicing

The judicial files documented a **TBML-scheme** involving LTD3_B and LTD6_B. In 2016, LTD6_B paid LTD3_B more than EUR 150,000 for alleged real estate consultancy services; however, according to the file, these payments actually represented the settlement of cocaine deliveries made by C14_B to C8_B. In this scheme, LTD3_B issued fictitious invoices that were recorded in LTD6_B's accounting records to justify the payments. This created a paper trail that disguised the criminal proceeds as legitimate business expenses, thereby integrating drug money into the regular financial system.

Post-activity or post conditions

The criminal activities involving the companies in question **lasted several years**. Regarding the logistics sector, Sky ECC communications indicated that the principal operational window occurred between 2019 and 2021. During this period, the network infiltrated LTD1_B through insider employees and carried out at least fourteen cocaine extractions. In the same timeframe, the shell company LTD5_B was established to develop a controlled timber supply chain and, subsequently, for selected shipments containing cocaine. However, intercepted communications only referenced 'bogus shipments' and provided no evidence of actual cocaine consignments. Consequently, it cannot be determined whether this route was ultimately used successfully for drug trafficking. In addition, companies in the hospitality industry and car retail sector (LTD2_B, LTD3_B, LTD4_B) served as the network's financial and documentary infrastructure for several years. Through these entities, the network succeeded in achieving its objectives: laundering illicit proceeds, committing VAT fraud related to intra-Community vehicle purchases, and creating a paper trail to disguise payments linked to cocaine trafficking.

Over time, there were some **red flags** pointing to the criminal use of these businesses, particularly in the wholesale, hospitality and car retail sectors. These include the use of strawmen, failure to file annual financial statements and corporate tax declarations, and the commingling of personal and business funds. Notably, LTD3_B exhibited a pattern indicative of a 'phoenix company arrangement', in which the business was deliberately wound down and reconstituted to evade liabilities. In the logistics sector, however, no indicators of corporate-level criminal infiltration were observed, as infiltration occurred at employee level than through corporate ownership structures. Employee-level indicators may include unusual or suspicious staff activity.

Ultimately, the **judicial investigation** was initiated in 2018 following a referral from the Belgian FIU. This referral flagged C1_B for indications of unexplained wealth, particularly in relation to property acquisitions and renovations between 2015 and 2017, despite no bank credit and reliance on welfare benefits until 2015. As part of subsequent law enforcement actions, C1_B's communications were intercepted and analysed, and numerous shipments were seized by customs and police authorities between 2019 and 2021. Following the proceedings, several members of the network were convicted.[57]

4. Financial profile of the criminal network involved in Case Bravo

Financing sources and start-up capital

Overall, C1_B systematically combined drug proceeds with VAT fraud and multiple money laundering schemes across his companies, using both personal and corporate accounts to circulate funds and conceal their illicit origin.[58] The primary source of **illicit income** was cocaine trafficking, originating from multi-tonne consignments through the Port of Antwerp. In addition, C1_B engaged in practices of VAT evasion and money laundering through schemes involving the intra-Community acquisition of second-hand vehicles. The resale of these vehicles generated both cash and bank transfers that were not recorded in LTD2_B's accounts. Through TBML, more than EUR 150,000 of criminal proceeds were disguised as legitimate business expenses.

On the other hand, in addition to these illegal activities, C1_B also reported **legitimate-looking income**. He owned rental properties, which were likely partially financed by illegal means, and he received rental income. Despite performing no work, he received monthly payments from ostensibly legitimate companies (EUR 1,500 per month from LTD2_B; EUR 2,500 per month from LTD4_B). Daily hospitality-related revenues from these businesses were commingled with illegal cash, creating the appearance of legitimate business turnover.

Payment methods and arrangements within the network

C2_B, identified as a drug lord and clan leader, supplied the network with substantial **sums of cash** that were physically transported between members by couriers, with cash drops typically arranged in car parks. For example, when C2_B needed to pay C1_B, a courier collected cash from C2_B and delivered it to a designated drop-off point, often using a stash vehicle, where another courier linked to C1_B collected the funds.[59]

Payments within the network were made **in cash or in kind**. For certain extractions of cocaine, members requested a percentage of the cargo rather than a fixed fee. Monetary payments were usually made upon completion of the work; in practice, however, this did not always happen immediately. Intercepted Sky ECC messages suggested that delays in payment caused tension among the core members of the network, out of fear that intermediaries would withdraw their cooperation.

[57] C1_B was convicted on several occasions: in 2016 for participating in a criminal organisation, in 2023 for the importation of narcotics and related offences (*in absentia*), and in 2024 for forgery, money laundering, and VAT fraud in connection with this case (*in absentia*). Open-source records indicate that other network members, notably C2_B and C3_B, have also been convicted of various criminal offences.

[58] As the judicial files are structured around C1_B, the financial analysis in this section also focuses on the resources and money flows of this specific network member.

[59] Recorded transactions of this type included amounts of EUR 165,000, EUR 195,000, and EUR 215,000, suggesting that the network regularly managed significant cash balances.

Costs of business operations

On the one hand, general corporate infrastructure costs were incurred. The incorporation of LTD2_B and LTD3_4 and the acquisition of LTD3_B involved costs related to notarial acts, licences, bank account management, and changes to the registered office, insurance, and utilities over time. On the other hand, additional costs were associated with the network's specific criminal activities. The costs of organising **cocaine extraction operations** varied, ranging from EUR 80,000 to EUR 230,000 per operation. Individuals responsible for removing the cocaine from the containers received EUR 100,000 if the extraction was successful, and EUR 30,000 if customs intercepted the consignment. Complicit truck drivers were usually paid around EUR 50,000 per run. To remove the cocaine, the network also rented an off-site warehouse. The lease was registered in the name of a strawman, which generated additional costs for rent, utilities, and basic security. The network also paid the so-called 'Sky Man' who provided encrypted phones and required communication subscriptions.

The cover-up **timber transport route** required initial investments. Before any illicit shipments were made, LTD5_B financed legitimate timber consignments to establish a low-risk trading record. The costs associated with these cover shipments included the purchase of timber, inland transportation fees, port handling charges, customs duties, and routine administrative expenses. LTD5_B's start-up and customs-related costs amounted to at least EUR 65,000. Moreover, to maintain its legitimate appearance and credibility, ongoing expenses were incurred: the company was registered, a straw owner was compensated, and a vehicle and minimal branding were maintained.

Revenues and proceeds

The network's main revenue stream is the **sale of cocaine** following its successful import from South America. Encrypted communications use EUR 1,5 million as a benchmark for the proceeds from the import and sale of a one-tonne shipment of cocaine. Additional revenue derives from vehicle sales linked to the VAT scheme, hospitality takings mixed with illicit cash, and property rentals.

5. Harms caused by Case Bravo

Harms to individuals

Employees of LTD1_B who facilitated the network's activities were exposed to intimidation and threats of violence, including references to the use of firearms, creating sustained fear and uncertainty among those involved. In addition, complicit truck drivers and other facilitators responsible for extracting and transporting illicit consignments faced considerable personal risks arising from their participation in criminal operations. Case Bravo also indicates broader risks to individuals connected to businesses associated with the network. Violent incidents targeting hospitality venues linked to the network (LTD2_B, LTD4_B) exposed *bona fide* employees, customers, and bystanders to potential physical harm and psychological distress.

Harms to other businesses

Insider corruption within LTD1_B poses a significant reputational risk to the company, given its position as a major logistics operator. In addition, legitimate businesses whose containers were unwittingly used for switching may face negative repercussions, including delivery delays, cargo damage, additional inspection-related costs, and potential contractual penalties. Similarly, LTD6_B, a prominent actor in its sector with substantial projects in Antwerp and established political connections, faces considerable

reputational harm as a result of its association with Case Bravo. Its involvement raises questions about the company's credibility and integrity.

In the hospitality and car retail sectors, the main consequences of VAT fraud and money laundering, as well as the use of shell companies, are unfair competition and financial losses for legitimate counterpart businesses. Sham or criminally used companies can gain an unfair competitive advantage over compliant businesses by evading taxes, thereby distorting market prices and undermining fair commercial practices.

Harms to public institutions

Public institutions are affected by VAT evasion, resulting in direct losses to the treasury. Customs and other control services at the Port of Antwerp are similarly affected, as they must devote substantial time and personnel to inspecting dummy consignments and investigating switch operations. The network also appears to have exploited capacity constraints by scheduling cocaine shipments towards the end of the year, when customs staffing levels are typically lower. This deliberate timing placed additional strain on control services and diverted resources from other enforcement priorities. Furthermore, allegations of customs corruption emerged from intercepted communications within the network, in which C1_B claimed to maintain multiple connections with cooperative customs officials. Nevertheless, no independent evidence has been identified to substantiate these allegations.

Harms to the physical environment

The wood import front relied on timber shipments that were reportedly intended to conceal cocaine. The proposed concealment method, which involved drilling into the timber, had the potential to damage the wood, potentially rendering the cargo unsellable or resulting in its complete destruction once the narcotics had been removed. However, the case file does not confirm that this trade line was actually used for cocaine trafficking. Consequently, there is no recorded evidence of direct ecological harm.

Harms to the social environment

Gun attacks targeting hospitality venues caused public nuisance, heightened fear, and an increased sense of insecurity among local residents. In addition, criminal activity within the hospitality sector further erodes public trust in local businesses. Furthermore, the intimidation of internal facilitators may discourage *bona fide* colleagues from reporting misconduct, due to fear of retaliation or social pressure.

Annex 1.C – Case Charlie: From Cannabis to Concrete

1. Criminal network involved in Case Charlie

Case Charlie concerns a wider **international clan** centred around C1_C, his brother and cousins. The network is known to have been involved in the production and trade of cannabis and can be linked to ongoing investigations in numerous European countries, including Germany, the Netherlands, and Spain. However, the Belgian case discussed here covers only a small part of that larger network, focusing particularly on the criminal use of two legitimate businesses (LP1_C, LP2_C) in Antwerp. Table 6 provides an overview of the members involved in this network.

Table 6
Overview of the members of the criminal network involved in Case Charlie (Antwerp)

Member	Role	Gender	Born between	Nationality
C1_C	Leader	Male	1954-1973	Turkish
C2_C	Money launderer	Male	1974-1993	Belgian
C3_C	Intermediary	Female	1954-1973	Belgian
C4_C	Intermediary	Female	1994-2007	Belgian
C5_C	Intermediary	Female	1994-2007	-
C6_C	Intermediary	Male	1994-2007	Dutch
C7_C	Strawman; Financial management	Male	1974-1993	Turkish
C8_C	Strawperson; Intermediary	Female	1974-1993	Belgian
C9_C	Intermediary	Male	1994-2007	Turkish
C10_C	Intermediary	Male	1974-1993	Belgian
C11_C	Strawman of LP1_C	Male	-	Bulgarian
C12_C	Strawman of LP1_C	Male	-	Bulgarian
C13_C	Intermediary	Female	-	-
C14_C	Intermediary	Male	-	-
C15_C	-	Female	-	-

Family ties formed the core of the network. Furthermore, this network turned out to have a clear hierarchical structure centred on C1_C, the leader and patriarch, who issued instructions, decided on the allocation of resources, and determined who would occupy key positions within the companies and among the intermediaries. Despite controlling substantial real estate assets, he appeared insolvent by placing them in the names of his wive and children.

In addition to C1_C's leadership role, the other **roles in the network** were also clearly defined. The core group consisted of around eight individuals, supported by a flexible network of intermediaries who were mobilised as needed to facilitate transfers and conceal the origin of illicit funds. While C2_C, a jurist without criminal record, received funds and invested these in real estate and cryptocurrency, C7_C managed the companies' finances on behalf of the network and transferred funds from corporate accounts to intermediaries (see Figure 3).

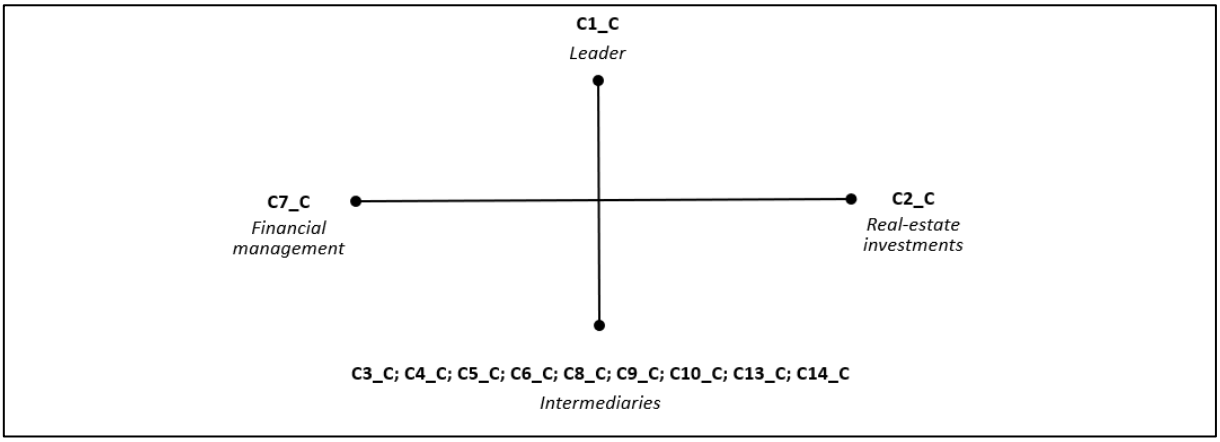


Figure 3
Structure of the criminal network involved in Case Charlie (Antwerp)

The wider clan around C1_C appeared to be **highly resilient** and had an established presence across several European countries. Furthermore, various network members had prior convictions, such as participation in a criminal organisation and drug offences. Initially, C7_C and C8_C appeared to have had genuine entrepreneurial intentions after being recruited by the network in a bar. They were promised support in establishing a (legitimate) company but, however, were subsequently pressured into providing their bank accounts and identities to the network. Both reported fearing C1_C and receiving threats, with their involvement evolving from naïve participation as strawman to knowing facilitation under intimidation.

2. Legitimate businesses involved in Case Charlie

The criminal network's money laundering scheme used small **limited partnerships** (LP) as the legal structure for the companies involved.

- **LP1_C** was established in 2021 in Antwerp by C7_C, the majority shareholder, and C8_C as a silent partner. Its registered activities involved the retail sale of building materials, hardware, glass, and paint. In practice, however, LP1_C carried out legitimate activities only to a limited extent, mainly small painting jobs executed by C7_C and C8_C. No staff members were officially registered as employees. From the outset, the company failed to file VAT returns, customer and supplier lists, or any accounting or fiscal documentation. Bankruptcy proceedings were initiated in 2023. By this time, C7_C and C8_C had resigned as managers and been replaced by foreign straw managers. In practice, the announced transfer of control to these new managers did not take place, and factual control remained in the hands of members of the network.
- **LP2_C** was established in 2022 in Antwerp by C9_C, the majority shareholder, and C7_C as a silent partner. Its stated purpose was the purchase and sale of real estate, the rental thereof, the trade of building materials, and general renovation work. LP2_C did not file VAT returns or other accounting documentation and only had a limited duration period, closing in 2025 after liquidation.

3. Crime script based on Case Charlie

Motivation – Purpose

Within Case Charlie, the criminal use of LP1_C and LP2_C was primarily motivated by the purpose of concealing the origin of illicit funds and integrate them into the legitimate economy. The predicate offence is the cultivation of and trafficking in cannabis by the wider criminal clan. As the judicial files did not provide information on the broader criminal process, it can only be concluded that both companies were used at the **money laundering** stage.

Preparation

The network has chosen to infiltrate small **construction firms**, making false invoices schemes appear plausible by credibly issuing invoices for building materials or labour without extensive documentation, on-site inspections or visible staff. Moreover, it was relatively straightforward to register multiple employees at such companies, even if no actual work was being performed, thereby creating additional opportunities for fictitious wage payments and cash flows through the payroll. This combination of features enabled the network to process illicit funds through business processes that are common and seeming plausible in the sector.

In addition, the network exploited the characteristics of **limited partnerships**, such as their limited transparency and lenient regulatory regime. Due to the absence of a minimum capital requirement and the possibility to incorporate a company through a private agreement, initial oversight is less stringent. By using a silent partner, the actual beneficiary can remain hidden, while on paper a strawman acts as the managing partner.

Pre-activity or enabling conditions

Both companies were primarily established and managed as vehicles for moving and disguising criminal income, rather than as genuine commercial enterprises. Neither LP1_C nor LP2_C maintained customer or supplier lists or prepared accounting or tax records. Payments recorded as wages or loans were made to family members and associates without any professional link to the companies, and no payroll declarations or loan agreements were issued. Furthermore, the cooperation of some network members was not entirely voluntary, as this case falls somewhere between deliberate cooperation and **coerced facilitation**.[60]

In addition, the network succeeded in obtaining a set of customer companies, mainly Turkish, that appeared to have normal commercial relationships with LP1_C and LP2_C. In practice, however, they acted as counterparties in a **trade-based money laundering** scheme: at least seven of these customer firms transferred amounts to LP1_C that could not be matched to prior invoices or credited balances on their own accounts.[61] In other cases, clearly false invoices were used. For example, LP1_C received an invoice for six hundred work trousers and work gloves, even though it had no registered staff.

Activity

As neither LP1_C nor LP2_C maintained customer or supplier lists or produced accounting or fiscal documentation, the process of criminal use was reconstructed almost entirely based on on-site inspections and bank statements. LP1_C was found to have conducted limited **legitimate activities**, mainly minor painting work by C7_C and C8_C, while C1_C made cash payments to certain workers. As these cash transactions were unrecorded, the extent of lawful operations remains unclear. Based on inspections, police officers concluded that LP2_C carried out little to no genuine economic activity.

Based on the available information, the criminal use of LP1_C and LP2_C can be described as follows:

- **Step 1: Creating inflows into LP1_C through customer firms**
  As noted above, the network had designated a number of existing firms as customers, which made significant transfer to LP1_C, ranging from EUR 75,000 to over EUR 430,000 per firm. The judicial files did not clarify how these firms obtained the funds subsequently transferred to LP1_C. One plausible explanation is that the network first supplied cash derived from cannabis trafficking, which was channelled back to LP1_C via bank transfers supported by false invoices.

[60] Initially, C7_C and C8_C appeared to be entrepreneurs who failed to ask critical questions, but their role later shifted towards deliberate facilitation. Although structurally used as strawmen, they knowingly allowed their accounts and companies to be used once they became aware of the scheme. However, their voluntariness was not straightforward, given reported fear and threats from C1_C.

[61] Since the customer firms were not the primary focus of the judicial investigation, their awareness of involvement in the laundering scheme is difficult to assess. Their level of culpability likely varied. Some appear to have had clear personal or professional links to clan members and may have knowingly facilitated false invoicing or undocumented payments, while others may have engaged in transactions without being aware of their criminal context.

- **Step 2: Layering inside LP1_C and routing via intermediaries**
  Once the funds had been credited to LP1_C's account, they were recorded as ordinary business income or as funds available for payroll. From there, the money was transferred to members of the network and intermediaries who had no actual employment or service relationship with LP1_C. The network's leader, C1_C, decided who received money and how much, while C7_C executed the transfers and managed all financial streams. Outflows were recorded as wages or loans, yet no loan agreements, interest terms, or repayment schedules existed. In a normal business context, such undocumented lending would be highly unusual. Here, the absence of any contractual framework or repayment plan strongly suggests that both wages and loans were sham arrangements designed to conceal the distribution of cannabis proceeds.

- **Step 3: Integrating money into the legal economy**
  Ultimately, funds were channelled into C2_C's accounts via intermediaries. Increases in these balances closely preceded purchases of real estate. In many cases, transfers were converted into property on the same day or shortly thereafter. C2_C also invested part of the proceeds in cryptocurrency. Rental income from the properties and gains from crypto trading then generated additional, ostensibly legitimate income.

- **Step 4: Continuity**
  On paper, LP1_C was transferred to new managers, but this change was purely formal: strawmen were appointed while the network retained effective control. In the lead-up to bankruptcy, LP1_C concentrated unexplained inflows and channelled funds to private accounts and intermediaries. Assets were stripped before liabilities crystallised, preventing creditors and public authorities from recovering their claims. In the Belgian context, this is consistent with bankruptcy offences and fraudulent insolvency, as company funds were diverted for private benefit while debts remained unpaid. Alongside these transfers, the network operated a cash compensation scheme, using cannabis proceeds to finance renovations of acquired real estate and paying contractors and construction workers entirely in cash. This enabled the simultaneous laundering of criminal proceeds and the commission of social and fiscal fraud.

Post-activity or post conditions

The Belgian inquiry into LP1_C and LP2_C was initiated as a criminal execution investigation following C1_C's conviction in another EU Member State for drug offences.[62] During this period, the network converted a substantial share of the cannabis proceeds into ostensibly legitimate assets. The **judicial inquiry** estimated that the entities involved had unlawfully obtained at least EUR 2.2 million through LP1_C and more than EUR 220,000 through LP2_C.

[62] A 'criminal execution investigation' (in Dutch: *strafuitvoeringsonderzoek*) was introduced to address cases in which defendants in large-scale proceedings are sentenced to high fines and confiscations, yet appear to possess few or no assets that can be seized because they have impoverished themselves artificially, for example by hiding property abroad or transferring it to third parties (Van den Wyngaert et al., 2019).

Over time, there were some **red flags** pointing to the criminal use of these limited partnerships. For example, VAT returns were missing and there were no statutory accounts or lists of customers and suppliers. Company funds were transferred to family members with no professional connection to the firms. Payments were recorded as wages despite the absence of corresponding payroll declarations in the recipients' personal tax records, and loans were documented without contracts or repayment schedules. Transfers from customer firms to LP1_C consisted almost systematically of rounded monthly amounts. Investigators noted that non-rounded figures would have appeared more consistent with genuine payments for specific deliveries and therefore less suspicious. Announced ownership changes in the corporate registry did not result in any effective transfer of control. After LP1_C went bankrupt, LP2_C emerged with the same key figures and similar patterns of unexplained inflows and outflows, which further heightened suspicions.

4. Financial profile of the criminal network involved in Case Charlie[63]

Financing sources and start-up capital

The network's principal source of funding was the proceeds of **cannabis cultivation and trafficking**. The accounts of LP1_C and, later, those of LP2_C served to channel these proceeds to private beneficiaries and to convert them into real estate and, to a lesser extent, cryptocurrency. A substantial part of the revenue consisted of false invoices and undocumented payments from so-called customers of LP1_C. At least seven entities transferred a total of more than EUR 1.2 million in amounts that could not be linked to previous invoices or credit balances in their own accounts. Additional flows included frequent cash deposits and a public bridging loan of EUR 50,000, which was intended to support LP1_C but was largely diverted to a private account and to the purchase of a car, and was never repaid. LP1_C also conducted limited legitimate activity, although its precise nature and scale remain unclear.

Payment methods and arrangements within the network

The judicial files provided little insight into how members and intermediaries were remunerated for their involvement in the scheme. For example, there is no indication that they received fixed commissions or fees for the use of their bank accounts or identities. The available information primarily concerns the movement of funds for laundering purposes rather than internal compensation arrangements. One concrete detail that did emerge, however, concerned the use of cash couriers: cash was physically transported to Turkey on behalf of C1_C by travellers who received a free airline ticket and a small fee in return.

Costs of business operations

The case files did not provide a detailed breakdown of the costs associated with the money laundering scheme. Nevertheless, such costs could be inferred from company formation and maintenance, the use of strawmen, routine banking operations, and the couriering of cash.

[63] As the case files covered only a small segment of a much larger international clan, the full financial profile of the criminal network could not be reconstructed. Even within this segment, the picture remains incomplete, as not all financial flows can be traced from source to final destination.

Revenues and proceeds

The identified asset diversions amounted to over EUR 2.2 million in relation to LP1_C and approximately EUR 220,000 in relation to LP2_C. The judicial files identified **four recurring mechanisms** through which value was extracted from the companies. First, false invoicing and undocumented customer payments generated credits on LP1_C's account, despite the absence of underlying trade. Second, sham wages were paid to family members and associates with no professional connection to the firm. Third, loans were granted without contracts, interest, or repayment schedules, facilitating transfers to intermediaries and C2_C. Funds credited to C2_C's accounts were swiftly converted into real estate and, to a lesser extent, cryptocurrency holdings. Rental income from these properties and profits from cryptocurrency transactions subsequently generated further income streams that appeared legitimate. Fourth, in the pre-insolvency phase, assets were systematically extracted from LP1_C in anticipation of bankruptcy. This pattern continued subsequently through LP2_C.

Financial investigation

As mentioned above, the Belgian investigation into LP1_C and LP2_C was initiated following C1_C's conviction in another EU Member State for drug offences. Investigators reconstructed the money flows, mainly based on bank statements from LP1_C, LP2_C, and key individuals' personal accounts. The investigation remains ongoing. Although the main suspects are currently at liberty, the financial reconstruction is already supporting asset recovery efforts and may underpin further proceedings against related companies and individuals.

5. Harms caused by Case Charlie

Harms to individuals

Initially intending to establish a legitimate business, C7_C and C8_C became coerced facilitators, with their identities, companies, and bank accounts being used to channel criminal funds. They reported receiving threats from C1_B, suggesting that they were subjected to exploitation and coercion.

Harms to other businesses

The criminal use of LP1_C and LP2_C created unfair competition within the construction and real estate subsectors. The companies were able to record inflows without conducting genuine trade by relying on false invoicing and undocumented customer payments, while circumventing tax and social security obligations.

Harms to public institutions

Public institutions incurred direct losses as a result of foregone tax revenue at LP1_C and LP2_C. Furthermore, LP1_C misused a public loan administered by the Flemish Agency for Innovation and Entrepreneurship and the investment company of the Flemish Government in 2022. LP1_C obtained a EUR 50,000 bridging loan intended for Flemish firms facing acute liquidity needs as a result of crisis-related price and energy shocks. These funds must be used for essential business activities (VLAIO, n.d.). However, immediately following disbursement, EUR 25,000 was transferred to C7_C's personal account, while EUR 12,500 was used to finance a car purchase. The government consequently incurred a direct financial loss, as the loan was never repaid.

Harms to the physical environment

The file does not document any direct environmental harm linked to LP1_C and LP2_C. However, the international network surrounding C1_C is involved in cannabis production, which may have local environmental impacts such as electricity theft, chemical waste and water pollution.

Harms to the social environment

Sustained money laundering through family-controlled companies can erode trust in public institutions and the local business environment. Furthermore, repeated real-estate purchases for money-laundering purposes may distort local housing markets. The visible presence of financially successful family members with a known criminal background, combined with limited visible enforcement, may foster perceptions of impunity and undermine confidence in the rule of law.

ANNEX 2

BRUSSELS

DETAILED CASE STUDIES

Annex 2.D – Case Delta: The Brussels Brazilian Filière

1. Criminal network involved in Case Delta

Case Delta concerns a criminal network centred around C1_D and his family members. The network is known to have been involved in money laundering practices through cash compensation schemes. Such schemes constitute **service-based money laundering** (SBML), a particular form of TBML in which services, rather than goods, are used in commercial transactions to launder money (Snaphaan et al., 2025). Criminal actors holding large volumes of illicit cash are linked with companies seeking to pay workers off the books. In this case, the network connects these complementary needs and acts as an intermediary by providing financial services to both parties, thereby facilitating a range of criminal activities. For this purpose, the network involved in Case Delta used two accounting firms (LTD1_D, GP1_D) in Brussels. Table 7 provides an overview of the core members of this network.

Table 7
Overview of the core members of the criminal network involved in Case Delta (Brussels)

Member	Role	Gender	Born between	Nationality
C1_D	Leader	Male	1954-1973	Belgian
C2_D	Leader	Male	1994-2007	Belgian
C3_D	Facilitator	Female	1974-1993	Belgian
C4_D	Leader	Male	1994-2007	Brazilian
C5_D	Facilitator	Female	1994-2007	Belgian
C6_D	Facilitator	Male	1934-1953	Belgian
C7_D	Facilitator	Male	1994-2007	Brazilian
C8_D	Cash courier	Male	1994-2007	Brazilian
C9_D	Cash courier	Male	1994-2007	Brazilian
C10_D	Facilitator of money transfers	Male	1954-1973	Brazilian
C11_D	Cash courier	Male	1994-2007	Brazilian
C12_D	Cash courier	Male	-	-
C13_D	Director of LP1_D	Male	1954-1973	Portuguese
C14_D	Supplier of cash derived from drug trade	Male	1954-1973	Dutch
C15_D	Money transfers	Female	1974-1993	Belgian

In total, the juridical files identified 81 individuals as being linked to core members of the network or involved companies. This network turned out to have been **centred around C1_D**, a known criminal with prior convictions for participation in a criminal organisation, document and VAT fraud, and money laundering. Following his professional ban in 2020, rather than withdrawing from economic activity, he repositioned himself in the background and continued to direct operations through close relatives and trusted associates, primarily via two accounting firms (LTD1_D, GP1_D). Through his inner circle, he maintained an extensive network of contacts with clients and partners in Belgium, the Netherlands, Portugal, and Brazil.

While C1_D was in custody in connection with another judicial investigation, his stepson (C2_D) and associates further coordinated the money laundering operations. This succession of leadership generated tensions, with C1_D accusing C2_D of building a competing structure based on C1_D's contacts and expertise without adequate remuneration. The structures surrounding both criminals were linked to a broad range of individuals with criminal intentions and made use of the same corporate vehicles. They are therefore better understood as a **single, large criminal network** comprising several partially autonomous branches or cells, rather than as distinct groups.

Between 2021 and 2023, C2_D and C4_D emerged as the **network's key coordinators** in Brussels, the Netherlands, Portugal, and Brazil. They organised and supervised cash transports carried out by money couriers, ensuring that cash collected from clients was delivered to providers of fictitious invoices, who in turn executed compensating bank transfers. Within LTD1_D and GP1_D, two key members managed the financial flows, while another individual worked for both entities and also held shares in LTD1_D, assisting the creation of corporate structures for organised criminals. Other members performed more specific operational roles, such as executing money transfers or providing bank accounts used for laundering transactions. With regard to the origin of the cash, one actor was identified as a supplier whose funds were presumed to derive from drug trafficking, while another was identified as a client whose funds were presumed to originate from prostitution.

2. Legitimate businesses involved in Case Delta

The judicial files linked the network to **more than a hundred** Belgian and foreign **companies**. As it is neither feasible nor desirable to describe them all, this case study focuses on nine businesses. Some operated exclusively as shell companies within the money laundering scheme, while others combined money laundering activities with their legitimate commercial operations. The judicial investigation identified **LTD1_D and GP1_D** as key facilitators responsible for establishing and managing structures used in complex money laundering schemes. Table 8 provides an overview of the most relevant companies involved.

Table 8
Overview of the businesses involved in Case Delta (Brussels)

Company	Economic sector	Status in 2025	Location
GP1_D	Accounting	Active – Bankruptcy opened	Belgium
GP2_D	Construction and cleaning	Active	Brussels, Belgium
LP1_D	Construction and cleaning	Bankrupt	Brussels, Belgium
LTD1_D	Accounting	Active	Brussels, Belgium
LTD2_D	Construction and cleaning	Active – Bankruptcy opened	Brussels, Belgium
LTD3_D	Construction	Unknown	Brussels, Belgium
LTD4_D	Construction and cleaning	Bankrupt	Belgium
LTD5_D	Real estate	Unknown	Portugal
LTD6_D	Real estate	Unknown	Portugal

GP1_D, an accounting firm, was founded in 2016 and had been operating as a general partnership since 2020. The firm also functioned as a bookkeeping office and was closely linked to LTD1_D through shared shareholders and employees. Over time, the shares shifted among C1_D's family members. The company entered bankruptcy proceedings in 2024, although it was still operational at the time of the judicial investigation.

LTD1_D is a private limited company with two branches, one of which is located in Brussels. It was founded as an accounting firm in 2020 and was still active in 2025, with C5_D serving as CEO. All customers of the company were analysed as part of the judicial investigation, as they were considered potential users of the compensation scheme facilitated by LTD1_D (i.e., companies that needed cash to pay off-the-book employees). A total of 478 clients were identified. Of these, 74 companies (15%) were linked by the Belgian authorities to criminal offences in 2023, primarily related to money laundering.[64] Most of these businesses operated in the construction, cleaning, and transportation industries.

Moreover, GP1_D and LTD1_D held **mandates** for 432 companies that were classified as 'dubious' within the judicial files. In at least 53 deeds of incorporation, clients appointed GP1_D and/or LTD1_D as special representatives with extensive powers, including the authority to communicate with third parties, sign contracts, and conduct checks on behalf of the company. In practice, this meant that C1_D and his entourage exercised effective control over these companies. Many of these entities also appeared in other referrals by the Belgian FIU relating to the '**Brazilian *filière***', where they were associated with serious indicators of money laundering, social fraud, and tax fraud.[65] The compensation scheme thus relied on a constellation of companies that either required cash or functioned as buffers. Examples of businesses investigated in the judicial files include the following:

- **GP2_D** is a Brussels-based general partnership operating in the construction and cleaning industries. The firm's bank accounts displayed the typical profile of a user of the compensation system, including outgoing transfers to previously identified shell companies with no genuine economic activity. GP2_D was still active in 2025.
- **LP1_D** was a limited partnership established in 2020 in Brussels and registered for construction and industrial cleaning activities. The firm constituted another link in the compensation scheme and was closely connected to LTD3_D, from which it received substantial funds. The bankruptcy proceedings were closed in 2023.
- **LTD2_D**, a Belgian company located near Brussels, was created in 2020 by C2_D. On paper, the company operated in the cleaning and construction sectors. In reality, however, it was a shell company with no genuine economic activity or employees. It was used exclusively to issue fictitious invoices and receive compensating bank transfers within the cash compensation scheme. Bankruptcy proceedings were initiated in 2024.

[64] Most of these businesses were private limited companies (46%), followed by general partnerships (35%), cooperative societies (12%), and a minority were public limited companies (6%).

[65] The term '**Brazilian *filières***' is commonly used in Belgium to describe professional, often transnational, money laundering networks that use company structures and cash compensation schemes to move and disguise criminal proceeds. Although the term originally referred to cases involving Brazilian-Portuguese networks, it is now used more broadly to describe such schemes, regardless of the ethnic background or type of crime involved (CFI, 2021a; Van Maele, 2023).

- **LTD3_D**, a Brussels-based construction company, was established in 2018 and owned by a strawman. A report of the Belgian FIU in 2020 flagged the company as a key node in a larger money laundering network in the Portuguese and Brazilian milieu.
- **LTD4_D**, a 'Brazilian *filière'* company, was established in 2012 and operated in the construction and cleaning sectors. From 2021 onwards, the position of manager was held by a strawman who abruptly assumed managerial roles in four businesses linked to the network, some of them located far from their place of residence. LTD4_D's bankruptcy proceedings concluded in 2025.
- **LTD5_D** and **LTD6_D** were Portuguese companies controlled by C1_D's family members. Although they were officially active in the real estate sector, the file indicated that they have never engaged in genuine commercial activity.

3. Crime script based on Case Delta

Motivation – Purpose

The main purpose of the criminal network was to **generate profit** by offering professional money laundering services to a wide range of criminal clients. The network monetised its intermediary role within the cash compensation system: they charged commissions to criminal actors seeking to convert illicit cash into legitimate bank funds, as well as to companies requiring cash to pay undeclared labour.

Preparation

The network involved in Case Delta operated as a facilitator in cash compensation schemes by exploiting vulnerabilities in Brussels' **construction and cleaning industries**. These sectors are known to be susceptible to social and fiscal fraud, money laundering, and social dumping, and are linked to criminal activities such as human trafficking and economic exploitation. Moreover, the construction and cleaning sectors are labour-intensive, highly price-competitive, and characterised by substantial labour payments and comparatively weak regulation in day-to-day practice (CTIF-CFI, 2024b). Complex chains of subcontracting and extensive reliance on temporary, flexible, and migrant labour are also common.[66] Consequently, these sectors provide a legitimising environment for false invoicing linked to fictitious services or labour, increasing their vulnerability to criminal interference (Snaphaan et al., 2025). In addition, high social security contributions in Belgium, combined with persistent demand for low-cost cleaning and construction work, create conditions in which fully regular employment is financially challenging.

In this case, the criminal network exploited these conditions by organising a cash compensation scheme through **accounting firms**. Services such as company incorporation, financial planning, registration in the Crossroads Bank for Enterprises, VAT formalities, the provision of registered office addresses, and payroll administration are essential to legitimate entrepreneurship. However, these functions can also be (mis)used to construct complex corporate chains for money laundering purposes (CTIF-CFI, 2024b). Over time, the Belgian FIU had repeatedly warned that specialised intermediaries, including accountants, tax advisers, and corporate service providers, may facilitate money laundering by assisting in the establishment and management of company structures, bank accounts, and

[66] Whereas companies in these sectors previously relied on cash flows from customer payments or bank withdrawals, these practices have become increasingly restricted, including through the Money Laundering and Terrorist Financing Prevention Act (Snaphaan et al., 2025).

administrative documentation. In Case Delta, GP1_D and LTD1_D occupied precisely this intermediary role, providing the organisational infrastructure underpinning the compensation scheme.

Pre-activity or enabling conditions

The network invested in establishing and controlling a set of companies that functioned as **facilitators**, users, and buffers within the compensation scheme. GP1_D and LTD1_D were founded as accounting firms by C1_D and his close relatives. Their activities extended beyond standard bookkeeping and tax compliance, as they were involved in the **incorporation and management** of several hundred companies over a two-year period.[67] Clients paid incorporation fees in cash, typically between EUR 3,500 and EUR 4,000 per company. Around half of these amounts were not recorded in the official accounts, thereby constituting tax fraud. In at least 53 incorporation deeds, clients explicitly appointed LTD1_D and/or GP1_D as special representatives with far-reaching powers. Through these mandates, C1_D's family members and trusted employees were authorised to act on behalf of the companies, sign contracts, open and close bank accounts, and engage with authorities. The judicial files documented that at least 27 of these incorporations involving strawmen were specifically established for money laundering purposes. GP1_D, LTD1_D, and shell companies such as LTD2_D can thus be considered as fully criminally owned and knowingly and voluntarily used in line with the network's business model.

Alongside these key intermediaries, the criminal network positioned several companies within the 'Brazilian *filière'* as **users and buffers** in the system. In the judicial files, a number of firms (including GP2_D, LP1_D, LTD3_D, and LTD4_D) appeared to have been nodes or end users of the compensation scheme. Moreover, foreign businesses (such as LTD6_D) were established to introduce an additional foreign layer in the laundering process, functioning as buffer companies in Portugal. At the managerial and transactional levels, it is reasonable to assume that there was deliberate and voluntary participation in the laundering scheme, even though not all managers may have been aware of the full extent and international reach of the network. However, the judicial files did not clarify whether customers of these construction and cleaning firms – acting as first-tier contractors – were aware that part of the funds paid for legitimate work was being diverted through compensation structures. For some upstream clients, the scheme may have been used intentionally; for others, it may have remained hidden behind seemingly ordinary subcontracting chains.

Activity

The network managed a chain of legitimate businesses as part of a structured **service-based money laundering** (SBML) scheme. Its day-to-day operation can be described as a sequence in which the physical movement of cash was linked to corresponding bank transfers via specific firms.

- **Step 1: Client recruitment and corporate infrastructure**
  From the offices of GP1_D and LTD1_D, C1_D and his relatives built and managed the corporate infrastructure underpinning the scheme. Staff at these accounting firms recruited clients, incorporated new companies, maintained bookkeeping records, and coordinated invoicing flows. They served both regular clients and Brazilian *filière* companies (e.g., GP2_D, LP1_D, LTD3_D, LTD4_D), as well as shell and buffer companies (e.g., LTD2_D, LTD5_D).

[67] To attract clients, the network had positioned itself through GP1_D and LTD1_D as specialised accounting firms for **Portuguese-speaking entrepreneurs in Brussels**. LTD1_D's marketing materials and social media presence were explicitly targeted at this audience.

- **Step 2: Matching of demand and supply and collection of cash**
  The network then matched two types of clients: on the one hand, criminal actors holding surplus illicit cash from drug trafficking, sexual exploitation, and other offences; and on the other hand, Brazilian *filière* construction and cleaning firms requiring cash to pay undeclared workers. Once amounts and dates had been agreed, money couriers collected the cash, mainly in the Netherlands and Brussels. Handovers took place in large car parks of shops and hotels, where bags of banknotes were exchanged. The couriers delivered the collected cash to Brazilian *filière* companies participating in the scheme. These companies used part of the cash to pay undeclared workers on construction sites and cleaning contracts. In this way, they obtained the cash required without making conspicuous withdrawals from their own bank accounts.

- **Step 3: Issuing of fictitious invoices and compensating transfers to shell and buffer companies**
  In parallel, the banking side of the compensation scheme was organised from GP1_D and LTD1_D. C1_D, C2_D, and their staff coordinated the production of fictitious invoices and the timing of transfers. Brazilian *filière* companies issued invoices pretending to cover construction or cleaning services and, on this basis, executed bank transfers to shell and buffer companies. LTD2_D was a central example: it received repeated transfers from LP1_D, LTD3_D, and other *filière* firms, all jusitifed by such invoices, despite LTD2_D having no staff, equipment, or genuine activity.

- **Step 4: Onward transfers by buffer companies, compensation, and international layering**
  However, buffer companies did not retain the funds, as their role was to transfer the money in accordance with the instructions of C1_D, C2_D, and C4_D. Part of the funds was routed through other Belgian or Portuguese buffer entities to companies or individuals linked to the original cash suppliers. These transfers completed the compensation cycle, as the actors who handed over cash received equivalent amounts in their bank accounts, after deduction of the laundering commission.

Throughout these steps, the network applied a **commission structure** that turned the scheme into a business model. Clients seeking to dispose of criminal cash paid a fee of approximately 7% on amounts converted into bank funds, while user firms receiving cash to pay undeclared labour paid 2% on the corresponding compensation transfers. Brazilian *filière* companies retained an additional margin on the flows passing through their accounts. The remaining profits were channelled through Belgian and foreign buffer entities to accounts controlled by core members of the network, reinvested abroad, or recycled into new compensation transactions.

Post-activity or post conditions

Over time, several **red flags** emerged suggesting the criminal use of the businesses involved. For instance, GP1_D and LTD1_D held mandates over numerous suspect companies, whose ownership and management structures revealed close family ties to C1_D, reliance on trusted employees, and the use of strawmen who formally acted on behalf companies without exercising actual control. Moreover, several entities in the scheme displayed transaction profiles typical of Brazilian *filière* users and buffers. LTD2_D was a central example: over approximately three months, it processed around two hundred transactions with a total volume exceeding EUR 830,000, mainly from Belgian construction and

cleaning firms identified in FIU records as **Brazilian *filière* companies**. LTD2_D had no staff, no business infrastructure, and no evidence of genuine commercial activity, yet large sums were credited and debited at high speed. LTD3_D and LTD4_D showed similar patterns. Over eight months, more than EUR 5 million flowed through LTD3_D's accounts, with outgoing payments directed to a wide range of Belgian and foreign recipients. LTD4_D received more than EUR 2.8 million, largely from companies operating in fraud-sensitive sectors. Within the FIU analyses, GP2_D was identified as a user of the system. Its account profile suggested a combination of genuine activity and systematic participation in a compensation scheme. On the outgoing side, GP2_D made transfers to companies previously reported and that appeared to have no genuine economic activity, indicating payments for fictitious invoices in exchange for cash. More generally, entities in this laundering network tended to have short lifespans, frequent changes in name, registered office, and management, and processed high volumes over limited time periods, often accompanied by generic invoice descriptions.

Ultimately, the **judicial investigation** into the criminal use of these businesses concerned activity occurring between January 2020 and January 2023, following multiple referrals by the Belgian FIU to the Brussels Public Prosecutor's Office. During this period, the network effectively achieved its primary objective of providing professional money laundering services and generating profits through commissions. Financial reconstruction estimates total illicit assets at approximately EUR 3.4 million.[68]

4. Financial profile of the criminal network involved in Case Delta

Financing sources and start-up capital

The judicial files indicated that the network's capital comprised a mixture of **legitimate funds** and illicit proceeds. GP1_D and LTD1_D, as well as several other companies involved in the scheme, carried out at least part of their activities in the legitimate economy. They provided genuine accounting and administrative services, thereby generating lawful income that could be used to cover basic operating costs and maintain a credible business profile. At the same time, the incorporation activity of GP1_D and LTD1_D generated a significant source of liquid funds: clients paid incorporation fees in cash, typically between EUR 3,500 and EUR 4,000 per company. Around half of these amounts were not recorded in the official accounts. On the other hand, large volumes of **illicit cash** were supplied by external clients engaged in a range of criminal activities, as the network operated as a service provider laundering polycriminal proceeds. The judicial files explicitly referred to illegal cash derived from drug trafficking and the exploitation of Brazilian prostitutes.

Payment methods and arrangements within the network

As for payment methods within the network, both physical cash handling and high-volume bank transfers were used. Substantial sums of cash were transported by couriers, with handovers taking place in large car parks or shops and hotels. The police intercepted twelve transfers, ranging from EUR 7,000 to EUR 140,000. It is estimated that, between January 2020 and January 2023, at least EUR 2.9 million was physically transported and subsequently integrated into the legal economy through fictitious invoices and bank transfers. Within this combination of cash payments and bank transfers,

[68] However, even after police searches at several suspect addresses in 2023 and the detention of several key members, the compensation scheme continued for some time through the network around C2_D and C4_D. The files indicated that it remained operational until C2_D and C4_D, who had fled to Brazil and were subject to an international arrest warrant, were also arrested later in 2023.

the network applied a commission-based payment scheme, which was the primary revenue of the service-based money laundering process (cf. *supra*).

Costs of business operations

Although the network's operating costs were not explicitly described in the judicial files, some elements could be derived indirectly. For example, maintaining GP1_D and LTD1_D as professional accounting firms likely entailed expenses typical of companies operating in the services sector, including rent, utilities, advertising, basic staff salaries, accounting software, communication tools, and fees for notarial acts and registrations. The creation and maintenance of shell and buffer companies would have involved comparable **incorporation and administrative costs**. Moreover, the cash logistics of the compensation scheme entailed operational costs. To carry out transports, cash couriers needed vehicles, fuel, and communication equipment.

Revenues and proceeds

Financial reconstruction in the judicial file estimated the unlawful assets of the initial network at a minimum of **EUR 3.4 million** for the period January 2020 to January 2023. This figure was based on two components included in the calculation of illicit proceeds. On the one hand, approximately EUR 560,000 in inflows to the personal bank accounts of core network members was recorded from nine Brazilian *filière* companies. On the other hand, at least EUR 2,924,000 in documented clandestine cash transports, delivered by couriers to Brazilian *filière* firms and other invoice sellers, was also identified. However, inflows into the company accounts of entities controlled by the network were not fully included in this estimate. The figure of EUR 3.4 million should thus be interpreted as a lower bound, as the total amount laundered through the service-based money laundering scheme is likely higher.

Within this turnover, the network's actual earnings derived from **commissions** charged on transactions. C2_D and C4_D charged a commission of 7% to clients seeking to dispose of criminal cash, and 2% to companies receiving cash to pay undeclared labour. Based on the documented amounts, this yields an estimated commission income of approximately EUR 207,300 for the period examined. The judicial file indicated that C2_D received 80% of this commission, while C4_D received 20%.

5. Harms caused by Case Delta

Harms to individuals

The compensation scheme primarily harmed employees of the construction and cleaning firms, who were paid in cash and off the books. Without formal contracts, social security coverage, or pension contributions, they had limited protection in cases of illness, workplace accidents, unemployment, or retirement. At the same time, undeclared work may have offered perceived short-term advantages, such as higher net income or the ability to retain benefits or tax credits. For some workers, particularly those facing barriers to legal employment due to their residence status, it may have provided an entry point into the labour market. However, this also left them in a vulnerable and dependent position.

The cash entering the compensation scheme originated from organised crime activities, including prostitution and drug trafficking. The scheme therefore indirectly facilitated the continuation of harm associated with these activities such as the sexual exploitation of Brazilian prostitutes. Finally, widespread undeclared work in construction and cleaning may have undermined the quality and safety of services. This may have resulted in unsafe buildings, poor maintenance, and increased accident risks for workers and end users.

Harms to other businesses

The use of construction and cleaning companies as end users in the compensation scheme created unfair competition for law-abiding firms. By avoiding full social security contributions and wage-related taxes, companies participating in the scheme artificially reduced their labour costs. This allowed them to offer lower prices or maintain higher profit margins than compliant competitors. In tender procedures and subcontracting chains, such underpricing may disadvantage compliant firms or incentivise them to adopt grey practices to remain competitive. Brazilian *filière* companies were also used as disposable links in chains of bank transfers. Contracts and invoices that appeared to document ordinary subcontracting or cleaning services were instead used to channel criminal funds into the legitimate economy. This may have undermined trust in *bona fide* businesses and normal commercial relationships.

Harms to public institutions

The most direct harm to public institutions arose from fiscal and social fraud. Companies embedded in the compensation scheme failed to meet their obligations regarding income tax, corporate tax, and social security contributions. At the same time, some individuals involved in the network received social support, such as social assistance, unemployment benefits, or social housing. Public authorities therefore lost expected revenues while continuing to pay welfare benefits.

Harms to the physical environment

The judicial file did not document any direct harm to the physical environment. Nor did it provide any specific indication that construction or cleaning companies within the network were used for the disposal of hazardous waste or to circumvent environmental permit requirements.

Harms to the social environment

The normalisation of undeclared work can foster perceptions of unfairness among workers and residents who comply with the rules and undermine the solidarity required to sustain collective social security arrangements. The focus on Brazilian *filière* cases also carries a risk of stigmatisation. Public debate and media reporting often associate Portuguese and Brazilian communities in Belgium with such compensation schemes, although many professional networks use these types of construction arrangements. The label 'Brazilian *filière'* may therefore reinforce ethnic stereotyping of the wider community.

Annex 2.E – Case Echo: Façades and False Invoices

1. Criminal network involved in Case Echo

The criminal network in Case Echo comprised at least sixteen members of various nationalities and a broad network of legal entities. Although the judicial file did not specify a clear hierarchy or formal role allocation, several functional roles could be inferred from the case description. Table 9 provides an overview of the core members of this network.

Table 9

Overview of the core members of the criminal network involved in Case Echo (Brussels)

Member	Role	Gender	Born between	Nationality
C1_E	Organiser of the compensation scheme	Male	1974-1993	Spanish
C2_E	Strawman	Male	1994-2007	Portuguese
C3_E	Strawman	Male	1974-1993	Belgian
C4_E	Strawman	Male	1954-1973	Spanish
C5_E	Strawman	Male	1994-2007	Italian
C6_E	Strawman	Male	1974-1993	Tunisian
C7_E	Criminal accountant	Male	1954-1973	Pakistani
C8_E	Accountant; Facilitator	-	-	-

C1_E appeared as the **central actor**, as he was identified as the *de facto* manager of LTD1_E and LTD3_E and the legal director of LTD2_E. This linked him directly to three front companies that formed the core of the compensation scheme, of which C1_E was considered the organiser and coordinator. Five individuals (C2_E, C3_E, C4_E, C5_E, C6_E) were identified as **strawmen** whose identities were misused by the criminal network. However, the degree of awareness and voluntariness differed among the actors involved. Two of them were acquitted by the court, whereas the judicial files indicated that one accountant knowingly assisted in the transfer of company shares and the establishment and/or maintenance of corporate structures used by the network. Another member acted as a 'criminal accountant' linked to LTD10_E, using an Excel workbook to track transactions for dozens of companies.

2. Legitimate businesses involved in Case Echo

The judicial investigation focused on eleven companies, all of which were incorporated as **private limited companies** (see Table 10). Seven of these businesses listed construction as their primary registered economic activity. The companies involved in the network's cash compensation scheme can be grouped into three categories, reflecting their distinct functional roles within the scheme.

First, the judicial files identified three Brussels-based **façade companies** (LTD1_E, LTD2_E, LTD3_E) that engaged in no genuine economic activity and were registered at vacant or fictitious addresses. They had no staff, operating costs, infrastructure, or reliable bookkeeping.

- **LTD1_E** was established in 1985 and came under the network's control in 2019 when C2_E was appointed manager, acting as a strawman for C1_E. Although construction was listed as the company's primary economic activity, various additional activities were also registered in the Crossroads Bank for Enterprises, including cleaning and transportation. Ultimately, the company was dissolved, and bankruptcy proceedings were closed in 2025.
- **LTD2_E** was established in 2018 by C1_E, with construction and cleaning, respectively, listed as its primary economic activities. The business was dissolved and, in 2023, bankruptcy proceedings were closed. In the judicial files, however, **LTD3_E** was identified as a 'replacement company' for LTD2_E. It was established in 2022 and managed by a strawman.

Table 10
Overview of the businesses involved in Case Echo (Brussels)

Company	Economic sector	Status in 2025	Location
LTD1_E	Construction	Inactive – Bankruptcy closed in 2025	Brussels, Belgium
LTD2_E	Construction	Inactive – Bankruptcy closed in 2023	Brussels, Belgium
LTD3_E	Construction	Inactive – Bankruptcy closed in 2022	Brussels, Belgium
LTD4_E	Advertising	Active – Bankruptcy opened in 2020	Brussels, Belgium
LTD5_E	Construction	Active – Bankruptcy opened in 2020	Wallonia, Belgium
LTD6_E	Packaging	Active	Wallonia, Belgium
LTD7_E	Construction	Active	Brussels, Belgium
LTD8_E	Construction	Active	Brussels, Belgium
LTD9_E	Construction	Active	Flanders, Belgium
LTD10_E	Wholesale and retail of electronics	Inactive – Bankruptcy closed in 2021	Flanders, Belgium
LTD11_E	Hospitality	Inactive – Bankruptcy closed in 2019	Wallonia, Belgium

Second, most businesses identified in Case Echo appeared to function as labour-intensive **client companies**, characterised by a recurring demand for cash to pay workers partly off the books. LTD4_E to LTD9_E were classified in this category, paying employees in cash and paying fictitious invoices to LTD1_E, LTD2_E, and LTD3_E. Four of these companies operated, at least partially, in the construction sector, while others were active in the advertising (LTD4_E) and packaging (LTD6_E) industries.

Third, the judicial file classified two businesses as **cash suppliers** within the compensation scheme. LTD10_E was established in 2019 and managed by a strawman, with wholesale and retail in electronics as its primary economic activity. The business was dissolved, and bankruptcy proceedings were closed in 2021. LTD11_E was established in 2017 and operated in the hospitality sector until bankruptcy proceedings closed in 2019.

3. Crime script based on Case Echo

Motivation – Purpose

Within Case Echo, the criminal use of legitimate businesses was primarily motivated by the purpose of money laundering and generating profit through a **cash compensation scheme**. Client companies participated primarily to facilitate tax and social fraud, whereas façade companies and cash suppliers used the scheme to launder criminal proceeds by converting cash into funds in the banking system.

Preparation

Case Echo involved the criminal use of companies operating in labour-intensive service sectors, particularly the **construction** industry. As a subcontractor, entry into the sector was relatively easy due to persistent demand for labour. The sector is also characterised by subcontracting chains with limited oversight and controls. This lack of transparency may explain its frequent association with the shadow economy and exposure to organised crime.

Pre-activity or enabling conditions

In this case, the pre-activity phase can be divided in two parts: first, the acquisition of control over relevant companies; and second, the configuration of the cash compensation mechanism prior to routine operations.

The **three façade companies** (LTD1_E, LTD2_E, LTD3_E) were established and/or repurposed to facilitate fraud and money laundering, without any intention of providing genuine services. C1_E acted as the *de facto* manager of two companies and the judicially registered director of the third. He reportedly acquired or established these entities and recruited strawmen to serve as official managers. While some of them appear to have collaborated knowingly, others seem to have been unaware of their role, for example by signing documents in exchange for small payments and subsequently leaving Belgium. The judicial file also described the involvement of an accountant who knowingly arranged share transfers, thereby enabling the network to acquire control of LTD1_E and LTD2_E. In addition, C1_E actively targeted companies in need of cash. Recruitment reportedly took place in informal settings, such as bars, and relied predominantly on verbal agreements. According to the judicial file, the managers of the client companies knowingly and voluntarily involved their legitimate businesses in the scheme.

The illicit funds underlying the cash compensation scheme were generated through **intra-Community VAT fraud**. Telecommunications companies LTD10_E and LTD11_E served as key nodes in the cash generation process and were described as criminally controlled entities. In this context, both companies first acquired telecommunications products through intra-Community transactions. Supplies between EU Member States can be invoiced at a zero percent VAT rate, as the tax is generally accounted for in the Member State of destination. The companies then created a paper trail indicating onward intra-Community resales to clients in France, also invoiced at zero percent, implying that the goods left Belgium. However, the economic reality diverged from this documentation: the goods allegedly remained in Belgium and were sold on the domestic black market, without invoices or VAT. The proceeds were collected in cash and channelled to other companies within the network. This structure enabled the compensation scheme to operate on a routine basis.

Activity

Routine operations depended on the continuous production of a **credible paper trail** to justify regular bank transfers between companies. In practice, LTD10_E and LTD11_E generated cash, while the three front companies (LTD1_E, LTD2_E, LTD3_E) served as distribution and laundering hubs. These firms issued fictitious invoices paid by client companies via bank transfers. After receipt, these payments were tracked and matched to the cash requirements communicated by the client companies. The cash return was calculated after deducting a commission of 3% as reported in the file and was delivered in cash. The redistributed cash was then used to pay workers off the books, indicating social and tax fraud.

Post-activity or post conditions

The judicial files covered the period from 2018 to 2021. During that period, the network successfully laundered money and generated financial profit. Over time, several **red flags** emerged suggesting the criminal use of legitimate business structures, including repeated invoicing for vague and difficult-to-monitor services and rounded invoice amounts. These features suggested fabricated billing rather than market-based pricing. The façade companies further displayed structural characteristics typical of non-genuine businesses: they had no staff, plausible breakdown of operating costs, operational infrastructure, or reliable bookkeeping. Ultimately, the **investigation** was initiated following a referral by the Belgian FIU in 2019, flagging bank transfers involving LTD1_E and LTD2_E. The investigation resulted in seizures totalling approximately EUR 19.6 million.

4. Financial profile of the criminal network involved in Case Echo

Financing sources and start-up capital

The judicial file did not specify which predicate offences generated the network's start-up capital, in particular the funds used to initially purchase telecommunications products. It only noted that C1_E had 'various sources of illegal income'.

Payment methods and arrangements within the network

Payments within the network were primarily executed by **bank transfers** based on invoices between companies, after which cash was distributed to labour-intensive client companies to cover wages paid off the books. Moreover, payment agreements were reportedly made informally and verbally, for instance during meetings in cafés. Client companies paid the invoices via bank transfer and subsequently received cash back through the network. According to the judicial files, the cash-generating intermediary retained a commission of 3%. In addition, the files referred to bookkeeping practices carried out by a 'criminal accountant' who maintained an Excel workbook with separate tabs, each containing a list of bank transactions including recorded cash withdrawals and deducted costs. The workbook identified 58 Belgian companies, operating primarily in the construction and cleaning sectors. The recorded transfers took place in 2020-2021, amounting to over EUR 12.3 million.

Costs of business operations

The network's primary operating costs included the purchase of telecommunications products through intra-Community acquisition channels, as well as the practical costs associated with cash logistics and the maintenance of corporate vehicles. Additional cost items plausible comprised remunerations paid to intermediaries and strawmen and fees for professional services, such as accounting, administration, and banking, including the opening and maintenance of accounts. Finally, the handling, transport, and delivery of cash also resulted in operational costs.

Revenues and proceeds

The scheme outlined above facilitated the laundering and integration of funds into the financial system across the network. Client companies benefited from fiscal and social security savings, resulting from reduced effective labour costs and the improper booking of fictitious expenses. The network's cash-generating businesses, on the other hand, profited from the alleged black-market sale of goods and the resulting liquidity.

5. Harms caused by Case Echo

Harms to individuals

The potential harm to individuals primarily stems from undeclared work. This limits access to social protection may increase vulnerability to exploitation. It also creates uncertainty regarding pay, entitlements, and working conditions.

Harms to other businesses

The compensation scheme distorts competition by enabling companies to reduce labour and compliance costs through fiscal and social fraud, thereby placing *bona fide* competitors at a disadvantage.

Harms to public institutions

The state incurs fiscal losses through foregone VAT, social security contributions, and corporate tax revenues.

Harms to the social environment

At a societal level, such compensation schemes can erode trust in economic transactions, fair labour conditions, and competitive practices. They may also contribute to the normalisation of undeclared wages as an 'acceptable' practice in certain sectors.

Annex 2.F – Case Foxtrot: Games of Chance and Channels of Cash

1. Criminal network involved in Case Foxtrot

As no judicial files were available, no detailed description of the network, including its members and roles, can be provided for Case Foxtrot. However, the interviewee [R8_BE] offered a general overview of the criminal milieu, indicating that a small number of criminal actors currently control many bars with gambling machines:

> "*And that leaves four or five major players who, in fact, control a very large part of the hospitality industry in Brussels. (…) Every time you see a bingo machine, you know the lease will be in the name of the gambling operator. And that's the case, every single time. You can confirm that. So we have four or five companies where you know every time: okay, lease, lease, lease. So there really is a system in place.*"[69] [R8_BE]

[69] Original quotation in Dutch: "En dat geeft een stuk of vier, vijf grote spelers die een heel groot stuk van de horeca in Brussel onder hun hoede hebben, eigenlijk (…). Elke keer als je die bingokast ziet staan, dat je weet: oké, dat huurcontract zal op naam staan van de kansspelplaatser. En dat is elke keer opnieuw, dat je dat kunt bevestigen. Dus we hebben vier, vijf maatschappijen waarbij je elke keer weet: oké, huurcontract, huurcontract, huurcontract. Dus er zit echt wel een systeem in."

2. Legitimate businesses involved in Case Foxtrot

The legitimate businesses involved in this case are **bars** located in Brussels where legal **games of chance**, including bingo machines and slot-style gaming devices permitted in cafés, are offered alongside beverage sales. These businesses are generally regarded as combining legitimate activities (i.e., serving drinks) with fiscal and social fraud, as well as money laundering. The interview with the Brussels FJP official did not yield any concrete information about specific bars or their legal forms. Nevertheless, a recurrent pattern could be identified: usually, gambling machines are installed by criminally owned companies that supply and operate them, while the bars themselves are often managed by individuals acting as strawmen.

3. Crime script based on Case Foxtrot

Motivation – Purpose

The primary motivation described, is the pursuit of financial gain through the **laundering** of illicit proceeds via gambling revenues generated in bars. Based on the interview, however, the origin of the laundered illicit funds could not be determined. In addition to money laundering, the bars are often also used to commit fiscal and social **fraud**, particularly by using undeclared labour in the bar.

Preparation

A key enabling condition for this phenomenon is the deliberate exploitation of a **legislative gap** governing the relationship between gambling-machine operators and the premises in which the machines operate. Article 27 of the Belgian Gambling Act prohibits the gambling-machine placer from being the owner of the establishment where the devices are installed.[70] In practice, however, criminal networks circumvent this ownership restriction by entering into rental agreements themselves: rather than acquiring the premises as owners, they position themselves as tenants, thereby remaining formally outside ownership-based prohibitions while securing effective control over the location. The rented bar is then sublet to strawmen holding a licence for café gambling.

The interviewee described a typical Brussels café as hosting two bingo machines and two slot-style devices, operated under the standard licensing regime and requiring no additional 'special' permits beyond this baseline authorisation (Kansspelcommissie, n.d.-b). The ease of installation, combined with the high concentration of hospitality venues in Brussels and the high turnover in the sector, makes bars a particularly **attractive target** for criminal actors looking for opportunities to launder money. Furthermore, oversight and control by the Belgian Gambling Commission are often considered inadequate (Hendrickx, 2024).

Pre-activity or enabling conditions

In connection with this phenomenon, members of a criminal network seek out bars that are available for rent. Once they have secured an establishment through a rental contract, they sublet the bar and appoint a strawman to manage day-to-day activities. The sublease arrangements reportedly include provisions aimed at **maximising turnover** from gambling, such as the requirement that the bar remains open 24 hours a day and seven days a week, ensuring that the machines can be played at any time.

[70] Art. 27 of the Law of 7 May 1999 on games of chance, betting, gaming establishments and the protection of players, *Belgian Official Journal,* 30 December 1999.

Although the degree of awareness and voluntariness among the strawmen can vary, the interviewee identified recurring profiles of economically precarious groups, including recently arrived migrants in Brussels seeking employment. For example, Ukrainian and Romanian women are informally approached and offered a monthly payment or a share of the turnover in exchange for formally managing the bar. In this arrangement, the strawmen are presented as 'clean', in the sense that they do not necessarily engage in overtly illegal activities themselves and may not be fully aware that they are being used within a broader criminal structure.

Activity

Within regard to this criminal phenomenon, the bars usually combine lawful hospitality services with the intensive criminal use of games of chance. The criminal value of this arrangement lies in the fact that the gambling activity is, on paper, legal and embedded in an ordinary café setting, while the surrounding structure enables the systematic use of these businesses for money laundering and fraud. Within this structure, members of the criminal network **generate income** through two principal mechanisms. First, the gambling proceeds are divided: roughly half of the revenues go to the machine operator (i.e., a member of the network) and the other half to the café manager, who acts as a strawman. Second, because the machine operator is also the tenant of the premises and charges substantial rent when subleasing the bar, part of the café manager's share is effectively channelled back to the machine operator through rental payments.

The money laundering method is embedded in the first revenue stream mentioned. Members of the criminal network approach individuals, provide them with cash, and instruct them to insert that money into gambling machines and play on their behalf. Through this method, **illicit funds** of unknown origin **enter a legal gambling circuit** that operates within a licensed and publicly accessible business. The illicit cash is converted into recorded revenue from slot machines and, where applicable, into payouts derived from games of chance. When proxy players win, they are reportedly allowed to keep the winnings, serving as a form of payment. This practice is facilitated by circumventing measures related to player identification. Although gambling is, in principle, supposed to require identification, many bars reportedly keep a blank 'white card' in their machines. Originally, this was justified as an exceptional tool to accommodate foreign players but is in practice used to allow anonymous play. In addition, these businesses are frequently associated with fiscal and social fraud, particularly through the undeclared employment of bar staff.

Post-activity or post conditions

As mentioned above, an enabling condition for this phenomenon is legislative gap governing the relationship between gambling-machine operators and the premises in which the machines operate. Although the Gambling Act restricts ownerships links between gambling-machine operators and the premises where the devices are operated, it does not prohibit operators from renting such premises. The interviewee [R8_BE] noted that this poses challenges in terms of enforcement. In response, the FJP and the Brussels Public Prosecutor's Office reportedly pursue a **pragmatic strategy** in which cases involving this approach are consolidated at the Public Prosecutor's Office to build jurisprudence. The purpose is to obtain case law in which such rental agreements are recognised as equivalent to ownership for enforcement purposes. Given the absence of judicial files for Case Foxtrot, no judicial outcomes, sanctions, or asset recovery measures can be documented.

Despite these limitations, the interviewee identified several **indicators** associated by law enforcement with this *modus operandi*. One key indicator is a pronounced discrepancy between turnover from beverage sales and gambling revenues, with drink sales remaining extremely low while gambling income is disproportionately high. A second indicator is the repeated involvement of the same tenants across multiple bars.

4. Financial profile of the criminal network involved in Case Foxtrot

Financing sources and start-up capital

The origin of the start-up capital underlying this money laundering method is unknown.

Payment methods and arrangements within the network

Almost nothing is known about the payment methods and internal arrangements of the criminal network(s) in this case. However, the interview suggested the existence of cash-based arrangements in which money is physically handed over to proxy players, who subsequently insert it into the machines. The proxy players are reportedly permitted to retain any winnings, which serves both as an incentive and as compensation for their participation.

Costs of business operations

Operational costs likely include the incentives embedded in arrangements with proxy players, since these individuals are reportedly allowed to retain any winnings (cf. *supra*). In addition, gambling proceeds are shared with the café manager, with approximately half of that amount accrued to the manager. Other cost items are not specified, although operating the bar also entails ordinary business expenses.

Revenues and proceeds

According to the interviewee, a single gambling machine generates approximately EUR 100,000 to EUR 150,000 per month.

5. Harms caused by Case Foxtrot

Harms to individuals

At the individual level, gambling entails well-documented risks, including addiction and financial distress. The interviewee also suggested heightened vulnerability among people in precarious situations who are recruited as proxy players, as well as among individuals working undeclared in these bars. Moreover, strawmen who formally manage the bars may ultimately bear responsibility for the criminal use of gambling machines operated through the businesses they represent. Finally, open sources point to intimidation and threats linked to the licensing process, including threats against municipal council members when negative advice is issued regarding new permits (Hendrickx, 2024).

Harms to other businesses

Illicitly supported venues can distort competition and normalise criminal influence within the local hospitality sector. At the same time, legitimate gambling machines can provide an important source of income for small cafés, contributing to rent and staff costs. Therefore, the mere presence of such machines does not in itself indicate criminal use for money laundering.

ANNEX 3

CASERTA

DETAILED CASE STUDIES

Annex 3.G – Case Golf: The Prince and the Ballot Scheme

1. Criminal network involved in Case Golf

The criminal network involved in Case Golf was linked to the Casalesi clan, one of the most structured and complex Camorra organisations. The operation was primarily coordinated by the Schiavone and Russo factions, with the involvement of the Bidognetti family. In this case, the network rested on a stable nexus of politics, business, and crime, with **institutional actors** serving as strategic nodes. Professionals such as lawyers, accountants, and financial experts played a key role in legitimising illicit activities, particularly in money laundering and public procurement. Alongside political actors operated colluding entrepreneurs and intermediaries who managed businesses and financial flows. This allowed the network to function without violence, relying instead on established relationships and mechanisms of exchange.

A total of 75 individuals were identified in connection with this case. In addition to the core members listed in Table 11, two distinct groups of **individuals linked to Case Golf** could be identified. The first group was involved in the manipulation of the electoral process, including public officials performing functions such as fraud, corruption, and document falsification, as well as beneficiaries who profited from electoral manipulation, for instance through payments in exchange for votes. The second group was linked to the construction project of the 'Il Principe' shopping project, comprising both beneficiaries of the project and facilitators, such as those producing false technical reports, influencing financial arrangements, or securing political support for its implementation.

Table 11
Overview of the core members of the criminal network involved in Case Golf (Caserta)

Member	Role	Gender	Born between
C1_G	Entrepreneur; External aiding and abetting	Male	1934-1953
C2_G	Operational support; Political contact	Male	1954-1973
C3_G	Political facilitator providing political and administrative support; External aiding and abetting	Male	1954-1973
C4_G	Entrepreneur; External aiding and abetting	Male	1954-1973
C5_G	Management of illegal activities	Male	1974-1993
C6_G	Local politician; Electoral vote broker	Male	1974-1993
C7_G	Clan representative; Electoral vote intermediary for the clan	Male	1954-1973
C8_G	Manager; Coordinator of illegal electoral activities	Male	1954-1973
C9_G	Material perpetrator; Misappropriation of school meal vouchers	Female	1954-1973
C10_G	Clan representative; Electoral intermediary; Vote broker and distributor of electoral payments	Male	1974-1993
C11_G	Public official; Falsification of official documents; Illicit issuance of building permits	Male	1954-1973
C12_G	Clan leader; Director and coordinator of the economic-entrepreneurial operation involving illicit capital	Male	1974-1993
C13_G	Leader; Beneficial owner of assets and economic activities	Male	1954-1973

Several key features define the operation of this network. A central element was the '**common fund**', managed by its historical leaders and financed through illicit and legal-economy revenues. It functioned as an internal welfare mechanism: it sustained members of the network, supported families of detained affiliates, and ensured organisational cohesion. Previously, the fund was financed primarily through illicit activities, including money laundering, but it has increasingly shifted towards the direct capture of public resources to consolidate economic and political power. Moreover, the network's strength lies in its **resilience**, persisting despite arrests and repression through relatives, strawmen, and evolving

entrepreneurial configurations. Over time, its structure has become more horizontal and territorially diffuse, intertwined with professionals and public officials. Finally, a key feature is its capacity to blend into the economic and social fabric, since the clan's activities often resemble ordinary businesses that generate employment and income.

2. Legitimate businesses involved in Case Golf

An analysis of the judicial files related to Case Golf revealed the involvement of **three legally registered companies** operating in the Province of Caserta, which were directly linked to members of the criminal network. The scheme relied on several entities formally operating in the social services sector, namely one private limited liability company (LTD1_G) and two social cooperatives (LTD2_G, LTD3_G). Table 12 provides an overview of these companies.

Table 12
Overview of the businesses involved in Case Golf (Caserta)

Company	Economic sector	Status in 2025	Location
LTD1_G	Social services; Management of municipal services (e.g., school meals, cleaning of public buildings)	Formally active	Casal di Principe, Italy
LTD2_G	Social services	Liquidated – Removed from the Business Register in 2024	Campania Region, Italy
LTD3_G	Social services	Formally active – Liquidation proceedings initiated in 2010	Campania Region, Italy

From an external perspective, these companies **appeared fully legitimate**, with proper registration, contracts, and financial reporting. The irregularities lay not in their formal structure, but in the underlying power relations governing hiring decisions and exchanges of favours linked to employment. Rather than pre-existing businesses, they were often created *ad hoc* by the criminal network, typically as social cooperatives established to manage specific activities.

- **LTD1_G**, a Naples-based private limited liability company, formally provided outsources social services to the municipality of Casal di Principe, as it held municipal contracts for school catering and cleaning services for public buildings. However, its formal management as an ordinary service provider was a façade concealing criminal control. The company was effectively controlled by a **municipal councillor** (MC_G) who acted as its *de facto* administrator. In this role, he exercised direct authority over hiring decisions, dismissals, and wage distribution. Dozens of female workers were employed, with wages managed directly by the councillor through an intermediary formally employed by the contracting company holding municipal contracts. This arrangement enabled MC_G to retain direct influence over workers and to use employment as a tool of political leverage.

- **LTD2_G** and **LTD3_G**, two social cooperatives operating in social assistance, managed care services and family homes for vulnerable groups, including persons with disabilities, minors, and socially disadvantaged individuals. These services were awarded through regional and municipal public procurement procedures. Both cooperatives were controlled by a senior figure in the Casalesi clan, who acted as the economic intermediary between the criminal leadership and the cooperative sector. He ensured that public contracts and employment opportunities generated by the cooperatives were allocated in line with the clan's political and strategic interests. In practice, the cooperatives functioned as reservoirs of employment that

could be promised to potential voters before elections and distributed afterwards as rewards for electoral support.

In addition to these legitimate businesses, the publicly funded **LSU programme** (*Lavoratori Socialmente Utili*) was also part of the scheme. Designed as a state-subsidised programme administered by the municipality, it aimed to support unemployed individuals through temporary work in municipal services such as maintenance, cleaning, and assistance activities. Although not a private company, the LSU scheme played a key role in the network's strategy by creating a pool of precarious workers whose contract renewals depended on municipal decisions. This dependency made LSU workers vulnerable to political pressure. The judicial investigation indicated that MC_G organised meetings with groups of LSU workers and used the prospect of contract renewal to influence their electoral behaviour.

Through the combined control of these companies and employment programmes, the network was able to transform legitimate social services into **instruments of electoral patronage**. Economically vulnerable individuals, particularly women in cleaning and catering services and workers participating in LSU programmes, were offered jobs or promises of future employment in exchange for electoral votes for candidates supported by the network. In some cases, voters were accompanied to polling stations to ensure compliance. Public resources, including school meal vouchers, were also diverted for vote-buying, alongside promises of employment in public institutions such as the local health authority.

3. Crime script based on Case Golf

Motivation – Purpose

Within Case Golf, the criminal use of legitimate businesses was primarily driven by **electoral corruption** and political control. The aim was to secure the election of candidates affiliated with or connected to the clan in municipal and provincial offices, including through fraudulent methods such as the so-called 'ballot scheme' (cf. *infra*), thereby ensuring continued access to public resources and administrative power, and maintaining territorial control. Alongside this political objective, a complementary economic dimension was central: legal businesses were used for money laundering, particularly through payroll systems and formal employment, and for extracting value from public contracts. At the same time, employment and welfare services were used as instruments of coercion and **social control**, creating dependency relations between economically vulnerable citizens and political-criminal power. In contexts of high unemployment, the promise or loss of employment proved sufficient to shape electoral behaviour without the need for explicit violence.

Preparation

The companies involved (LTD1_G, LTD2_G, LTD3_G) displayed characteristics that rendered them vulnerable to criminal exploitation through the opportunities afforded by their legitimate commercial activities. First, these companies operated through **public contracts**, meaning that market access depended on administrative decisions rather than purely competitive dynamics. This enabled the criminal network to influence the allocation of contracts once political control had been secured. Second, they exercised significant discretionary power over hiring and employment contracts, which was exploited as a key mechanism in political-electoral exchange by transforming employment into a negotiable resource. Furthermore, the **management of wages and employment** relationships, including irregular arrangements, enabled direct control over workers and reinforced dependency. Finally, the formal structure of these companies, often shielded by frontmen or opaque corporate

arrangements, concealed the real decision-making centre and thereby facilitated infiltration without raising apparent anomalies.

Alongside these company-specific factors, the **social services sector** in Campania, particularly in the Province of Caserta, offered opportunities for criminal infiltration.[71] First, the sector is heavily dependent on public funding (municipal, regional, and often European), with resources allocated through tenders, public procurement, and administrative concessions. Consequently, the sector has emerged as an area of strategic interest for criminal actors, since control over administrative decision-making enables the manipulation of procurement processes. Second, its workforce consists mainly of women working in precarious employment, with relatively low levels of formal education and limited alternative job prospects, making them vulnerable to exploitation and coercion. Third, oversight of managing entities, particularly social cooperatives, has historically been weak. Until relatively recently, prefectures and contracting authorities did not conduct thorough anti-mafia checks on cooperative members. This regulatory gap has been systematically exploited.

The combination of these factors creates a high-risk environment: the social services sector is funded by public resources yet remains highly susceptible to control through political and institutional connections linked to criminal networks. In Campania, criminal groups use social services not only for profit but also for **territorial control**, political mediation, patronage, and access to public resources. This is evidenced by numerous anti-mafia interdictions issued by the Prefect of Caserta against companies and cooperatives active in the social assistance sector, as well as by the dissolution of several municipalities in the province due to mafia infiltration.[72]

Pre-activity or enabling conditions

The preparatory phase of infiltration was based on the gradual construction of a **system of control** that preceded and enabled illicit activity. The Casalesi network became progressively entrenched in local institutions and the economic fabric, primarily through access to strategic political positions (e.g., mayor, councillor), which allowed direct influence over administrative decisions. In parallel, it built a network of colluding entrepreneurs, intermediaries, and workers, thereby creating a dependent electoral base (cf. *infra*). In this way, the clan was able to ensure control over public resources and employment opportunities even before electoral exchange was activated.

In this context, the companies involved (LTD1_G, LTD2_G, LTD3_G) did not function as autonomous entities later infiltrated but became operational extensions of the clan's political power. While their legitimate activities (e.g., catering, cleaning, social services) provided a formal cover, their primary function lay in managing **electoral consensus** and **territorial control**. Consequently, the majority of cases indicated a high degree of culpability. LTD1_G appeared to have been fully subject to the *de facto* control of a political figure linked to the clan (MC_G), who exercised direct control over hiring, dismissals, and payments, despite not formally appearing in the corporate structure. The company thus functioned as a conscious instrument, or at least as a fully functional component to the criminal system.

[71] Recent figures indicate that the private sector category 'education, health, and private social assistance' in Campania comprises 9,385 firms and more than 95,000 workers (5.8% of the regional workforce), underscoring that social services are not marginal but a significant, labour-intensive component of the regional economy (INPS, 2024).

[72] In the Italian legal system, the dissolution of a municipal council is an administrative measure by the central government, adopted where there is evidence of organised crime influencing local authorities. It involves replacing elected bodies with appointed commissioners for a fixed period to restore legality and prevent further infiltration.

The responsibility of LTD2_G and LTD3_G was even more evident, as they were created or controlled by colluding individuals and lacked genuine autonomy. By contrast, the workers were largely victims of economic coercion rather than active participants in the criminal dynamic.

Activity

As noted above, the business management of the companies involved (LTD1_G, LTD2_G, LTD3_G) was effectively exercised by individuals within the criminal network, often holding public office, who used their institutional positions to influence both the allocation of contracts and internal operations of the companies. A central element of their business management was direct **control over human resources**. Hiring, dismissals, and contract renewals were guided by an electoral logic. Personnel were selected based on their usefulness within the clientelist system and kept in a condition of dependency through precarious contracts and personalised wage management. Financial management followed the same logic: although formally legitimate instruments such as bank transfers and public contracts were used, intermediaries and informal practices enabled direct control over financial flows and workers, while maintaining an appearance of accounting regularity.

As outlined above, the system operated without explicit violence, relying instead on (implicit) economic and relational coercion. The operational model followed a consistent pattern across electoral cycles (2007; 2010). First, in the period preceding local elections, vulnerable individuals such as single parents, long-term unemployed, and precarious workers with expiring contracts were systematically identified and targeted. Second, they were approached by phone or in person (through home visits) and offered specific employment opportunities (e.g., in school cleaning, catering, municipal support, or social cooperatives) or contract renewals in exchange for **electoral support**. Public resources were also diverted for electoral purposes, notably through direct payments (of around EUR 50) or in-kind benefits as a form of exchange, including school meal vouchers.[73] In a third step, the exchange was formalised, in some cases in writing (e.g., photocopies of identity documents) and in others via intercepted telephone communications. Fourth, votes were cast on election day: some voters were accompanied to the polling stations to control voting, while in other cases a 'chain voting' scheme was used (i.e., 'ballot scheme').[74] Finally, in the post-electoral phase, the system was consolidated through the fulfilment of job-related promises when the candidate won, while non-compliance was sanctioned by withdrawing jobs or benefits. In this way, the cycle became self-sustaining and reproduced itself in subsequent electoral rounds.

The organisational architecture of the system was highly vertical, with a clear **division of roles** and tasks. At the top, a political actor linked to the criminal network exercised strategic control over the employment system, taking key decisions on recruitment and dismissal to align the allocation of resources with electoral objectives. A middle-tier intermediary managed day-to-day operations, including wage distribution through a controlled payment scheme in which cheques were issued, collected, and converted into cash. At the institutional level, municipal leadership played a central role in overseeing the allocation of public contracts to social cooperatives and in managing relations with

[73] These school meal vouchers were physically held in booklets by teachers. In one case, a teacher with access to them and family ties to the clan was able to divert and repurpose these public benefits as a form of electoral exchange.

[74] The investigations documented the use of the so-called '**ballot scheme**' (in Italian: *scheda ballerina*), through which voting was controlled. In practice, a blank ballot paper was taken out of the polling station, filled in externally, and given to a voter, who would insert it into the ballot box and return with a new blank ballot, which was then filled in again and reused in a continuous cycle.

regional authorities. At a higher political level, a national reference figure acted as a guarantor of institutional stability.

In addition to the system of electoral manipulation described above, the clan was involved in **money laundering activities**, in particular through the construction of the 'Il Principe' shopping centre in Casal di Principe. In this context, the entrepreneurial interests of individuals linked to the clan emerged, alongside connections to prominent political figures. Although this construction project served as the clan's principal money laundering vehicle, this report does not further examine the specific methods and activities associated with it.

Post-activity or post conditions

Documentary evidence indicates that the system exploiting social services for political-electoral purposes was active from at least 2000 to 2010-2011, spanning multiple electoral cycles and gradually consolidating. This shows that the phenomenon was not episodic, but a **stable and reproducible** mechanism over time. Such systems tended to persist even after repressive interventions, due to the continuity of the economic and familial relationships sustaining them.

The analysis of the case revealed numerous '**red flags**' pointing to the criminal use of these legitimate businesses. A first indicator concerned anomalous practices regarding personnel management, such as undeclared hiring, informal wage arrangements, and highly discretionary contract renewals. Additional indicators included the concentration of public contracts among the same sectors and the presence of family or relational ties between entrepreneurs and clan members. However, many signs of infiltration were difficult to detect through standard controls, as they were embedded in formally legitimate activities and did not produce immediately visible anomalies.

Law enforcement and judicial authorities intervened at an advanced stage of the criminal process, when the system was already consolidated and fully operational. The **investigations**, conducted by the *Direzione Investigativa Antimafia* (DIA) and the *Carabinieri* (i.e., the national gendarmerie of Italy), relied extensively on telephone interceptions, surveillance operations, and documentary evidence.[75] In addition to wiretaps, searches and seizures were carried out, yielding material evidence such as stolen blocks of meal vouchers, voter lists, and documents used in vote-buying activities. The investigation also included an analysis of corporate structures and financial flows, although financial inquiries proved complex due to fragmented records and the network's ability to conceal assets.

The investigations revealed a structured system in which legitimate social services and welfare programmes were systematically instrumentalised to sustain political power and reinforce the clan's influence over local institutions. The findings led to the issuance of **precautionary measures** against numerous suspects, on charges including mafia-type association, electoral corruption, and other offences aggravated by the use of mafia methods. However, the fact that the intervention occurred when the system was already deeply entrenched, highlights limitations in preventive capacities, since infiltration develops gradually and often becomes fully visible only once it is consolidated.

[75] With regard to the construction of the **shopping centre 'Il Principe'**, the investigation intervened at an earlier stage, when fundraising activities, access to financing, and negotiations with banking institutions were still ongoing. It also monitored the conduct of the electoral campaign of Casal di Principe.

4. Financial profile of the criminal network involved in Case Golf

Financing sources and start-up capital

The network's capital originated from the broader economic system of the Casalesi clan, fuelled by traditional illicit activities such as extortion, drug trafficking, and fraud. This capital provided a financial base supporting the clan's strategic activities, including the financing of electoral campaigns and the purchase of political support.

Payment methods and arrangements within the network

Financial exchanges within the network were largely untraceable, relying mainly on cash, although cryptocurrencies were also increasingly used. Cash was central to **vote-buying**, with payments typically ranging from EUR 50 to EUR 100 per voter, and higher amounts for organised 'vote packages'. Intercepted communications referred to sums of up to EUR 40,000 for a single electoral agreement, indicating a structured and systematic practice. In many cases, however, transactions did not take the form of direct payments. Professionals, for example, did not receive immediate remuneration but instead benefited over time from increased clientele and economic opportunities, creating a system of reciprocal advantage often more profitable than a single fee. Wages were partly paid through bank cheques (formally traceable) and partly through undeclared work. Due to their transferability and limited traceability, school meal vouchers were also used as in-kind payments.

Costs of business operations

With regard to the criminal use of companies operating in the social services sector, direct costs were relatively limited. There was no need to acquire companies outright; influencing the allocation of public contracts was sufficient. Moreover, staffing and management costs were largely avoided as key actors were already embedded within cooperative structures. Overall, social service employment was used as a political instrument that primarily redirected existing public expenditure rather than requiring new criminal investment. The main expenditures concerned vote-buying, payments to intermediaries, and the financing of political campaigns.[76] **Electoral corruption costs** were estimated at at least EUR 40,000 for the 2007 municipal elections, and EUR 15,000 for the 2010 provincial elections, alongside an unspecified number of cash payments ranging from EUR 50 to EUR 200 per vote across multiple electoral transactions. However, these costs were largely offset by the economic returns generated through access to public contracts secured via control over municipal decision-making.

Revenues and proceeds

A precise estimate of the revenues generated by the criminal network cannot be established. Nevertheless, the period under examination was characterised by significant financial capacity. This was reflected in regular payments to numerous households, reportedly amounting to approximately EUR 150,000 per month for senior members, and EUR 5,000 for affiliates. The distribution of proceeds followed the network's internal hierarchy, with shares allocated to leadership figures, operational actors, and the financing of new activities.

[76] The diversion of school meal vouchers also entailed a direct cost, quantified in terms of stolen booklets, although not precisely specified in the judicial records.

In general, the clan's revenues derived primarily from extortion, drug trafficking, and construction fraud (including EUR 5.5 million related to the 'Il Principe' shopping centre). Political infiltration, by contrast, generated indirect, non-monetary benefits such as access to public contracts, the appointment of loyal officials, and territorial control, which in turn facilitated further criminal activities. Within the social services sector specifically, revenues stemmed from public procurement contracts awarded to LTD1_G (for cleaning and catering services) and to LTD2_G and LTD3_G (for social care). Part of these funds was allegedly diverted to finance political operations and the personal enrichment of individuals involved.

5. Harms caused by Case Golf

Harms to individuals

At the individual level, the most significant harm concerns workers in the social services sector, many of whom are economically vulnerable. They become subject to a system of dependence in which access to employment and income continuity is contingent upon political loyalty. This particularly affects women, who may be subjected over extended periods to continuous and implicit coercion, as their income can depend on a discretionary decision, sometimes reduced to a phone call. This creates a situation of permanent economic blackmail and substantially compromises freedom of vote, as the risk of job loss constitutes an effective form of coercion even in the absence of explicit threats. Moreover, often irregular working conditions further increase workers' vulnerability and limit their protections, thereby exacerbating the harm both materially and in terms of civil rights.

Harms to other businesses

With regard to other businesses, the system significantly distorts the market. Companies without links to the criminal network are excluded from public procurement due to the absence of political-criminal ties. As a result, competitive mechanisms are undermined and legitimate entrepreneurship is penalised, discouraging participation in public tenders and limiting opportunities for economic development.

Harms to public institutions

Case Golf reveals a direct compromise of administrative structures. The presence of individuals linked to the clan within local institutions undermines their neutrality and democratic legitimacy. As the analysis shows, control over public administration effectively transforms the state from a guarantor of the collective interest into an instrument of criminal power. This compromise affected multiple areas of local governance:

- The municipality was infiltrated by clan members, including the mayor, administrative board, and technical office;
- Public procurement processes for social services were corrupted, causing financial damage to the public purse;
- The school system of the First Educational District was directly affected by the embezzlement of state-owned school meal voucher booklets, depriving pupils from low-income families of a welfare entitlement;
- The local health authority was implicated in promises of corrupt hiring;
- Multiple electoral processes were systematically falsified, undermining the democratic legitimacy of local governance;

- The Campania Region suffered harm through the diversion of social care funding into a patronage system controlled by organised crime.

Harms to the physical environment

Case Golf does not show significant direct impacts on the physical environment. However, the broader context in which the clan operates, including its infiltration into sectors such as construction and land management, suggests potential indirect effects arising from the misuse of public resources and the non-transparent management of territorial development.

Harms to the social environment

In the social environment, where infiltration can produce lasting and difficult-to-reverse effects, the clientelist system normalises the perception that access to employment depends on personal relationships rather than merit, fostering a culture of dependence and resignation. Consequently, a 'normalisation of subordination' emerges, whereby the system comes to be perceived as inevitable. Although such activities are illicit, they may nevertheless be socially tolerated because they generate income and employment, creating a grey area of acceptance that further entrenches the phenomenon.

Annex 3.H – Case Hotel: From Waste to Wealth

1. Criminal network involved in Case Hotel

The criminal network involved in Case Hotel was **linked to the Casalesi clan**, particularly to the Schiavone and Bidognetti factions, and emerged as a structured system integrating criminal, economic, and institutional dimensions. A total of 75 individuals were identified in connection with the case. In addition to the core members listed in Table 13, the network included numerous facilitators, including money launderers, colluding entrepreneurs and public officials, and professionals (e.g., lawyers, accountants, notaries). These actors helped ensure access to institutions, business management structures, and formal covers for activities. They performed distinct roles and functions, including the management of public procurement and tender procedures, operational support, disclosure of confidential information, and practices related to the preparation or simulation of bids. The network also included a chain of subcontracting, which made the structure more opaque and fragmented responsibilities.

Table 13

Overview of the core members of the criminal network involved in Case Hotel (Caserta)

Member	Role	Gender	Born between
C1_H	Leader; Group management and coordination; Strategic management of the clan	Male	1974-1993
C2_H	Leader; Group management; Overall management of criminal activities	Male	1954-1973
C3_H	Manager of the procurement sector (in the controlled territories)	Male	1974-1993
C4_H	Manager of the procurement sector (in the controlled territories)	Male	1954-1973
C5_H	Colluding entrepreneur; Support in tender management and bid rigging	Male	1974-1993
C6_H	Senior clan member; Top-level support and internal coordination within the clan	Male	1954-1973
C7_H	Senior clan member; Support and liaison between top management and other affiliates	Male	1954-1973
C8_H	Coordinator of bid-rigging activities; Providing mafia cover-ups	Male	1954-1973
C9_H	Leader	Male	1954-1973
C10_H	Senior figure in the criminal organisation; Providing mafia cover-ups	Male	1954-1973
C11_H	Colluding businessman and politician; Political intermediary facilitating contracts and sector control	Male	1954-1973
C12_H	Public official; Intervening in fund management and tender allocation	Male	1934-1953

The organisation has been operational since the early 1980s and, despite decades of judicial proceedings and mass arrests, it has demonstrated remarkable continuity, rebuilding its leadership through successive regent appointments.[77] The network was based not only on economic relationships but also on personal, trust-based ties built up over time. Within this framework, C11_H emerged as a key facilitator: a criminal manager capable of translating the clan's interests into the language of markets, public procurement, and administrative processes, without resorting to the overt violence traditionally associated with organised crime leadership. Moreover, the network mirrored a **corporate hierarchy**, with a *de facto* 'board' on top, composed of the heads of the main families and factions. Intermediate levels (often referred to as 'colonels') oversaw specific economic activities and channelled proceeds to a central fund. Below them, territorial managers (in Italian: *copa-zona*) controlled defined geographic areas, with each manager leading a group of affiliated members and remitting monthly earning to the central treasury. From this common fund, members received monthly salaries, while remaining resources covered shared expenses such as legal costs and weapons procurement. In addition, the clan historically formed alliances with rival organisations to divide territorial influence.

The network was involved in a **range of criminal activities**, including extortion across productive sectors (e.g., construction, commerce, and industry), typically applied as a percentage of contract value; systematic manipulation of public procurement tenders in civil engineering and waste management; drug trafficking; homicides and armed confrontations with rival clans; money laundering and reinvestment in legitimate businesses; corruption of public officials at municipal, prefectural, and regional levels; monopolistic control of key economic sectors; receiving stolen goods; and cheque-cashing schemes used to launder extortion proceeds.

2. Legitimate businesses involved in Case Hotel

An analysis of the judicial files related to Case Hotel revealed the involvement of several legally registered companies operating in the Campania Region that were directly linked to members of the criminal network. In this case, legitimate business activity was mainly represented by businesses operating in the collection, transport, and disposal of municipal waste. Based on these files, **two private limited companies** (LTD1_H and LTD2_H) appeared particularly relevant. A further thirteen smaller entities involved were either private limited companies or sole proprietorships.

- Formally, **LTD1_H** was a limited liability company based in the Province of Caserta. It regularly participated in public tenders and was awarded numerous contracts with local authorities, providing waste collection services in several municipalities both within the Province of Caserta (at least fourteen) and other Italian territories. These contracts involved substantial financial volumes. On the surface, its activity was fully legitimate: the company employed formally registered workers, operated a specialised fleet (e.g., compactors, street sweepers, light vehicles), and complied with the regulatory framework governing the environmental sector. In practice, however, LTD1_H functioned as an **instrument of the Casalesi clan** to secure public contracts, control a strategic economic, and channel illicit capital. Rather than being merely infiltrated, the company was structured and managed to serve the interests of the clan.

[77] Over time, the network has been subject to multiple judicial proceedings, mass arrests, and the application of the **'41-bis regime**' to its top leaders. The latter refers to a strict prison regime (in Italian: *carcere duro*) for mafia-related offences, as stipulated by Article 41bis of the Italian Prison Administration Act (Law No. 354 of 26 July 1975).

Effective control was exercised by C11_H, who acted as a key intermediary between the political-institutional sphere and the criminal network. He carried out a series of fictitious transfers of company shares to relatives, compliant associates, and frontmen, in order to circumvent anti-mafia certification requirements and asset freezing and confiscation measures.[78] LTD1_H remains formally active as of 2026, although it is currently under dissolution and liquidation following bankruptcy proceedings initiated in 2008.

- The same scheme involved **LTD2_H**, another company operating in the waste management sector. The business was managed in a manner similar to LTD1_H. Following share transfers in 2004-2005, ownership was fictitiously attributed to two members of the network, who were aware of the fictitious nature of the arrangement. The company held assets worth of at least EUR 120,000 (including two sweepers, two compactors, and vans). In 2026, LTD2_H was liquidated and removed from the Business Register.

3. Crime script based on Case Hotel

Motivation – Purpose

Within Case Hotel, the criminal use of legitimate businesses pursued **multiple objectives**.

- First, the network aimed to generate direct **economic profit**. Control over public procurement in the waste management and construction sector ensured high, stable, and continuous financial flows derived directly from public budgets. As waste collection constituted an essential public service, municipalities were rarely able to suspend contracts, even where contractors were affected by delays, deficiencies, or breaches of contractual obligations.

- A second objective was **money laundering** and the reinvestment of illicit capital. The companies functioned as laundering mechanisms embedded within legitimate economic activities. No *ad hoc* front structure was required, as the businesses were already operational, credible, and formally compliant. Illicit proceeds were mixed with revenues generated through public contracts, thereby acquiring the appearance of lawful income.

- Third, the network sought to establish **monopolistic control over the market**. Control of waste collection within a given area entailed a broader form of territorial control, including the daily circulation of vehicles, a workforce embedded in local communities, direct relationships with municipal authorities, and a constant operational presence.

- Fourth, the network sought to secure **political leverage**. C11_H's dual role as businessman and Regional Councillor enabled him to influence local administrative decisions in the awarding of tenders, thereby reinforcing the clan's institutional penetration.

[78] The **Anti-Mafia Code** (Legislative Decree No. 159/2011) currently regulates anti-mafia preventive measures, including anti-mafia documentation issued by the Prefectures. The system aims to prevent companies with direct or indirect links to organised crime from obtaining public contracts, concessions, or authorisations. In this context, practices such as fictitious share transfers, the use of frontmen, and fragmented ownership structures are designed to obscure beneficial ownership and circumvent preventive controls.

Preparation

The network involved in Case Hotel exploited companies operating in the **waste management sector**, one of the most sensitive sectors in the Campania Region.[79] The sector could be understood as comprising two distinct segments:

- **A fully illicit segment;**
  In the 1980s and 1990s, the Casalesi clan developed a large-scale criminal system centred on the illicit trafficking and disposal of waste, coordinated by key entrepreneurial actors. Industrial, toxic, and in some cases radioactive hospital waste, originating from Italy and abroad, was illegally dumped in the Caserta Province, generating substantial profits by avoiding lawful disposal costs. These proceeds were channelled both to the clan's leadership and to the common fund, thereby contributing to the consolidation and expansion of the organisation. However, these practices had severe environmental and public health consequences in the affected area, commonly referred to as 'Terra dei Fuochi' (cf. *supra*).

- **A formally legal segment;**
  As judicial pressure increased through arrests, seizures, and cooperation with justice, the organisation shifted from clandestine disposal to the formal management of the urban waste cycle via companies operating under public contracts.[80] This transition marked a key turning point, as embedding itself in the legal economy reduced visibility, making detection and enforcement more difficult. Moreover, criminal interests have shifted towards the transport of waste outside the Campania Region, environmental remediation activities (i.e., decontamination of the polluted land), and the management of stockpiled waste sites.

Waste management remains an essential public service, indispensable to the functioning of communities and the protection of public health, involving all municipalities in the region. The sector is labour-intensive and **structurally complex**, involving multiple stages, numerous (public and private) companies, and thousands of workers. It generates stable financial flows and high-value, multi-year public contracts but remains affected by infrastructural shortages, territorial disparities, and limited oversight due to the complexity of the waste cycle. Within an emergency-based governance framework (see Footnote 80) and a limited number of qualified operators, these conditions facilitated rapid entry by actors with substantial financial capacity, including organised crime groups. Although anti-mafia certification aimed to exclude criminal actors, it often incentivised concealed ownership structures rather than effective prevention. The sector's reliance on municipal and regional political networks further increased its vulnerability to infiltration by actors operating at the nexus of politics and organised crime. Consequently, the distinction between lawful and unlawful operations has become increasingly blurred, as companies originating in a criminal context progressively operated within the formal economy while retaining, less visibly, links to the criminal organisation.

[79] The Campania Region generates approximately 2.5 to 2.6 million tonnes of municipal waste annually (Porrazzo, 2025).

[80] In 1994, following the saturation of several landfills across the region, the Italian Government declared an environmental emergency in Campania (Law No. 225/1992) and established an extraordinary governance regime under a Special Commissioner with extensive powers to derogate from ordinary public procurement and administrative rules. This prolonged emergency framework (1994-2009), based on centralised decision-making and simplified contracting procedures, significantly reshaped the waste management sector and created structural vulnerabilities that could be exploited by organised crime (European Parliament, 2010).

In addition to these sector-specific vulnerabilities, the criminal network also exploited company-specific characteristics to facilitate infiltration. In particular, the legal form of LTD1_H and LTD2_H as **limited liability companies** proved conducive to the network's strategy, enabling flexible ownership arrangements, including rapid changes in shareholding structures, the replacement of shareholders and directors, and the concealment of beneficial ownership. This structure also facilitated the use of frontmen, allowing effective control to be concealed and anti-mafia checks circumvented through fictitious ownership transfers. As investigative pressure increased, the companies' formal structures could therefore be altered without affecting underlying control. Both LTD1_H and LTD2_H operated at a strategically advantageous intermediate scale: sufficiently large to secure significant contracts, yet not so prominent as to attract immediate regulatory scrutiny.

LTD1_H operated through public contracts, formally employed staff, and owned equipment, providing a **credible façade** that blurred the distinction between lawful and unlawful activity. Its reliance on relationships with public authorities further strengthened the network's position. Since the waste sector is dependent on public procurement, control over political and administrative relationships made it possible to exert influence over contract awards and consolidate the companies' market position. LTD1_H's dominant role in Caserta's waste management created barriers to entry for competitors, while its geographically dispersed operations across multiple municipalities generated multiple points to extract illicit rent.

Pre-activity or enabling conditions

In the pre-activity stage, activities included the establishment of companies, the selection of nominee shareholders, the structuring of bids for public tenders, and the identification of subcontractors, all conducted through **formally lawful mechanisms**. Regarding market entry, in the early 1990s a convicted member of the Nuvoletta faction introduced C11_H into the waste management sector as a replacement frontman for a company then under investigation. Subsequently, he remained involved in the establishment and management of LTD1_H. Regarding ownership concealment, as anti-mafia scrutiny increased, C11_H fictitiously transferred shares to nominees. When pressure eased, ownership was transferred back. This cycle was repeated several times between 2004 and 2006.

From its inception, LTD1_H was established and managed as an **operational instrument** for the clan. Core business functions, such as participation in tenders and contract management, were aligned with the interests of the criminal network. Legal and illegal activities were thus closely intertwined: while the company performed public waste collection services, it simultaneously functioned as a vehicle for market control, money laundering, and the distribution of illicit proceeds. The company's level of **culpability** can be characterised as maximal. The individual exercising *de facto* control (C11_H) was fully aware of, and directly involved in, the criminal activities. The nominal shareholders and frontmen also appear, for the most part, to have been aware of the fictitious nature of their roles. Although they did not exercise genuine decision-making power, they facilitated the system by consenting to act as formal owners or directors, thereby concealing the true locus of control.

Activity

LTD1_H operated as a genuine **'dual use' enterprise**. On the one hand, its day-to-day operations were real, providing effective cover: the business regularly provided waste collection and management services with staff, equipment, and public contracts. On the other hand, it formed an integral part of the clan's economic strategy. Criminal management activities included negotiating extortion payments to multiple clan factions, orchestrating fictitious share transfers in anticipation of anti-mafia checks, leveraging its legitimate status to access public tenders, and managing relations with representatives of the criminal organisation.

In practice, the network operated as follows. C1_H, the regent of the criminal organisation, delegated the management of all public tenders in Casal di Principe to C3_H (his son), who also fraudulently managed regional funding from the Campania Region. Compliant contractors prepared so-called '**supporting bids**' (in Italian: *buste di appoggio*), fictitious tenders calibrated to manipulate the mathematical average used to determine the anomaly threshold under Law 415/1998.[81] C11_H attended meetings with municipal officials and administrators to pre-arrange tender outcomes, while complicit officials provided insider information on competing bids and the identities of non-compliant bidders. Non-compliant bidders were coerced into withdrawing or submitting artificially inflated or deflated bids. Following the formal award of the contract, C1_H and C3_H effectively controlled and supervised the works, while C5_H functioned merely as an intermediary for invoicing and payments, transferring the proceeds to the clan.

Post-activity or post conditions

In Case Hotel, legitimate businesses were used for criminal purposes over a **prolonged and continuous** period. The information gathered indicated that the companies' involvement in the criminal network dated back to the early 1990s, when C11_H entered the waste sector with the support of criminal circles. This activity continued for approximately eighteen to twenty years, at least until the conclusion of the investigation around 2008. This demonstrated the continuity and resilience of the system, which remained operational over time despite regulatory controls and investigative pressure.

Over time, however, there were some **signs pointing to the criminal use** of these businesses. One of the main indicators was the repeated suspension or refusal of anti-mafia certification for LTD1_H by the Prefecture of Caserta, the authority responsible for verifying the absence of links between companies contracting with the public administration and organised mafia crime. Further indicators included multiple fictitious share transfers linked to periods of investigative pressure. They also included documented meetings between C11_H and one of the leaders of the Bidognetti faction at the premises of LTD1_H, as well as assets, including vehicles registered in the name of LTD2_H, that were found to have been acquired through false invoicing.

[81] Under **Law 415/1998** (*Merloni Ter*), public contracts were generally awarded to the lowest bidder. To prevent unreliable or artificially underpriced offers, the law also provided for the automatic exclusion of 'abnormally low' tenders through a mathematical mechanism based on the average of submitted bids. Criminally linked companies therefore had to submit bids low enough to secure the contract, but not so low as to trigger exclusion. Criminal organisations manipulated this system through fictitious **'supporting bids'**, designed not to win the contract but to distort the average used to calculate the anomaly threshold. By strategically coordinating multiple collusive bids, the network could favour a pre-selected company, making its tender appear formally compliant while the outcome had in reality already been predetermined.

The intervention of the authorities took the form of a complex and wide-ranging **investigation** conducted by the District Anti-Mafia Directorate (DDA) of Naples, with the support of the Carabinieri's ROS. This required extensive investigative efforts, including the following:

- Wiretaps and long-term environmental interceptions, which enabled the reconstruction of relationships between the suspects and clan members;
- Financial and asset analyses, aimed at identifying suspicious financial flows and economic inconsistencies;
- Documentary checks, such as the examination of company records, public procurement contracts, and anti-mafia certifications issued by the Prefecture of Caserta;
- The collection of testimonies and statements from cooperating witnesses, which provided crucial evidence.

The investigation concluded with the issuing of a **pre-trial detention** order by the investigating judge (GIP) of the Court of Naples, who found serious indications of criminal offences. The charges included, *inter alia*: mafia-type criminal association, fictitious registrations of assets, bid rigging, and money laundering.[82] At the same time, asset seizure and confiscation measures were initiated, targeting company shares, vehicles, and other assets linked to the criminal activity, with the aim of disrupting the network's operational capacity. However, even following judicial clarification, the understanding of the underlying mechanisms has remained partial, underscoring the inherent difficulty in fully capturing the scope of such phenomena.

4. Financial profile of the criminal network involved in Case Hotel

Financing sources and start-up capital

Initial capital mobilised by the Casalesi clan derived from **criminal proceeds** accumulated since the 1980s, including extortion of local businesses in the Province of Caserta, drug trafficking, monopolistic control of the concrete and aggregates market, and agricultural subsidy fraud. These funds were subsequently reinvested in entrepreneurial activities. While the waste sector remained the principal area of accumulation for a long time, interests later expanded into environmental remediation and waste transport, both characterised by substantial public funding.

Payment methods and arrangements within the network

The network's preferred payment method was cash delivered via trusted couriers, supported by handwritten accounting records documenting payments and outstanding balances. The network also used bank cheques and promissory notes, which were laundered through operations involving complicit contractors. In just one documented transaction alone, EUR 7,800 was laundered in this way. Bank transfers were also used, particularly for the distribution of LTD1_H's monthly revenues amongst individuals linked to the clan. Another commonly used method involved false invoicing schemes: vehicles belonging to LTD1_H and LTD2_H were formally purchased through fictitious invoices issued by a complicit company.

[82] The case also provided evidence of C11_H's direct involvement in appointing a compliant General Director at a hospital in Caserta, demonstrating the clan's penetration of the healthcare sector through his political role. Article 323 of the Italian Criminal Code (as applicable at the time of the facts), criminalised conduct by public officials who, in breach of their legal duties or the principle of impartiality, intentionally procured an unlawful financial or professional advantage for themselves or third parties, or caused unjust harm to others.

With regard to the financial arrangements within the network, several examples of payments were documented. For example, C11_H paid approximately ITL 30 million (EUR 15,500 at the time; approximately EUR 28,000 to EUR 30,000 in today's value) per month to the Casalesi clan in exchange for protection. Electoral financing constituted another significant financial channel. During the 2004-2005 regional elections, approximately EUR 45,000 (EUR 30,000 plus an additional EUR 15,000) was provided to C11_H's representatives to a particular faction of the Casalesi clan in exchange for electoral support. In the construction sector, extortion was typically calculated as a percentage of the value of public contracts. Judicial records documented payments of 2.5% of the contract value in one case, and an agreed rate of 5% in relation to another tender. More broadly, the organisation operated through a centralised treasury system in which revenues collected across clan-controlled territories were pooled and subsequently redistributed as monthly salaries to affiliates.

Costs of business operations

The criminal network incurred substantial operational costs required to maintain territorial control and ensure the continuity of its activities. These included monthly **salaries** paid to hundreds of affiliates, with amounts varying according to rank and role within the organisation. Additional recurrent costs comprised legal defence expenses for detained members, the procurement of weapons, and the management of fugitives through safe houses and communication systems. The organisation also incurred costs associated with negotiated territorial 'peace agreements' with rival criminal groups. In addition, specific costs arose in connection with the criminal use of LTD1_H and the waste-management sector. These included **notarial and registration expenses** related to fictitious share transfers between 2004 and 2006. The network also covered payments and bribes to municipal officials involved in the manipulation of tender procedures, as well as legal and administrative expenses linked to anti-mafia certification proceedings.

Revenues and proceeds

The waste-management sector represented a profitable source of revenue for the Casalesi clan. One single municipal contract generated approximately EUR 13.2 million in revenue in 1999, with additional profits derived from more than thirteen further **municipal contracts**. LTD1_H formally declared capital of around EUR 830,000, although judicial findings indicate that this figure significantly underestimated the network's actual economic value. LTD2_H declared approximately EUR 416,000 in capital, together with an additional EUR 120,000 in equipment. Further profits were derived from public tenders, including a EUR 530,000 programme contract in Caserta. Municipal payments were received by LTD1_H, which functioned primarily as an invoicing intermediary. Subsequently, extortion payments were distributed to the relevant clan factions, and the remaining profits were retained by C11_H.

Proceeds were laundered through repeated fictitious share transfers and a complex corporate network involving more than thirteen companies operating across different sectors. Criminal profits were subsequently reinvested in additional service businesses, including two sports-betting shops, as well as in the acquisition of real estate and agricultural assets.

5. Harms caused by Case Hotel

Harms to individuals

With regard to individuals, the harm manifested both directly and indirectly. On the one hand, control exercised by the criminal network created an environment of pressure, intimidation, and coercion towards economic operators and those unwilling to comply with the system. On the other hand, citizens in multiple municipalities were exposed to higher service costs and lower service quality, as clan-controlled companies were incentivised to minimise operating costs to maximise clan rents. As noted in the interviews, the population is often aware of links between certain companies and the criminal environment, yet struggles to fully recognise their severity, partly because these activities generate income and employment. This, in turn, contributes to a process of normalisation whereby the harmful nature of illegal activities is downplayed or insufficiently perceived.

Harms to other businesses

From an economic perspective, the harm to other businesses and workers is significant. Companies linked to the criminal network enjoy a competitive advantage, distorting the market and progressively marginalising or excluding legitimate businesses. Consequently, the local economic system is fundamentally altered, as the selection of market actors is no longer based on efficiency or quality, but on their ability to integrate into illegal relational networks. Workers employed under irregular conditions may also be used instrumentally in clan negotiations, for instance as bargaining chips in territorial discussions between clans. Moreover, clan-backed incumbency artificially raises barriers to market entry, preventing new entrants and contributing to cascading harm, particularly in the construction sector.

Harms to public institutions

Public institutions are likewise deeply affected. Tender procedures are manipulated, public resources are allocated inefficiently, and political decision-making is influenced by illicit interests. Consequently, the systematic corruption of municipal officials erodes public trust in both public institutions and democratic governance.

Harms to the physical environment

The damage to the physical environment is severe. Illegal waste management, particularly the illicit disposal of industrial and toxic waste, has resulted in the contamination of extensive areas of the Province of Caserta, comprising soil and groundwater quality and causing long-term consequences for ecosystems and public health. Criminal infiltration also creates broader infrastructural risks. In public works projects managed by clan-controlled firms, the incentive to minimise construction and operational costs in order to maximise illicit profits may compromise the quality and safety of civil engineering works, including sewage systems, roads, and other public infrastructure.

Harms to the social environment

The analysis reveals a significant impact on the social environment. The infiltration of organised crime into the legitimate economy undermines mechanisms of trust and social regulation, gradually fostering the normalisation and acceptance of illegality.

Annex 3.I – Case India: Gambling as Governance

1. Criminal network involved in Case India

The criminal network involved in Case India was **linked to the Casalesi clan**, particularly to a faction holding significant influence within the organisation. As noted above, the network is characterised by a long-standing historical continuity, marked by the intergenerational transmission of roles, relationships, and operational practices, despite arrests and leadership changes. Its structure appeared hierarchical yet streamlined, prioritising economic efficiency over territorial control. A total of 50 individuals were identified as members of the network. Table 14 presents an overview of its core members. In addition, the network also comprised individuals involved in drug trafficking (including storage, transport, and distribution) and other faction members performing a variety of roles.

Table 14
Overview of the core members of the criminal network involved in Case India (Caserta)

Member	Role	Gender	Born between
C1_I	Regent; Clan management; Coordination of illicit activities	Male	1954-1973
C2_I	Clan member; Operational support; Cash management; Salary distribution	Male	1974-1993
C3_I	Clan member; Operational support; Cash management; Drug trafficking	Male	1954-1973
C4_I	Clan member; Operational support; Cash management; Drug dealing; Territorial control	Male	1934-1953
C5_I	Historical leader; Strategic leadership; Clan command; Definition of criminal operations	Male	1954-1973
C6_I	Leader; Management of clan activities	Male	1974-1993
C7_I	External aiding and abetting; Management of entertainment-equipment businesses	Male	1974-1993
C8_I	External aiding and abetting; Collaboration in company management	Male	1974-1993
C9_I	External aiding and abetting; Participation in business management; Generation of illicit proceeds	Male	1974-1993
C10_I	Clan member; Use of the clan's intimidatory power to issue threats and enforce victim subjugation	Male	1974-1993
C11_I	Clan member; Extortion facilitator; Application of mafia-type coercion against victims	Male	1954-1973
C12_I	Clan member; Involvement in commercial imposition practices; Contribution to extortion	Female	1974-1993
C13_I	External aiding and abetting; Complicity in possession and availability of illicit weapons	Male	1954-1973
C14_I	Financial intermediary; Revenue collection; Management of relationships with drug dealers	Male	1934-1953

C1_I appeared to occupy the apex of the organisation, **acting as 'regent'** and playing a central role in reorganising the network's criminal activities following his release from prison in August 2014. His position must be understood within a context of 'leadership under constraint', whereby historical clan leaders were detained under the 41-bis regime (cf. *supra*) yet continued to exert indirect influence over the organisation. The network maintained a continuous functional link with its upper levels, ensuring the systematic transfer of financial resources to detained members and their families, thereby sustaining internal cohesion and operational continuity.

More broadly, the network was structured across multiple intermediate and peripheral levels. On one level, **economic operators and facilitators**, including highly skilled professionals, particularly those involved in the technical organisation and management of digital gambling platforms, such as IT specialists (so-called 'white-collar' actors). Although formally external to the organisation, these actors maintained stable relations with the clan and functioned as its primary interface with the legal market. They were responsible for configuring servers, structuring the technological infrastructure, and managing the organisation's IT operations. This reflects an evolution in the organisation's internal dynamics, characterised by the integration of technological expertise and an increasing role diversification. On another level, a broader group of **affiliates** and collaborators, both free and

detained, received periodic payments from a common fund, ranging from EUR 500 to EUR 2,500. This system of regular remuneration constituted a structural feature of the organisation, sustaining member loyalty and preserving the associative bond, including under conditions of detention.

Moreover, the network was largely grounded in **family and territorial ties**, which reinforced internal trust and reduced the risk of defection. These ties not only structured the organisation but also enhanced its resilience, enabling rapid member replacement and continuity of operations. Relational dynamics were therefore as significant as hierarchical structures, producing a system combining vertical organisation with dense territorial and social embeddedness. A further defining feature was its economic orientation: the clan functioned as an organised system for managing financial resources, in which the collection, distribution, and control of monetary flows constituted core activities. In this sense, the network operated as a form of illicit **economic governance**, integrating licit and illicit activities within a coordinated framework. Finally, the network's adaptive capacity was evident. Its shift towards less visible sectors more deeply embedded in the legal economy, such as gambling, reflected an evolutionary strategy aimed at reducing legal exposure while securing more stable revenue streams.

2. Legitimate businesses involved in Case India

An analysis of the judicial files related to Case India revealed the involvement of a legally registered private limited company operating in the Campania Region (**LTD1_I**), which was directly linked to members of the criminal network. LTD1_I operated as a formally legitimate enterprise engaged in the rental and management of **gaming machines** (slot machines and video lottery terminals), with approximately four hundred devices deployed across several municipalities in the Agro Aversano area. Alongside this direct market presence through a registered company, a second line of activity emerged in the form of **online gambling platforms**. Although formally part of the regulated market, these platforms were in practice accessed via locally controlled intermediary channels. Bets were channelled through retail outlets (such as bars), which functioned as collection points.

The company displayed typical **features of indirect control**, including the use of nominee ownership, a separation between formal ownership and effective decision-making power, and stable networks linking economic operators with criminal actors. In particular, the company, although formally registered under a nominee, was in practice managed by individuals with sector-specific expertise and established local connections. Retail operators, particularly bar owners, constituted the final link in the commercial chain. Although formally operating within the legal market, these actors often functioned under conditions of contractual vulnerability. The available evidence suggested that, in most cases, they did not act as fully aware or autonomous participants, but rather as operators constrained by external pressures that significantly limited their decision-making autonomy.

3. Crime script based on Case India

Motivation – Purpose

The involvement of the Casalesi clan in the gambling sector was primarily aimed at ensuring the economic sustainability and organisational stability of the criminal structure, while consolidating **territorial control** through the management of market dynamics. Gambling, both through gaming machines (i.e., its material component) and online platforms (i.e., its digital dimension), played a central role in financing the so-called 'clan fund' (in Italian: *cassa del clan*). Moreover, the network strategically exploited the revenues generated by these activities. Beyond profit-making, these resources served to maintain internal cohesion. In particular, financial flows from the sector enabled the systematic payment of 'salaries' to affiliates, including individuals detained under the 41-bis regime (cf. *supra*) and their families. This mechanism reinforced loyalty and discouraged cooperation with judicial authorities, positioning the gambling sector as an **instrument of criminal governance**. It supported both profit generation and the long-term survival of the organisation, reflecting the full integration of legitimate business activities into the operational model of the Casalesi clan.

The gambling sector was preferred over more traditional and visible criminal activities, such as drug trafficking or violent extortion. Its integration within the legal economy enabled the organisation to reduce legal exposure while enhancing its capacity for concealment (cf. *infra*). The criminal exploitation of the sector served **three interrelated purposes**: securing stable and predictable financial flows, limiting exposure to law enforcement, and consolidating territorial and economic control through coercive influence over market dynamics. The presence of approximately four hundred slot machines linked to the network in the Agro Aversano area illustrated how gaming machine management served as a mechanism for systematic profit extraction through territorial control. This reflects a significant evolution in the business model of mafia-type organisations, which increasingly adopt forms of 'meta-regulation' of the market. The clan operated not only as a direct economic actor, but also as an illicit guarantor of territorial monopolies, imposing conditions of market access and excluding competitors. This configuration can be interpreted as a form of '**criminal franchising**', characterised by low operational costs and a strong capacity for adaptation and long-term continuity.

Preparation

Within the Agro Aversano area (Province of Caserta), the **gambling sector** represents a major economic activity while remaining highly vulnerable to criminal infiltration. In Italy, the gambling market generated approximately EUR 157 billion in turnover in 2024 and contributed around EUR 11 billion annually in tax revenues. The sector also experienced a growing shift towards online gambling, which accounted for more than half of total turnover. It is not only economically significant but also widely used, with an estimated twenty million people in Italy regularly engaging in public gambling, underscoring its entrenchment in everyday life. In this context, Southern Italy consistently records among the highest levels of gambling activity, both in absolute and *per capita* terms. The provinces of **Naples and Caserta** are especially affected: the widespread availability of gaming machines (both slot machines and video lottery terminals) in bars and small businesses, combined with the growing accessibility of online gambling platforms, normalises gambling as a routine social activity. This pervasive presence is closely associated with adverse socio-economic conditions, including unemployment rates exceeding 20% in the Province of Naples in 2024, which heighten population vulnerability and reinforce reliance on marginal or supplementary income sources.

Case India illustrates how the sector's dynamics operated at the local level, as its key economic features closely aligned with the vulnerabilities exploited by organised crime. First, the network benefited from a **pre-existing infrastructure** inherited from earlier phases of clan leadership. The system of gaming machines and betting platforms was not created *ex novo* but taken over and reorganised through already established relationships with local economic operators. This continuity reduced entry costs and enabled the rapid reactivation of financial flows, as reflected in the swift reorganisation implemented by C1_I following his release from prison. The sector's vulnerabilities were also linked to the **territorial distribution** of betting machines: profitability depended on the widespread installation of gaming devices, a requirement that criminal organisations were particularly well positioned to exploit due to their operational capacity and territorial control.

The attractiveness of the gambling sector for organised crime was further reinforced by structural vulnerabilities, including the lack of transparency in financial flows, particularly in online betting. Moreover, the network exploited opportunities arising from the growing **digitalisation** of the sector, particularly through online betting and poker platforms. The use of digital infrastructures, often located in offshore or complex jurisdictions, further increased the opacity of financial flows and hindered the identification of beneficial ownership, thereby expanding its activities and limiting oversight and enforcement. **Legal restrictions** also created opportunities. In Italy, for example, maximum betting thresholds encouraged criminal organisations to establish illegal circuits through which bets could be played beyond the permitted limits, thereby increasing their attractiveness to bettors (cf. *infra*).

Furthermore, the sector operated within a multi-layered economic system involving equipment suppliers, operational managers, local retailers, and digital platforms. The sector offered a favourable balance between risk and profit, combining high revenues with relatively limited criminal sanctions. Investigations were further complicated by the use of prepaid cards loaded with betting funds and registered under strawmen, making it difficult to trace both bettors and the networks managing the system. This was compounded by the extensive **use of cash**, which further obscured financial flows. At the same time, the sector was characterised by a limited number of operators, as market access depended on state authorisation. This reduced competition and facilitated the identification of key market actors, thereby creating favourable conditions for criminal infiltration.

Alongside sectoral vulnerabilities facilitating criminal infiltration, business-level vulnerabilities include discrepancies between formal ownership and effective control. Although LTD1_I was formally legitimate, it was in practice managed by individuals linked to the clan. In combination with a **territorial context** characterised by a longstanding mafia presence, these factors fostered coercive dynamics that were difficult to detect externally. As noted above, the Agro Aversano area is characterised by a long-standing presence of organised crime, which facilitates the implicit acceptance of informal forms of market control. In such an environment, widespread awareness of criminal dynamics coexists with a limited capacity for resistance, creating favourable conditions for the expansion of the system.

Overall, the preparatory phase in Case India can be understood as resting on **three interrelated factors**:

- The continuity of relationships and historical embeddedness, enabling immediate access to the market;
- The exploitation of sectoral vulnerabilities linked to organisational and regulatory features;
- Adaptation to economic and technological transformations, particularly digitalisation.

Pre-activity or enabling conditions

The infiltration process can be broadly outlined as follows. Initially, the clan identified the gambling sector as a strategic area for investment. The selection of activities and operators was guided by criteria of profitability and controllability, both closely linked to territorial dominance. Criminal organisations established and maintained their presence in a given area through intimidation, violence, and threats, ensuring pervasive control exercised via individuals physically present in the territory and capable of asserting the organisation's dominance. In the context of Caserta, **territorial control** by the Casalesi had long been near-total: for over forty years, they exercised widespread dominance across the municipalities of the Caserta Province and along the Domitian Coast, without effective counteraction. Infiltration in this sector thus initially developed through strong territorial embedding, whereby criminal organisations asserted their dominance through direct control of the territory. Over time, however, the *modus operandi* evolved into a more complex and circulated system, for instance through the use of companies established abroad to circumvent the national regulatory framework. Overall, Case India illustrates a shift from predatory forms of criminality towards structured, systemic, and continuous models of organised economic crime.

From an operational perspective, the criminal exploitation of business activities relied on consolidated mechanisms of **indirect economic control**. In the slot machine segment, the clan did not generally manage the equipment directly but instead imposed a territorial monopoly. Authorised operators were granted exclusivity within the controlled area in exchange for fixed monthly fees, ensuring a stable revenue for the organisation. While resembling franchising arrangements, this model operated through coercive means, with economic value deriving not from entrepreneurial efficiency but from the capacity to enforce territorial control. Control was exercised through the exclusion of competitors and the monitoring of compliance, thereby establishing a form of illegal market regulation. In the online betting segment, the operational model was more intrusive and control was more centralised: representatives of the clan identified retail outlets and imposed the use of specific betting platforms on local operators. Technical management, including the activation of credits and the control of digital accounts and financial flows, was centralised and handled remotely by individuals within the network. This enabled the organisation to position itself as an indispensable intermediary between supply and demand, without relying on a formally attributable corporate structure.

In the present case, LTD1_I exhibited a **high degree of responsibility**. Although formally legitimate, it operated within a system characterised by a clear separation between formal ownership and effective control, often mediated through nominee arrangements. In other cases, however, business operators have no real alternative and are compelled to enter into arrangements with the criminal organisation. Such arrangements are convenience-based, but not fully voluntary. This is evident at the level of retail operators, such as bar owners, who constitute the final link in the distribution chain. In these cases, the organisation imposes the installation of specific gaming machines or betting platforms. The

agreements, while formally consensual, are in fact shaped by coercion and an underlying climate of intimidation. As a result, these actors display limited or negligible culpability.

Activity

The *modus operandi* was characterised by a structured system designed to circumvent regulatory controls and obscure financial traceability. Patterns of infiltration into legal businesses were similarly diverse. Multiple mechanisms coexisted, ranging from wholly illegal activities to forms of penetration within the legal market. Criminal networks frequently targeted already **existing firms**, particularly those in financial distress, leveraging their structures and injecting illicit capital to foster expansion. Alternatively, ***ad hoc* companies** were established, often registered under a strawman, albeit with greater exposure to detection. In some instances, established firms entered into arrangements with criminal networks, creating *de facto* partnerships or allowing individuals linked to the network to participate in the management of the business alongside formal leadership.

In the **fully illegal betting sector**, operations typically involved the use of prepaid cards registered under fictitious identities, thereby preventing the identification of bettors. These cards enabled users to place bets exceeding statutory thresholds established under Italian law, with transactions channelled through companies located abroad, often in jurisdictions where such limits did not apply. While authorised venues in Italy imposed caps on betting amounts, these restrictions were effectively bypassed through foreign platforms. Bets covered a wide range of events and, in the case of winnings, proceeds were repatriated to Italy in cash, without passing through traceable financial channels. These funds were then redistributed locally by designated members of the criminal network. **Foreign-based companies** thus functioned as financial hubs, facilitating the transfer of substantial sums abroad, often exceeding legal thresholds (e.g., EUR 5,000 under Italian law). This generated significant untaxed revenue. Within this framework, the criminal organisation coordinated access to betting platforms, managed local operators, and oversaw cross-border financial flows. In some cases, this reflected direct control, with the criminal organisation managing the activity itself. More commonly, however, involvement took indirect forms: entities operating abroad were not formally linked to the organisation but maintained stable relationships with it, for example through the payment of a '*tangente*' in exchange for the possibility to operate within a given territory.

In other configurations, particularly within the **legal betting sector**, the organisation did not directly operate betting services but imposed territorial monopolies. In this scenario, profits derived from service provision, with the criminal organisation acting as a concealed partner entitled to a share of the proceeds. Business owners were often compelled – either through coercion or profit-sharing arrangements – to install specific slot machines supplied by operators affiliated with the clan, who in turn paid a '*tangente*' to operate within the territory. This arrangement distorted market competition and also applied to legally authorised slot machines connected to the State monopoly circuit. Such systems were enabled by strong **territorial control**. Service providers seeking to install machines were required to reach agreements with the organisation, typically paying a fixed or variable share of profits. In return, they obtained exclusivity within the territory, as well as protection from competitors. The relationships between the clan, service providers (e.g., bars or gaming halls), and business owners varied: the criminal organisation sometimes acted as a *de facto* partner sharing profits, while in other cases it simply imposed its conditions without any possibility of refusal.

In certain cases, the organisation **manipulated betting outcomes**, effectively determining whether wagers resulted in wins or losses. This was achieved, *inter alia*, by altering the results displayed on screens for sporting events, often taking place abroad. At times, to favour a criminal organisation's leader or other high-value individuals, betting centre displays were altered to show a predetermined winning outcome. In most cases, however, the opposite occurred: bettors, for example on US basketball matches, were presented with manipulated results indicating outcomes different from the actual ones, resulting in losses even where the bets would otherwise have been winning.

From a structural perspective, the organisation functioned as a form of **illicit economic governance**. Rather than operating as a conventional entrepreneur, it acted as an informal regulator of the gambling market, shaping economic behaviour through coercion, relational networks, and control over access to business opportunities. Legitimate activities – such as the distribution of gaming machines and the use of online betting platforms – were incorporated into a system that replicated the core functions of a firm, including coordination, resource allocation, and financial management, while remaining outside formal regulatory frameworks. This configuration could be described as an 'enterprise without ownership': legal ownership remained with ostensibly independent actors, whereas effective control was exercised by the criminal network. Overall, Case India illustrated that contemporary organised crime extends beyond market infiltration to **active market governance**. Legitimate economic activities were transformed into instruments of social and economic control, enabling criminal networks to extract resources, regulate competition, and ensure long-term resilience.

Post-activity or post conditions

The analysis of Case India showed that business activities in the gambling sector were used for criminal purposes in a continuous rather than occasional manner. Although the judicial investigation covered the period between August 2014 and May 2015, the evidence suggests that the illicit use of economic activities formed part of a **long-term dynamic** linked to the historical presence of the Casalesi clan in the Agro Aversano area. Additional ongoing investigations indicate that the phenomenon persists over time and extends beyond national borders, thereby confirming its transnational dimension. In this sense, the duration of criminal use could not be confined to the timeframe of the specific investigation but should be understood as the manifestation of a stable infiltration of the gambling sector, whereby formally legitimate activities were incorporated into the economic model of the criminal network.

The **indicators of infiltration** into the gambling sector were multiple and consistent with established patterns of organised crime penetration into the legal economy. One key warning sign was the sudden growth of companies with no prior economic strength, or the rapid development of large-scale construction projects by firms lacking sectoral experience. In concrete terms, this was reflected in previously marginal companies becoming key actors within a short timeframe, for example through investments such as shopping centres or large development projects. This pattern indicated a mismatch between formal ownership and effective control, as ostensibly legitimate companies were in fact managed by individuals linked to the criminal network, often through nominee arrangements. Another indicator was the existence of imposed territorial monopolies, whereby the same operators systematically obtained exclusivity in the management of slot machines or betting platforms within specific areas, in the absence of genuine competition.

With regard to Case India, law enforcement authorities relied on a combination of investigative tools, including telephone and environmental interceptions, surveillance activities, financial analysis, and the collection of testimonial evidence.[83] **Law enforcement intervention** in these contexts was complex, as the system relied on dynamics of widespread adaptation and implicit complicity: business owners were unlikely to report misconduct, and operators excluded from the market rarely challenged distortions. As a result, the system tended to be self-reinforcing. The information provided by cooperating witnesses was therefore crucial in enabling investigative authorities to identify initial leads and activate more intrusive measures. More rarely, judicial investigations also originated from high-profile or violent events, such as attacks or acts of intimidation.

Ultimately, judicial action led to the identification of key individuals, including leaders and economic intermediaries, and to **prosecutions** for offences such as participation in a mafia-type organisation, extortion, and unlawful control of economic activities. However, the arrest of individual actors was not sufficient to disrupt the system, which tended to regenerate through established networks of relationships. This underscored the importance of financial and asset investigations, including seizures, as a primary tool in countering organised crime. They represented the most effective means of targeting the mechanisms of accumulation and redistribution of illicit resources, thereby dismantling the criminal network. In addition, the case also revealed **challenges**, including the formally legitimate nature of the activities involved, the indirect exercise of control, and the limited use of overt violence, all of which render such forms of infiltration less visible and more difficult to detect at an early stage.

4. Financial profile of the criminal network involved in Case India

Financial processes at the core of Case India

The financial analysis revealed a model of resource management based on three key concepts: cash economy, money laundering, and criminal financial governance. A first central element concerned the gambling sector's nature as a **cash-intensive** economy. Activities involving slot machines and, to a lesser extent, betting generated frequent, fragmented, and difficult-to-trace financial flows, particularly when organised through extensive networks of local businesses. This high-cash environment, characterised by numerous small daily transactions, created favourable conditions for criminal intervention. In Case India, the widespread presence of gaming machines across multiple establishments enabled continuous revenue streams, part of which could be diverted from official channels without visibly affecting business operations.

This cash-based dimension was closely intertwined with **money laundering** dynamics, understood not only as the concealment of illicit proceeds but also as the incorporation of legitimate resources into criminal circuits. In Case India, the funds originated not from illegal activities, but from regulated economic activities, such as authorised gambling, which were subsequently diverted into the clan's financial system. This hybrid model reflects an evolution in laundering practices: rather than merely 'cleaning' illicit funds, the organisation appropriates legal financial flows for criminal purposes. Consequently, the boundary between legal and illegal economies becomes increasingly blurred.

[83] Efforts to counter these phenomena were constrained by the limitations of **international cooperation mechanisms**. Procedures such as mutual legal assistance and European Investigation Orders, and European Arrest Warrants remained procedurally complex and resource-intensive, requiring coordination, translation, and reconciliation of differing legal frameworks. These mechanisms continued to hinder the timeliness and effectiveness of investigations.

Although businesses formally comply with regulatory frameworks, part of their revenues is systematically extracted and redistributed through informal channels. This mechanism constitutes a form of '**economic parasitism**', whereby organised crime embeds itself within existing financial flows without visibly altering their structure.

Criminal financial governance emerged as another key dimension of the analysis, referring to the mechanisms through which the organisation managed, controlled, and redistributed economic resources. Financial flows were largely centralised within the so-called 'clan fund' (in Italian: *cassa del clan*), which functioned as the core decision-making centre for resource allocation. Revenues generated through commercial activities were pooled and redistributed according to hierarchical and strategic priorities. This redistribution fulfilled a stabilising function by financing members and supporting detained individuals and their families, thereby reinforcing organisational cohesion and loyalty while reducing the risk of defection. The system combined decentralised revenue generation through extensive business networks with centralised financial control at the top of the organisation.

The increasing **digitalisation** of the gambling sector introduced additional complexity. The integration of online platforms expanded opportunities for financial management, offering channels with greater opacity and reduced traceability. Through centralised control of accounts and credentials, the criminal network exercised indirect control over digital financial flows, extending its operations beyond traditional territorial boundaries. This evolution reflected a process of financial hybridisation, in which traditional instruments (i.e., cash and territorial relations) coexisted with digital tools (i.e. online platforms and remote management), thereby enhancing the system's resilience.

Financing sources and start-up capital

In terms of financing sources and start-up capital, the gambling sector requires relatively low initial investments. In the case of slot machines, production and leasing are typically conducted by private operators who enter into a symbiotic relationship with the criminal organisation. Start-up capital is therefore **provided by entrepreneurs** already active in the sector, rather than by the clan itself. Although illicit funds may occasionally be introduced, they are not essential to the system's functioning. Unlike other criminal markets, such as drug trafficking, entry does not require substantial upfront investment. In most cases, Case India being an exception, no company can be directly attributed to the clan. Instead, the organisation embeds itself within pre-existing businesses. Where *ad hoc* companies are established, as in Case India, higher investment is required, though the sums involved remain relatively limited. Manufacturers of gaming machines bear the principal costs but depend on the criminal organisation for territorial distribution, in return obtaining a significant competitive advantage through exclusivity.

Payment methods and arrangements within the network

In this sector, the mafia structure is not strictly hierarchical. The Camorra generally intervened indirectly, extracting profits from those who effectively controlled the activity. Payments were predominantly made **in cash**, particularly at lower operational levels, where the use of cryptocurrencies remained limited due to insufficient knowledge or access among those involved. Cryptocurrencies were used, if at all, only for larger-scale transactions.

Revenues and proceeds

Proceeds generally flowed into a common pool from which salaries were paid and further activities were financed, including other illicit operations (e.g., drug purchases) and investments in the legal economy, or the provision of funds to complicit entrepreneurs for investments such as in the construction sector. Resources were redistributed across multiple levels and reinvested in both criminal and semi-legal activities. Payment arrangements between the organisation and individuals varied according to roles and functions. Some individuals operated abroad to establish companies and were remunerated for this work. Others were responsible for opening prepaid cards under nominee names, receiving a fixed fee (e.g., approximately EUR 100 per activated card).

5. Harms caused by Case India

Harms to individuals

Case India highlights a significant restriction of individual economic freedom, as business operators are often compelled to accept imposed conditions under threat. Moreover, the widespread presence of gambling activities, combined with criminal control, exacerbates social vulnerabilities. In particular, it increases the risk of gambling addiction and exposes economically fragile groups to further financial harm. Furthermore, the economic system managed by the clan contributes to the intergenerational reproduction of criminal dynamics. Beyond generating income, it consolidates social relationships and behavioural patterns that sustain the organisation over time.

Harms to other businesses

From an economic perspective, Case India demonstrates a significant distortion of market functioning. The criminal network undermines competitive dynamics by creating barriers to entry through coercion and territorial control, resulting in imposed local monopolies in which the selection of operators is based not on efficiency or competitiveness, but on ties to the criminal organisation. Moreover, mandatory payments imposed on operators, such as monthly fees for the management of slot machines, systematically extract value from the legitimate economy in favour of the criminal organisation. This reduces the investment capacity of legitimate businesses and weakens the local entrepreneurial fabric. At the same time, these practices can reduce tax revenues, as significant financial flows are diverted into informal or illegal circuits and thus evade fiscal oversight.

Harms to public institutions

Case India clearly illustrates a form of illegal governance in which the criminal organisation performs functions typically associated with public institutions, such as regulating market access, resolving disputes among operators, and allocating economic opportunities. The criminal network thereby acts as a parallel regulatory authority, imposing rules and enforcing them through intimidation. Consequently, the State's regulatory capacity and trust in public institutions are weakened, while legal and criminal forms of governance increasingly overlap. This also poses significant challenges to effective law enforcement in contexts characterised by high levels of infiltration. Moreover, when mafia control over the territory gains social recognition, criminal and institutional governance may coexist. This undermines the legitimacy of the State and limits the capacity of public authorities to intervene effectively.

Harms to the physical environment

Although the environment effects are indirect, Case India highlights a transformation of urban and commercial space. The widespread presence of gambling activities contributes to a form of economic monoculture, reducing the diversity of local economic activities and negatively affecting the quality of public space. Relevant territorial indicators include a high density of gambling venues in socially vulnerable areas, reduced commercial diversity, and a negative perception of the urban environment.

Annex 3.J – Case Juliett: Agri-Food Routes to Crime

1. Criminal network involved in Case Juliett

The criminal network involved in Case Juliett was **linked to the Casalesi clan**, particularly to the Schiavone faction, one of the most prominent branches of the Camorra operating in the areas of Casal di Principe and San Marcellino. This hierarchically structured mafia-type organisation was characterised by a strong capacity to infiltrate the legitimate economy and by an established presence at both national and interregional levels. Owing to the clan's historical links to the exploitation of agricultural land, it developed sector-specific expertise and an extensive network of contacts. In total, 73 individuals were identified in connection with the case, with the core members presented in Table 15.

The network exhibited a clearly defined **hierarchical structure**, enabling efficient and resilient operations. Leading clan members, including C1_J and brothers C3_J, C4_J, and C5_J, exercised strategic and directive functions. Mid-level actors were responsible for administrative and business management. Notably, C6_J played a central role in managing LTD1_J and coordinating logistics operations. The organisation also relied on nominees and frontmen to conceal beneficial ownership of affiliated companies. Moreover, territorial coordinators managed operations across specific geographical areas, such as Campania, Lazio, and Sicily. The network further depended on specialised actors, including weapons suppliers and technical experts, supported by auxiliary personnel facilitating on-the-ground activities, notably a broad base of drivers and operational executors.[84]

Table 15

Overview of the core members of the criminal network involved in Case Juliett (Caserta)

Member	Role	Gender	Born between
C1_J	Leader; Coordinator; Control over criminal operations	Male	1934-1953
C2_J	Leader; Coordinator; Contribution to the management of the mafia organisation	Male	1974-1993
C3_J	Leader; Coordinator; Participation in the management of the mafia organisation	Male	1934-1953
C4_J	Leader; Coordinator; Involvement in management and organisational activities	Male	1954-1973
C5_J	Leader; Coordinator; Contribution to strategic guidance of organisation	Male	1974-1993
C6_J	Logistics coordinator; Liaison with contacts in Sicilian markets	Male	1954-1973
C7_J	Logistics coordinator; Operational management; Organisation of transport network	Male	1934-1953
C8_J	Manager of transport operations (to Sicily)	Male	1954-1973
C9_J	Manager of fruit and vegetable market in Fondi	Male	1954-1973
C10_J	Financial manager; Management of LTD2_J	Female	1974-1993
C11_J	Armourer; Storage and supply of weapons	Male	1934-1953
C12_J	External aiding and abetting; Participation in intimidation and control	Male	1954-1973
C13_J	Leader of the Quindici clan; Provision of territorial control	Male	1954-1973
C14_J	Senior mafia figure; Provision of intimidating force and criminal legitimacy	Male	1954-1973
C15_J	Senior mafia figure; Co-leader of the association; Control of illicit activities in transport sector	Male	1954-1973
C16_J	Senior clan leader (Mallardo clan); Provision of intimidating force	Male	1954-1973
C17_J	Senior clan leader; Participation in the management of territorial control	Male	1954-1973
C18_J	Senior clan leader (Mallardo clan); Contribution to enforcement of monopolistic rules	Male	1954-1973

A distinctive feature of the criminal network was its **inter-organisational dimension**, grounded in stable cooperative arrangements with other mafia groups. The Casalesi clan entered into agreements with other Camorra groups operating in the Campania Region, including the Licciardi and Mallardo clans, as well as with Sicilian mafia organisations active in key fruit and vegetable markets on the island. These arrangements enabled the network's extension of control across the agri-food supply chain, facilitating the coordination of flows between Campania and Sicily and securing market access through systems of authorisation and financial remuneration. The network also demonstrated a high degree of adaptability and **temporal continuity**. Criminal activities in the fruit and vegetable transport sector have persisted over several years, despite law enforcement interventions and arrests, through the reorganisation of structures, replacement of personnel, and modification of corporate arrangements within the companies involved. This resilience was reinforced by a strong culture of internal secrecy, which restricted information flows and mitigated the risk of cooperation with law enforcement authorities.

The Schavione faction was involved in various **criminal activities**. These included the monopolistic control of key economic sectors as horticultural haulage, public procurement, and food distribution, as well as the systematic extortion of businesses, contractors, and traders. Its activities further encompassed the trafficking of military-grade weapons (via C11_J through Bosnia), fraudulent asset registration, and money laundering. The group also engaged in systematic violence and intimidation against competitors, including shootings, assaults, and threats, alongside electoral manipulation, corruption of public officials, and drug trafficking via horticultural transport routes.

2. Legitimate businesses involved in Case Juliett

An analysis of the judicial files related to Case Juliett revealed the involvement of two legally registered companies (LTD1_J and LTD2_J) operating in the Campania Region that were directly linked to members of the criminal network. **LTD1_J** was a road haulage company specialising in the refrigerated transport of fresh fruit and vegetables by lorry to and from the main wholesale horticultural markets in Central and Southern Italy and Sicily. LTD1_J's main headquarters were located in the Province of Caserta, where a yard comprising offices and warehouses served as the logistical hub. The premises were also identified as a storage and distribution site for military-grade weapons. A key local unit was based in Fondi (Lazio Province), providing direct access to the Fondi market. Its commercial reach extended across a **broad geographic area**, covering multiple wholesale markets in Campania, Salerno, Sicily, and Abruzzo, as well as transport routes into North-West Italy.

In December 2008, the company was converted from a general partnership (in Italian: *società in nome collettivo*) into a cooperative (In Italian: *società cooperativa a responsabilità limitata*).[85] It operated in close connection with an affiliated subsidiary, **LTD2_J**, which managed distribution routes from Fondi to North-West Italy. LTD1_J operated a fleet of lorries and articulated vehicles, supported by a network

[85] Under Italian law, a *società in nome collettivo* is an unincorporated partnership in which all partners bear unlimited and joint personal liability for the company's debts, allowing creditors to pursue the personal assets of any partner. A *società cooperativa a responsabilità limitata*, by contrast, is a fully incorporated legal entity governed by cooperative law. Members' liability is limited to their subscribed share, thereby shielding personal assets from company debts. Cooperative structures typically feature a broader and more fluid membership base, with shares that may be held by multiple members and transferred or restructured more easily than in a general partnership. The governance framework, including a 'one member, one vote' principle rather than voting rights proportional to capital, makes it more difficult for external investigators to identify ultimate control, as formal voting rights do not necessarily correspond to underlying economic interests.

of satellite companies and affiliated sole-trader firms, which facilitated transport operations and extended coverage across multiple routes. The company presented itself as a legitimate, duly registered transport operator. Its annual revenues were not precisely quantifiable based on available judicial documentation, as the formal accounts were systematically used as a concealment mechanism. The shareholding structure was restructured on multiple occasions (in 2003, 2005, and 2008) to conceal the identity of ultimate beneficial owners and circumvent asset-freeing measures. Formal ownership was attributed to a series of **nominees**, which masked the involvement of senior figures of the Casalesi clan, including C1_J, C3_J, and C4_J.

From an operational perspective, LTD1_J operated in an economic environment characterised by a strong demand for logistics services for perishable goods, requiring speed, continuity, and reliability in delivery. In this context, the company functioned as a significant **transport operator**, facilitating links between producers, wholesale markets, and distributors. It operated on strategic routes and, in certain cases, emerged as one of the principal providers on specific transport routes, thereby increasing its relevance within the sector. Operational activities were not limited to the direct management of vehicles but also relied on the coordination of a network of external transporters. LTD1_J acted as an intermediary structure, engaging small independent hauliers who were assigned individual transport routes, thereby extending its operational capacity.

3. Crime script based on Case Juliett

Motivation – Purpose

The Schavione faction of the Casalesi clan used LTD1_J to pursue a **dual objective**. On the one hand, it facilitated the laundering and reinvestment of proceeds derived from the clan's criminal activities, including extortion, public procurement fraud, and drug trafficking. Moreover, evidence indicated that money laundering activities and nominee ownership were used to conceal the true ownership of the business. On the other hand, it served to consolidate monopolistic control over the strategic agri-food transport sector. This control was exercised through a system of informal authorisations that rendered access to the market contingent on the clan's approval, effectively positioning the organisation as a *de facto* regulatory actor within the sector. LTD1_J functioned as an instrument through which the clan exerted its intimidating power and consolidated economic control over the territory, including through extortion and violence aimed at eliminating competitors.

Preparation

The network involved in Case Juliett exploited companies operating in the **fruit and vegetable transport** subsector in Campania, within the broader logistics and agri-food industries, both of which are central to the regional economy. According to recent statistics, approximately 1,471 companies were active in the road freight transport sector in Campania in 2025, placing the region among the leading areas in Italy in terms of the number of operators in this field (Unioncamere & InfoCamere, 2025). The sector is also closely linked to the agri-food supply chain, which represented one of the pillars of the Campanian economy. Data indicated the presence of approximately 79,000 active agricultural holdings in Campania, with a strong specialisation in fruit and vegetable production (ISTAT, 2024). This production base fed into a complex logistics system that required intensive road transport activity to ensure the distribution of goods to national and European markets.

However, the characteristics of the sector contribute to its significant exposure to the risk of criminal infiltration of the legitimate economy. In the fruit and vegetable transport sector, the **perishable nature** of the products requires very tight delivery times, creating strong pressure on economic operators. This makes transport operators and producers more likely to accept imposed conditions in order to avoid the loss of goods, thereby reducing their capacity to resist external pressure by organised crime groups. In addition, road transport is characterised by relatively low barriers to entry and a **high number of vehicles** in circulation; factors that make systematic and effective monitoring by the authorities complex. This difficulty of control, combined with the need to ensure rapid distribution, also renders the sector suitable for the transport of illicit goods, such as weapons and drugs, concealed with agri-food shipments. Furthermore, the sector is characterised by limited traceability of financial flows, where payments can also be made in cash and business relations are often based on trust, thereby facilitating money laundering and the informal management of proceeds.

Another key opportunity stems from the **centrality of wholesale markets**, such as the Fondi market, which represent crucial logistical hubs for product distribution at both national and European levels. Control over such hubs makes it possible to influence large-scale commercial flows and affect the entire agri-food supply chain. This is further reinforced by the **fragmented nature** of the sector, characterised by the presence of numerous small operators who are more exposed to intimidation and lack the economic capacity to resist external pressure.

In addition to these sector-specific vulnerabilities, LTD1_J also exhibited several characteristics that made it suitable for criminal infiltration. First, its **legal form** and corporate structure allowed a degree of flexibility in management and in changes to ownership arrangements, enabling frequent transfers of shares and the use of nominees to conceal the true ownership. Moreover, road transport activity provided a **plausible legal cover** for the movement of goods, making it more difficult to distinguish between legitimate and illicit activities.

Pre-activity or enabling conditions

The *modus operandi* underlying the criminal use of the companies developed through a series of coordinated phases and mechanisms. First, the clan established or acquired the corporate structure and formally registered it under the names of nominees in order to conceal the true ownership. The organisation subsequently imposed **control over the market** through intimidation, eliminating competitors by means of threats, assaults, and violent acts. Once a dominant position had been consolidated, the company was used to systematically manage transport flows, impose economic conditions, and determine which operators were authorised to operate. At the same time, the system relied on **agreements with other criminal organisations**, including Sicilian mafia groups, in order to extend control along the principal commercial routes. The company also served as a cover for additional illicit activities, including the transport of weapons and, potentially, drugs, exploiting the apparently legitimate nature of agri-food transport.

In Case Juliett, the degree of criminal use was total: LTD1_J did not merely constitute an infiltrated enterprise, but rather a structure established and directly managed by the Casalesi clan for illicit purposes. The legitimate economic activity was therefore subordinated to the **criminal interests** of the organisation, effectively operating as a mafia enterprise within the lawful economy. The use of the corporate structure was systematic and extended across all phases of activity, from the operational management of transport to the reinvestment of illicit proceeds.

The level of **culpability** of the individuals involved varied according to their role within the organisation. At the highest levels, responsibility was complete, as clan leaders and company managers were fully aware of the illicit nature of the activities and directed the organisation's strategies. At an intermediate level were individuals who knowingly participated in operational management, even though they did not formally belong to the upper ranks of the mafia organisation. At the base of the structure were drivers and collaborators whose involvement may have been more limited, at times confined to the execution of tasks, although they operated within a context clearly shaped by criminal influence.

Activity

In Case Juliett, the Casalesi established a *de facto* monopoly over the transport of fruit and vegetable products from Southern Italy to the Fondi wholesale market. The *modus operandi* centred on the **control of transport operations** linked to this market. Any operator wishing to load or unload goods at the market was required to operate through an intermediary structure, formally presented as the transport company LTD1_J, which in practice functioned as a placement agency. This structure determined which operators were permitted to carry out transport activities and under which economic conditions. The company itself did not maintain a particularly large fleet of vehicles but instead relied on a network of small independent hauliers engaged on a case-by-case basis for specific routes (e.g., the transport of a designated number of pallets in exchange for a fixed payment). These operators were fully aware that prior authorisation from the criminal organisation was required in order to operate.

A further key mechanism involved **relations with Sicilian criminal groups**. Initially, a company from Giugliano (located in the Campania Region) operated independently in the transport of goods between Sicily and the Fondi market. Once the Casalesi recognised the economic significance of this sector, they sought to exclude the operator and assume control of the Sicilian markets (i.e., Vittoria, Catania, Palermo). The competing company was forcibly driven out, with its trucks prevented from operating. This triggered violent reactions, including armed clashes and arson attacks between rival groups. In this context, the Casalesi imposed a strict rule: goods destined for the Campanian market, particularly the Fondi market, could only be transported by **clan-authorised operators**. Unauthorised transporters were denied permission to unload their goods. The situation was subsequently stabilised through a direct agreement between the Casalesi and Sicilian criminal organisations, particularly those linked to the Corleonesi.

Following these agreements, road transport to and from the Fondi market, originating from all of Southern Italy and Sicily, was placed exclusively under operators linked to the Casalesi (LTD1_J) or authorised vehicles. The system proved economically highly efficient, as transporters operated circular routes to ensure that trucks travelled fully loaded in both directions. In practice, the same vehicle transported goods from Campania (or other areas, such as Spain) to Sicily, unloaded them in local markets (i.e., Vittoria, Catania, Palermo), and then reloaded goods destined for Fondi. This model reduced transport costs by op to 50% and enabled the Casalesi to eliminate competitors unable to match this efficiency. These arrangements were founded on **mutual benefit**: the Casalesi guaranteed access to the Fondi and Campanian markets for Sicilian products, while Sicilian groups granted access to their local markets for Campanian goods, all transported by carriers linked to the Casalesi clan.

Another central mechanism concerned **control over producers' remuneration**. In Sicily, as in the Caserta area, farmers understood that without transporters linked to the clans, their goods would never reach the markets. Given the perishable nature of the products, this effectively meant losing the entire harvest. Producers were therefore compelled to comply with the system, lacking any viable alternative route to the market. This mechanism also enabled criminal organisations to exert direct influence over price setting. Wiretaps in Sicily revealed that mafia actors imposed highly unfavourable conditions on producers, stating that certain goods, such as melons, would only be sold on their terms and at prices too low to ensure farmers' economic survival.

Finally, road transport also served as a **conduit for illicit activities**, including the trafficking of weapons, drugs, and counterfeit goods concealed with agri-food consignments. The high volume of traffic and the requirement for rapid distribution complicated effective controls. The investigation established that vehicles were used to transport weapons, including Kalashnikov rifles, to Sicily, as well as drugs handled by Campanian criminal groups. Investigations further revealed that major Campanian criminal organisations operated their own transport companies with the agri-food sector, underscoring the strategic importance of this segment.

Post-activity or post conditions

In Case Juliett, legitimate companies were used for criminal purposes over a prolonged period, estimated at around nine years (2000-2009), with activities still ongoing when the investigations began. With regard to **indicators of infiltration**, a typical pattern emerged. The competitor company, based in Giugliano (Campania), operated successfully in the transport of fruit and vegetable products along the Campania-Sicily route. At its peak, it handled more than sixty trucks per shipment to Sicily, effectively holding a near-monopolistic position in the sector. Once the Casalesi recognised the profitability of this market, they sought to take control, imposing compliance with its system or exclusion from legitimate businesses. This triggered a violent conflict between the two entities, resulting in shootings and reciprocal acts of intimidation.

Over time, the competitor company was weakened and ultimately forced to relinquish control of the market. In an attempt to maintain his position, the entrepreneurs sought protection from the Mallardo clan, agreeing to cede approximately 50% of profits in return. The Mallardo clan, itself linked to other organised criminal groups such as the Bidognetti clan, secured control of the Giugliano area for competitors, while the Casalesi assumed full control of the Fondi-Sicily transport route. This case

represented one of the first judicially established examples of an agreement between highly structured criminal organisations, particularly between the Casalesi clan and groups linked to the Corleonesi.

Ultimately, the system was uncovered by the authorities at the execution stage of the criminal activity, following violent incidents that exposed the conflict between the groups involved. In particular, the investigation was initiated through telephone interceptions authorised after a series of shootings and arson attacks between LTD1_J and a competitor. Unusually for this type of case, the **investigation** did not originate from informant testimony but from these high-profile incidents, which drew investigative attention. The financial investigation relied on telephone and environmental interceptions, video surveillance, company registry analysis, examination of bank accounts and cash flows, statements by cooperating witnesses, and parallel asset-prevention proceedings. Confiscation measures ordered during the proceedings concerned company shares, business assets, vehicles, bank accounts, and real estate linked to LTD1_J, as well as other businesses and individuals associated with the organisation.

4. Financial profile of the criminal network involved in Case Juliett

Financing sources and start-up capital

The network's start-up capital derived from the illegal proceeds of the Casalesi clan, in particular the Schiavone faction, including extortion, drug trafficking, fraudulent public contracts, usury, and monopolised food distribution in the milk, butter, and coffee sectors.

Payment methods and arrangements within the network

The network employed multiple payment methods. Cash was used for monthly salaries to affiliates, commissions to mafia intermediaries, and informal payments. Bank cheques and transfers were used to manage commercial relations and invoices, maintaining a façade of legitimacy. Weapons were also used as a form of payment or compensation. In one documented case, a Kalashnikov and a revolver were exchanged for gatekeeping activities at the Bracigliano market. The transport system further generated commissions linked to haulage activities, amounting to approximately EUR 5 per pallet on minor routes, with variable percentage rates on larger routes.

The organisation operated through a system of monthly **'wages'** for affiliates. Drivers and low-ranking members received approximately EUR 1,000 to EUR 2,000 per month, while senior figures and leaders received approximately EUR 4,000 to EUR 5,000. Judicial proceedings documented a clan common fund with an estimated annual flow of EUR 3 million to EUR 4 million allocated solely to salaries. Additional periodic commissions were paid to Campanian and Sicilian mafia intermediaries, calculated as a percentage of revenues from transport routes under their control. Company profits were formally distributed to nominees but wee in practice retained by concealed shareholders linked to the clan through fiduciary arrangements.

Costs of business operations

The network's operational costs included standard business expenses such as vehicle maintenance, fuel, driver salaries, lorry hire, and market logistics. Illicit costs included commissions to local mafia intermediaries in exchange for market access, contributions to the clan's common fund, the purchase and maintenance of military-grade weapons, payments for intimidatory and violent acts, legal defence costs for multiple defendants, and expenses associated with repeated corporate restructuring to evade asset seizure.

Revenues and proceeds

The extraction and laundering of money occurred through multiple mechanisms, including fictitious profit distributions to nominees subsequently transferred to concealed shareholders, inflated or fictitious company expenses, payments for non-existent consultancy services, and the use of company accounts for the personal expenses of the leadership. Criminal proceeds were reinvested through the expansion of the transport fleet, the establishment of additional companies, the acquisition of real estate and luxury vehicles, and fraudulent asset registration. The proceedings also documented the creation of further companies under different nominal shareholders.

5. Harms caused by Case Juliett

Harms to individuals

Case Juliett documents numerous instances of direct violence and intimidation. Victims were subjected to slaps, punches, baton strikes, threats involving firearms, and explicit death threats, including threats of being dissolved in acid. In one documented episode, occurring within the Fondi wholesale market area, a transport operator was shot and wounded. Other operators and drivers were physically assaulted in market yards to enforce compliance with the transport system controlled by the organisation. In addition to physical violence, traders and transporters suffered significant economic harm, as they were forced to operate under disadvantageous conditions or risked losing their goods entirely. These forms of harm were compounded by substantial psychological effects, particularly a pervasive climate of fear and subjugation that limited the ability of operators to resist or report incidents.

Harms to other businesses

The harm to other businesses is equally significant, primarily taking the form of distorted competition. The imposition of a *de facto* monopoly forcibly excluded numerous legitimate operators from the market. Competing companies were left unable to operate on equal terms, regardless of their efficiency or competitiveness.

Harms to public institutions

Case Juliett caused significant economic and reputational harm. In particular, the Fondi wholesale fruit and vegetable market, one of the sector's main public infrastructures, was influenced by criminal dynamics for years, undermining both its functioning and public image. Trade associations and organisations involved in combating extortion were also indirectly affected, operating within a highly compromised environment. Furthermore, Case Juliett highlights instances of collusion involving individuals linked to public institutions, including law enforcement officers, which further strengthened the capacity of the criminal network.

Harms to the social environment

At the social level, the clan's activities contributed to entrenching a system of relations based on silence, subjugation, and the normalisation of illegal practices.

ANNEX 4

FRANKFURT

DETAILED CASE STUDIES

Annex 4.K – Case Kilo: The Corrupt Cargo Chain

1. Criminal network involved in Case Kilo

The network involved in Case Kilo comprised **two components**. The first consisted of low-level employees of an international logistics company who facilitated the movement of drug shipments arriving from outside the EU through Frankfurt Airport. The airport handles an annual cargo volume of nearly two million tonnes and supports the operations of approximately 250 logistics companies (Frankfurt Airport, n.d.). The second network component was involved in the local distribution of these drugs in a rural part of the Rhine-Main area. The two components were connected by a central actor who initially recruited one employee of the logistics company, who subsequently recruited at least two colleagues. Both components displayed some degree of horizontal differentiation. Within the logistics company, employees occupied different positions, providing them with varying levels of access to information and facilities that, collectively, enabled the manipulation of internal processes and the circumvention of controls and monitoring. Within the distribution component, network members performed distinct logistical roles, including courier and storage functions.

2. Legitimate businesses involved in Case Kilo

For confidentiality reasons, the identity of the infiltrated logistics company was not disclosed during the interviews, and no information enabling its identification was provided. The available information indicates only that the company was a **major international logistics provider** (LTD1_K) involved in the handling of cargo arriving in Germany and entering the European market. The logistics sector is one of the most important economic sectors in both Frankfurt and the state of Hesse, employing approximately 225,000 people across the state (HMWVW, n.d.).

3. Crime script based on Case Kilo

Motivation – Purpose

The purpose of the infiltration was to establish an **airfreight supply route** for the transportation of illicit drugs. More specifically, infiltrating the international logistics company (LTD1_K) enabled the criminal network to facilitate the secure handling of drug consignments at their point of entry into the EU.

Preparation

The drug smuggling operation associated with the network in Case Kilo was embedded within international trade, with illicit drugs transported in cover loads of legitimate goods. The infiltrated company (LTD1_K) functioned as a central node in the handling of cargo arriving at Frankfurt Airport. The opportunities exploited by the network to infiltrate this company were inherent in the structure and functioning of the international transport and logistics sector. The **integration of illicit drugs** into consignments of legitimate goods appears to represent one of the most cost-efficient methods of sustaining the transport of drugs from source countries in Latin America, North Africa, and Asia to major consumer markets in North America and Europe. Moreover, a key vulnerability exploited by the network was the comparatively **low remuneration** of lower-level employees in the logistics sector. Consequently, these employees were reportedly susceptible to recruitment through substantial financial incentives, with payments offered per shipment of up to approximately 50% of their annual legitimate income (Degen, 2026a).

Pre-activity or enabling conditions[86]

The available information indicates that the criminal use of the legitimate logistics company comprised **three broad phases**: the recruitment of business insiders through existing social contacts; the manipulation of internal processes by these insiders to facilitate the handling of individual drug consignments concealed within legitimate cargo; and the extraction of the illicit drugs from the logistics company through the unauthorised use of the identities of other legitimate businesses. Within this process, internal business operations were manipulated to the extent necessary to enable the removal of illicit drugs from consignments. This included influencing the routing and handling of cargo within the premises of Frankfurt Airport, as well as controlling access to specific storage and processing facilities at particular times. Notably, neither higher-level staff nor the company's management were involved in the smuggling operation. Rather, the company became an unwitting victim of criminal infiltration facilitated through the **corruption of lower-level employees**.

Activity

The recruited business insiders were directed by objectives and incentives established by the key figure within the criminal network, while the specific *modus operandi* for exploiting the logistics company were developed autonomously by the insiders themselves. The key offender within the network informed the business insiders of incoming drug shipments. The insiders subsequently used their access to specific components of the company's IT infrastructure, internal processes, and operational premises to redirect these consignments within the logistics system, thereby facilitating the eventual **retrieval of the illicit drugs**. This was achieved under the guise of routine outgoing shipments conducted using the identities of legitimate businesses.

Post-activity or post conditions

The logistics company (LTD1_K) appears to have been used for drug smuggling over a period of several months. In the course of extracting illicit drugs from legitimate consignments, the core business processes of the logistics company appear to have remained largely unaffected. Internal processes were manipulated only to the extent necessary to facilitate the removal of the drugs, while avoiding detection or triggering internal controls. This may also explain the absence of any indications that pressure was exerted on the logistics company or on members of management and staff who were not recruited by the network.

It remains unclear what led the authorities to identify the network and which **investigative measures** were undertaken in response. During the interviews, no information was provided on this matter due to security concerns. However, in the course of legal proceedings against several members of the network, information became publicly available suggesting that a van used to collect illicit drugs from the logistics company had previously been placed under surveillance as part of a separate investigation (Degen, 2026b).

[86] Only very limited information was provided during the interviews regarding the offenders' *modus operandi* within the logistics company. This level of secrecy was reportedly maintained to prevent the transfer of criminal know-how.

4. Financial profile of the criminal network involved in Case Kilo

No detailed information regarding the financial structure and activities of the criminal network was obtained during the interviews. It was only briefly indicated that cross-border **cash transactions** played an important role in remunerating suppliers, and that cash payments were also made to network members, including those operating within the logistics company.

5. Harms caused by Case Kilo

Harms to individuals

According to the interviews, the negative consequences were borne primarily by business insiders who allowed themselves to be recruited into the smuggling operation. In addition to facing criminal charges, they lost their jobs immediately and had their security clearances revoked, which barred them from future employment in security-sensitive sectors.

Harms to other businesses

In contrast, LTD1_K was not found to have incurred any harm. It faced no legal repercussions, as it reportedly had complied with all pertinent legal obligations, including those relating to personnel training. Nor did it experience business disruptions resulting from criminal activities or measures taken by the authorities. Importantly, the company did not suffer any reputational damage, as the authorities did not disclose its identity to the public as a matter of policy. Furthermore, there was no indication that other businesses, such as those whose names were used as part of the *modus operandi* or those competing with LTD1_K, were tangibly affected.

Annex 4.L – Case Lima: Hidden Hubs, Hidden Hauls

1. Criminal network involved in Case Lima

An estimated fifteen individuals were involved in the network associated with Case Lima, including persons residing in different locations along the transport routes across Europe. One **central figure** within the network coordinated the activities of members who occupied distinct roles within a division of labour, including money couriers, drug couriers, and storekeepers.

2. Legitimate businesses involved in Case Lima

The logistics business used in the scheme of Case Lima was a small, economically insignificant limited-liability company (LTD1_L) employing only a few individuals. The company operated short-term **storage facilities** to legitimate businesses for a diverse range of goods, including a large warehouse. Its premises were centrally located within the Rhine-Main metropolitan region, providing quick access to an interstate highway. Available information indicates that the business had experienced financial difficulties prior to its infiltration by the criminal network.

3. Crime script based on Case Lima

Motivation – Purpose

The infiltration of the logistics company was linked to drug trafficking within the EU and centred on the establishment of a **distribution hub** for the Rhine-Main region. To this end, the network required a suitable location where drug consignments could be received, stored, and reorganised for further distribution without raising suspicion. This was facilitated by integrating the unloading, storage, and onward loading of illicit drugs into the day-to-day operations of the logistics company.

Preparation

The logistics company (LTD1_L) appeared **suitable** for the purposes of the criminal network for three main reasons. First, it could function as an inconspicuous delivery location for consignments outsourced to legitimate haulage companies for transportation, whose employees and drivers were reportedly unaware of the true nature of the shipments. Second, the handling of drug consignments could be integrated into the routine activities and day-to-day operations at the company's premises. Third, due to the company's small size, the criminal network only needed to recruit two individuals – the manager and a warehouse employee – to gain operational control over the business. This process appears to have been facilitated by the financial difficulties the company was experiencing at the time.

Furthermore, the opportunities exploited by the criminal network to infiltrate the logistics company were inherent in the structure and functioning of the international **transport and logistics sector**. The use of this sector as part of the illicit drug supply chain, in this case for the bulk transportation of drugs by road within the EU, appeared to provide criminal networks with a relatively safe and cost-efficient method of operation.

Pre-activity or enabling conditions

The logistics company essentially provided the same types of services to the criminal network as it did to its legitimate customers through the provision of facilities for the handling and storage of goods. However, the criminal network exercised a greater degree of direct control over the company, as it was able to issue instructions that the manager and warehouse worker followed without question. Both the manager and warehouse worker were willing participants in the trafficking operation. They agreed to cooperate with the network in exchange for financial compensation.

The *modus operandi* involving the criminal use of the legitimate logistics company (LTD1_L) comprised **two phases**. First, business insiders, including the manager, were recruited through existing social network contacts. It appears that the manager of the company operated within the same broader social circles as members of the criminal network. Notably, by recruiting only the manager and the warehouse worker, the network was able to bypass an intermediate-level employee. Subsequently, the company was used to process large incoming drug consignments for further distribution within the Rhine-Main region. This involved the logistics company being consistently listed on the freight documentation accompanying the shipments. No detailed information was provided regarding the specific procedures through which the drug consignments were handled at the logistics company.

Activity

Network members contracted legitimate hauling companies to transport cover loads containing illicit drugs from within the European Union to the logistics company in the Rhine-Main region. Upon arrival, the cargo was unloaded and either handed over to drug couriers or placed in storage, from where the drugs were subsequently collected for further distribution. The logistics company (LTD1_L) was subject to criminal management through directives issued by the network. However, the instructions given to the manager and warehouse worker, apparently, were limited to matters directly relevant to the successful handling and processing of the drug consignments.

Post-activity or post conditions

There was reportedly nothing about the use of the logistics company for drug trafficking that would have raised suspicion. The activities associated with the handling of the drug consignments remained inconspicuous amid the regular movement of people and vehicles at the company's premises. No specific information was provided regarding the lifespan of the network or the duration of the criminal use. Moreover, it remains unclear what led the authorities to identify the network and which investigative measures were undertaken.

4. Financial profile of the criminal network involved in Case Lima

No detailed information regarding the financial aspects of the criminal network was obtained during the interviews. In particular, no estimates were provided concerning the revenues generated by the network. However, it was indicated that substantial profits had been accumulated and subsequently invested in valuables, real estate, and cryptocurrencies. These assets included high-value vehicles, boats, and yachts. No information was available regarding the use of hawala banking.

5. Harms caused by Case Lima

LTD1_L was temporarily closed following the arrest of its manager but subsequently resumed operations, while the manager was imprisoned. There is no indication that other businesses, particularly competitors, were negatively affected by the criminal use. Moreover, it remains unclear whether any payments were made to the company beyond those received by the manager and the warehouse worker. These payments were considered relatively low compared with those associated with other drug-trafficking networks and were described as 'pocket money'.

Annex 4.M – Case Mike: Dining with Dealers

1. Criminal network involved in Case Mike

The criminal network involved in Case Mike comprised a core group of approximately ten individuals, most of whom were connected through **family ties**. The network members linked by family relationships formed part of a broader clan structure originating in South-Eastern Europe and extending across several European countries. In addition, the network maintained connections with various criminal networks of different backgrounds in the Rhine-Main region and beyond, from which it could reportedly draw support.

Strategic decisions were made by **three central figures**, either individually or collectively. Within the network, there was a degree of task specialisation, with responsibilities divided according to specific drug types and geographical areas. Among the second-tier members of the core group, tasks were further allocated across various functions, including bookkeeping, storage management, logistics, local drug distribution, and the management of the restaurant and bar.

2. Legitimate businesses involved in Case Mike

Most of the available information concerned the restaurant involved in the criminal scheme, whereas only limited information was obtained about the bar. Consequently, the analysis presented here focuses exclusively on the **restaurant**, a high-end establishment located in the city centre of Frankfurt. Situated in close proximity to the courthouse, the restaurant was frequented by judges, prosecutors, and lawyers.

3. Crime script based on Case Mike

Motivation – Purpose

According to the interview data, three principal motives can be identified for establishing the restaurant. First, it provided formal **employment** for several members of the criminal network, thereby creating a legitimate source of income, although only two of these members actually worked at the restaurant. Second, the restaurant served to enhance the social status and prestige of the network members. As one interviewee recalled, a leading member of the network reportedly stated that "they had not come to Germany for the money, but for the name of the family". This suggests that the restaurant was intended primarily as an instrument of **image-building**. This objective was pursued by maintaining a high-end establishment capable of attracting celebrities and other high-status individuals. Third, the restaurant appears to have been used to gather **intelligence** on, and establish relationships with, prosecutors and judges who regularly frequented the restaurant.

In this way, the restaurant was used as a means of **shielding** members of the criminal network from a range of **perceived threats**. For example, formal employment at the restaurant enabled one network member to obtain a more favourable legal status in Germany. Moreover, the appearance of economic success and social recognition may have contributed to an aura of respectability, thereby reducing suspicion regarding the legitimacy of the members' income.

Preparation

A restaurant had already been operating on the premises prior to the network's acquisition of the business. Apart from the use of illicit funds to finance the acquisition and subsequent refurbishment of the restaurant, no information was obtained regarding any specific opportunities exploited by the criminal network in entering the hospitality sector. More generally, there appear to be relatively few barriers to establishing a high-end restaurant in Germany, aside from the capital required to refurbish the premises and recruit suitably qualified staff.[87]

[87] The restaurant sector constitutes an important component of the local economy in Frankfurt. With more than 1,000 restaurants, Frankfurt ranks fourth among the cities in Germany in terms of the total number of restaurants and second in terms of the number of restaurants *per capita* (Listflix, n.d.).

Pre-activity or enabling conditions

The restaurant was owned, operated, and fully controlled by members of the criminal network through a limited-liability company that served as the corporate vehicle for both the restaurant and the bar. Three core members of the network were listed as shareholders, each holding an approximately equal ownership interest. These members had access to drug supplies that were managed by a core network member who also acted as a bookkeeper. It is unclear whether any particular opportunities were required for the network to establish the restaurant of this type at this location. However, one interviewee suggested that the decision to open the restaurant in close proximity to the courthouse formed part of an established strategy employed by the network.

Activity

The restaurant was used for **several criminal purposes**. First, it served as a meeting place for individuals involved in drug trafficking. Second, attempts were reportedly made to establish influence over prosecutors and judges, although there is no indication that these efforts were successful. Surveillance technology was installed in the restaurant, with the aim of gathering intelligence on members of the judiciary. In one instance, for example, an intercepted communication revealed that a network member expressed disappointment that a customer had turned out to be 'only' a well-known attorney rather than a judge. Third, fraudulent claims for government support were allegedly submitted during the COVID-19 pandemic.

Beyond these activities, however, no further links to organised criminal activity could be identified. In particular, the investigation did not uncover evidence that the restaurant had been used to launder criminal proceeds. Although it was established that illicit funds amounting to EUR 170,000 had been invested in the refurbishment of the restaurant, no evidence was found of a continuing inflow of drug proceeds into the business.

Post-activity or post conditions

The restaurant was operated by members of the network for a period of approximately three years. During this time, the restaurant operated at a financial deficit, partly due to the costs associated with no-show employment arrangements, resulting in the seizure of business accounts by creditors. At the same time, substantial amounts of money could be mobilised whenever there was an imminent risk of the businesses being closed down, for example by the tax authorities. Funds were also available when the network needed to demonstrate its wealth, such as by hosting visitors in luxury hotels. Overall, there was a clear discrepancy between the luxurious lifestyle of network members and their officially declared income levels. Ultimately, the investigation targeting the criminal network was initiated on the basis of the decryption of encrypted communications. Beyond this, the involvement of network members in the operation of the restaurant could readily be established through open-source analysis.

4. Financial profile of the criminal network involved in Case Mike

The network operated primarily on a cash basis in relation to its drug trafficking activities. Reportedly, combined annual revenues generated from the **cannabis and cocaine trade** reached nearly EUR 10 million among the most senior network members. The majority of these funds were transferred abroad, at least in some instances through the use of concealed compartments in trucks. Financial accounts were reconciled at longer intervals rather than after each individual transaction. A similar system of periodic settlement was applied in relation to most customers and suppliers.

ANNEX 5

MADRID

DETAILED CASE STUDIES

Annex 5.N – Case November: The Cartel's Cannabis Network

1. Criminal network involved in Case November

The criminal network involved in Case November operated as a highly disciplined **family-based clan** with direct links to the Sinaloa Cartel in Mexico. Its core leadership comprised C1_N (father), C2_N (mother), and their son, C3_N, who was identified as the *de facto* leader in Spain. The organisation leveraged the identity of C3_N's deceased brother for more than thirty years to register companies and bank accounts in Mexico, demonstrating a long-standing capacity for financial fraud. The family, including 25 relatives (parents, uncles, and cousins), settled in Spain, ostensibly to escape persecution by a rival cartel in Mexico. The clan maintained a lavish lifestyle, characterised by luxury villas, high-end vehicles, jewellery, and substantial financial resources. The network relied on **trusted Mexican employees** residing at the main farm to oversee the illicit cultivation of marijuana. It also employed a well-connected accountant who managed its complex financial affairs and maintained records for its Mexican money exchange houses, which processed more than USD 170 million in less than two years.

In addition, the network relied extensively on external specialised criminal and corrupt service providers, including facilitators and 'crime-as-a-service' (CaaS) actors. This ecosystem comprised both corrupt professionals (i.e., gatekeepers) and specialised criminal logistics providers:

- **Facilitators (i.e., corrupt officials)**
  The network relied on a corrupt police officer (C4_N) who played a central role in helping the family establish itself. He registered luxury vehicle insurance policies and telephone lines in his own name and facilitated the use of false identities. In addition, he provided intelligence support by accessing police databases using another officer's credentials and fabricating reports on purported informants to justify his contact with the network's drug couriers, without complying with the required procedures to register the informant in police databases. This enabled the network to identify ongoing investigations and receive advance warnings.
  The family also benefited from the services of a lawyer (C5_N) who was known for representing members of other major organised crime networks. Acting as a CaaS provider, he assisted in establishing companies, organising business activities, arranging loans, concealing financial transactions linked to money laundering, identifying corrupt officials, and facilitating access to key contacts. His principal role was believed to be connecting the Mexican clan with established local CaaS providers. Nevertheless, C5_N subsequently testified as a witness during the trial.

  More broadly, the network demonstrated a willingness to pay substantial bribes, reportedly up to EUR 180,000-200,000, to facilitate its operations.[88] This included attempts to corrupt other police officers to legitimise the legality of its CBD plantations across multiple provinces. The network leader also persistently sought to influence police and judicial officials, including after his arrest.

[88] It should be noted that all monetary figures presented in the Spanish cases studies should be regarded as lower-bound estimates. They reflect only those transactions and assets identified and documented by the authorities in case files, rather than the full scope of financial flows within the criminal networks under investigation.

- **Crime-as-a-service actors (i.e., specialised logistics and fraud)**
  The network relied on a range of specialised criminal service providers to support its operations. It engaged with organisations specialising in the fraudulent importation of high-end vehicles from Germany, often involving VAT fraud schemes facilitated through shell companies in Portugal. The network also utilised providers offering luxury vehicle rental services to other criminal groups. To acquire firearms, the network sourced high-powered weapons, including assault rifles and pistols, from criminal suppliers operating from Eastern Europe (Serbia).

  The network further benefited from specialised technological support. The corrupt police officer (C4_N) and his brother-in-law established a robotics and automation company that appears to have supplied advanced indoor cultivation systems (including containers, lighting, and irrigation infrastructure) for the network's clandestine marijuana plantations. This venture was financially supported by C3_N, the network leader. At the distribution level, the network relied on criminal groups to facilitate the distribution of drugs. These included local Spanish gangs, such as criminal groups from the Cañada Real Galiana in Madrid, as well as other transnational criminal networks (e.g., from Croatia, the Netherlands, and Poland).

2. Legitimate businesses involved in Case November

The criminal network involved in Case November employed a **sophisticated and multifaceted strategy** to exploit the legal economy, with the dual objective of concealing its drug trafficking activities and laundering illicit proceeds. Its establishment in Spain was facilitated through the formal declaration of substantial assets to the Spanish Administration, including more than EUR 6 million in cash and 65 kilograms of investment gold transported from Mexico via charter flights in 2020. This process required legal assistance and the involvement of professional advisors. However, the illicit origin of these assets was subsequently uncovered through financial intelligence provided by the Spanish FIU (SEPBLAC) and the findings of the ensuing police investigation.

In this process, several **business entities and front companies** operated across various (sub)sectors of the legal economy, primarily to facilitate money laundering, create a façade of legitimate income, and provide logistical cover for criminal activities.

- The real estate and rental company (**LTD1_N**), whose sole administrator was C2_N, initially focussed on luxury goods and jewellery. Its corporate purpose was subsequently expanded to include other activities such as real estate, construction, and the purchase, sale, and rental of vehicles. Real estate was extensively used for asset acquisition and money laundering through 'house flipping' (cf. *infra*). The network acquired high-end residential properties and large agricultural estates. In parallel, the automotive and vehicle rental activities involved the acquisition and registration of dozens of luxury vehicles. These vehicles were rarely rented out and were instead used by members of the organisation, serving both as a means of laundering proceeds and as instruments for drug deliveries and payment settlements.

- The purchase of a gas station (**LTD2_N**), located near Madrid, provided a key local front in the town of Roe, where the main country house and farm were located. Although the gas station generated relatively low profits that did not correspond to the lifestyle of the network, it offered a seemingly legitimate commercial operation. It also supplied fuel required for the network's marijuana plantations and functioned as a vehicle for money laundering.
- As part of the network's strategy for long-term expansion into the synthetic drug market, it sought to acquire a pharmaceutical company (**LTD3_N**), representing its most ambitious infiltration attempt. This pre-existing company, with branches in Switzerland and Portugal, was presented as being engaged in the legal cultivation of cannabis for CBD extraction for state-regulated cosmetic production. Although this activity was authorised by the State, it lacked the necessary capacity to carry out such production. The company was used as a cover to conceal large-scale illicit marijuana cultivation and to facilitate the future importation of chemical precursors (i.e., fentanyl and methamphetamine) from China into Europe. The acquisition therefore represented more than a money-laundering vehicle; it was a forward-looking investment intended to position the cartel within one of the most profitable illicit drug markets emerging in Europe and sustaining demand in the United States.
- The network established a taco restaurant (**LTD4_N**) to launder illicit cash and to provide cover for the potential installation of a clandestine laboratory.

3. Crime script based on Case November

Motivation – Purpose

The central objective of the criminal network involved in Case November was to establish a permanent operational base for the Sinaloa Cartel in Europe for **financial gain**, using Spain as a strategic foothold to expand its influence across the continent and into third countries. From this position, the organisation sought to build a durable criminal infrastructure capable of supporting large-scale narcotics distribution, financial reinvestment, and long-term diversification into emerging illicit markets. The network adopted a sophisticated and multifaceted strategy to exploit the legal economy, with the dual purpose of concealing its drug trafficking activities and laundering illicit proceeds.

Drug trafficking constituted the core activity of the network. The organisation produced high-THC marijuana on an industrial scale behind the façade of authorised CBD cultivation, using agricultural sites equipped with advanced automated systems and operated by trusted personnel. In parallel, it imported and processed high-purity cocaine, supplying both domestic Spanish groups and international criminal organisations. These activities generated substantial volumes of illicit cash, forming the financial basis for all subsequent stages of the network's criminal strategy.

Furthermore, **money laundering** functioned as a structural component of the organisation rather than a secondary activity. The network reintegrated illicit profits through real estate purchases and rapid resale, the acquisition and circulation of luxury vehicles, the operation of hospitality and retail businesses, and the systematic use of complex corporate structures involving front companies and strawmen. These mechanisms enabled the clan to distance drug proceeds from their criminal origin while simultaneously investing in assets and enterprises designed to shield, legitimise, and expand its operations across multiple jurisdictions.

Preparation

The preparation phase of the network's activities was characterised by an unusually large initial capital deployment and the deliberate construction of legal and institutional **protective structures**. Upon arrival in Spain, the leaders introduced more than EUR 6 million in cash and 65 kilograms of investment gold, all of which were formally declared to the Spanish authorities. This substantial inflow of resources provided the financial foundation for establishing a broad legal and logistical infrastructure capable of supporting long-term criminal operations.

To conceal their intentions and create a **legitimate façade** for their activities, the network rapidly developed a multi-country corporate structure. Companies such as LTD2_N and LTD3_N were incorporated and presented as lawful business entities, enabling the group to mask illicit THC production by exploiting opportunities arising from the replacement of traditional crops with CBD plantations, to structure financial flows, and to anchor its presence within the formal economy. These companies also facilitated the circulation of assets and provided a channel through which future operational expansion could be concealed. In this way, the network situated its activities within a legal grey area. This regulatory ambiguity enabled the organisation to camouflage extensive marijuana plantations – cultivated with THC levels exceeding legal limits – within the appearance of an authorised agricultural and pharmaceutical project. The presumption of legality significantly deterred early police intervention and provided an effective shield for narcotics production.

At the same time, opportunities for **corruption** played a decisive role in the preparatory stage. The network leveraged the connections of an assisting lawyer (C5_N) with pre-existing ties to criminal environments, enabling it to secure the cooperation of a corrupt police officer (C4_N) and his brother-in-law. These individuals provided essential logistical and identity-related services, including the registration of vehicles and other assets, the activation of telephone lines, and the manipulation of administrative processes. Their involvement significantly enhanced the network's capacity to operate covertly while evading routine detection mechanisms.

Pre-activity or enabling conditions

Before fully initiating its criminal operations, the organisation established a set of **enabling conditions** that facilitated entry into Spain, integration into its legal framework, and the construction of a protective environment around its activities. One of the first steps involved creating a judicial façade through an asylum application in which the leaders claimed persecution by a rival Mexican cartel. This legal manoeuvre provided a plausible justification for their relocation and afforded a degree of institutional protection during the initial settlement phase. The establishment of **logistical channels** further strengthened the group's operational readiness. Through strategically positioned contracts, the network arranged a supply route for cocaine entering Spain via Adolfo Suárez Madrid-Barajas Airport. Couriers acting as 'mules' transported cocaine paste concealed within coffee packages, exploiting vulnerabilities at the point of entry. This arrangement ensured a steady flow of narcotics into the country while enabling the organisation to circumvent conventional interdiction measures. Together, these conditions laid the groundwork for the cartel's broader ambitions, enabling it to operate under a veneer of legality, exploit systemic gaps, and secure reliable logistical routes prior to the full-scale launch of its criminal activities.

With regard to **company acquisition**, the network employed elaborate financial engineering involving an asylum seeker (acting as a strawman) and a European-Hispano-American individual. To acquire the pharmaceutical conglomerate (LTD3_N and its Swiss and Portuguese subsidiaries), the organisation advanced approximately EUR 3.5 million. The company was subsequently transferred to the leader's mother (C2_N) for EUR 1 through a complex arrangement involving interlinked loans between individuals and companies, followed by the forgiveness of debt owed by the strawman. This mechanism effectively converted illicit funds into legitimate ownership and corporate control.

Activity

The operational phase of the criminal network was characterised by a fully integrated system of drug production, processing, distribution, and financial recycling, designed to sustain large-scale criminal activity while maintaining a veneer of legitimacy. Its financial cycle was anchored in the systematic **laundering of drug proceeds**. The organisation recycled illicit funds primarily through the acquisition of and resale of luxury assets and real estate. High-end vehicles served not only as status symbols but also as payment instruments (cf. *infra*), enabling the circulation of substantial amounts of cash outside the formal banking system. Real estate played a particularly important role in this process. The network repeatedly purchased luxury homes in Madrid and resold them shortly afterwards, in some cases within six months, as a means of distancing illicit proceeds from their origin (i.e., '**house flipping**'). Crucially, these transactions were often conducted at a loss, with losses of EUR 50,000 to EUR 60,000 incurred on properties purchased for approximately EUR 1.15 million. This cycle reinforced the network's capacity to sustain its operations, reinvest profits, and finance further criminal expansion.

Post-activity or post conditions

The investigation into Case November, conducted by the Spanish National Police (in Spanish: *Cuerpo Nacional de Policía*) and the Customs Surveillance Service (SVA) of the Tax Agency (AEAT), culminated in 2022. The operation resulted in 24 arrests, the seizure of large quantities of narcotics, assault rifles and pistols, luxury assets (including vehicles, properties, and jewellery), and the freezing of twenty bank accounts. Following the arrests, the criminal network adopted a deliberate judicial strategy aimed at obstructing and **destabilising the legal process**. The defendants and their legal representatives inundated the examining court with motions, petitions, and extensive documentation, exploiting procedural vulnerabilities and the limited capacity of a local investigative court ill-equipped to manage a case of such international complexity. This tactic placed considerable strain on judicial resources and contributed to significant delays.

The **handling of confiscated assets** further illustrates the challenges that followed the investigation. High-value luxury vehicles, including Rolls-Royces and Lamborghinis, deteriorated significantly while in police custody. The investigating judge refused to authorise either their sale or provisional use by law enforcement agencies, resulting in substantial depreciation of the vehicles' value. This outcome highlights the financial losses incurred by the State and reflects broader weaknesses in asset management following major organised crime investigations. Moreover, attempts to **corrupt the institutional environment** persisted after the dismantling of the operational structure. While in detention, the principal leader continued to seek influence over public officials, including attempts to bribe court personnel and administrative staff. The network also sought to obtain residence permits and nationality through illicit channels, demonstrating its continued reliance on corruption as a strategic instrument to secure legal protection and restore operational stability.

4. Financial profile of the criminal network involved in Case November

Financing sources and start-up capital

The network operated with substantial capital derived from high-level cartel activities, supporting a costly and high-risk operational structure. Its financial profile reflected a degree of capitalisation, liquidity, and transnational financial sophistication that is uncommon even among organised criminal networks. The group entered Spain with significant **start-up capital**, which was formally declared to the authorities (cf. *supra*). This strategy enabled the leadership to reduce initial scrutiny and present themselves as legitimate investors. The resulting influx of capital provided the foundation for the rapid establishment of companies, real estate investments, and high-value assets.

The capital injected into Spain was complemented by a strategic pattern of **asset acquisition** designed to facilitate both concealment and reinvestment. Luxury homes, high-value vehicles, agricultural estates, and a gas station served not only as lifestyle markers but also as instruments for money laundering and asset churning. These assets could be rapidly purchased, transferred, and resold, often at a financial loss deliberately incurred to distance illicit proceeds from their origin. Corporate structures such as LTD1_N, LTD2_N, and LTD3_N enabled the group to channel capital through multi-jurisdictional commercial networks, including subsidiaries or related firms in Switzerland, Portugal, Colombia, Argentina, and the United States. Furthermore, the organisation's financial strategies also relied on **sophisticated mechanisms**, including the use of strawmen, artificially structured loans, complex intra-company transfers, and the manipulation of purchase prices.

Beyond the funds physically introduced in Spain (more than EUR 6 million in cash and approximately 65 kilograms of investment-grade gold), the network controlled a substantial **financial infrastructure in Mexico**. It owned and operated thirteen to fourteen money exchange houses, generating a continuous flow of revenue and handling exceptionally large volumes of currency transactions. These exchange houses reportedly processed more than USD 170 million in less than two years, illustrating the scale at which the organisation was able to move funds and maintain liquidity across borders. This financial infrastructure enabled the group to sustain its European operations, reinvest profits, and cover operational expenses without relying solely on drug-related cash flows generated within Spain.

Payment methods and arrangements within the network

Financial transactions within the network reflected a preference for liquidity, mobility, and anonymity, consistent with the operational needs of a transnational drug trafficking organisation. **Cash** remained the primary means of payment for both internal and external expenditures. It was routinely used to acquire luxury properties, high-end vehicles, and other major assets, enabling the organisation to avoid traceable financial channels and operate with considerable discretion. The central role of cash was further reinforced by substantial liquidity generated through the group's Mexican exchange houses and the proceeds of narcotics trafficking in Europe.

In parallel, the organisation relied extensively on asset-based transactions. **Luxury vehicles**, including Ferraris, Lamborghinis, and Rolls-Royces, served not only as symbols of status and mobility but also as alternative currencies within the criminal economy. They were frequently used as partial or full payment for drug shipments and, at times, as covert means of narcotics transportation. The buyer received both the vehicle and the narcotics, paying the cartel for the drugs and part of the vehicle's value. In some cases, high-value vehicle rental agreements were simulated. Strawmen were also used

to hold legal title to luxury vehicles, while certain purchases were conducted through transactions originating in other jurisdictions. This approach enabled the network to settle transactions outside formal financial channels while facilitating the legitimisation of high-value assets.

At the operational level, the network maintained detailed accounts of **payments to drug couriers** (i.e., mules). These covered airfare, accommodation, food, and other costs associated with airport transit, including bribes intended to facilitate the safe passage of cocaine mules. The meticulous recording of such expenditures reflects the organisation's structured approach to logistics and its reliance on systematic financial planning to support international drug trafficking operations.

Costs of business operations

The organisation's operational model required sustained investment in resources to secure logistical cover, maintain legitimacy, and ensure the continuity of its illicit activities. These expenditures formed an integral part of its strategic calculations and were regarded as routine 'costs of doing business' within a transnational criminal enterprise. **Corruption** constituted one of the network's principal recurring expenditures. The organisation allocated substantial resources to bribes and facilitation payments to secure administrative advantages, obtain sensitive information, and shield its operations from law enforcement scrutiny. These payments targeted both corrupt intermediaries and public officials at various levels, with bribes to public officials in Spain reportedly ranging from EUR 180,000 to EUR 200,000 per contact. The use of corruption payments reflects the network's recognition of the strategic value of compromised officials and institutional insiders in ensuring operational continuity.

Furthermore, money laundering activities generated deliberate **financial losses** that the organisation accepted as necessary within its economic strategy. The repeated purchase and rapid resale of luxury properties, often at substantial loss, served as a mechanism for cleansing illicit capital. In this model, depreciation from 'house flipping' (cf. *supra*) was anticipated and incorporated into the network's financial planning, helping to distance large volumes of illicit funds from their criminal origin.

Operational expenses further illustrate the breadth of the organisation's financial commitments. Maintaining luxury properties used as clandestine laboratories required continuous investment in upkeep, utilities, and security. The acquisition of weapons, including high-powered firearms, and advanced technological equipment such as automated indoor cultivation systems and robotics added to its financial outlays. Legel fees and payments to strawmen acting as nominal administrators or assets also constituted predictable, recurrent costs.

Revenues and proceeds

The criminal organisation generated revenue through highly profitable illicit markets and sophisticated financial infrastructures, producing a diversified and resilient income stream. Central to its financial strength were **money exchange houses** operated in Mexico, which processed over USD 170 million in under two years. These entities provided a continuous source of liquidity, enabling the organisation to sustain its operations in Spain while reinforcing its financial base abroad. **Drug trafficking** constituted the second main pillar of the network's revenue model. Large-scale production of high-THC marijuana in Spain was intended to supply international markets where wholesale prices were significantly higher. The organisation sold cannabis to distributors in the United Kingdom, France, and the Netherlands at approximately EUR 8,000 per kilogram, exploiting substantial price differentials across European jurisdictions. This activity represented a considerable and stable income stream.

Cocaine trafficking provided an additional, highly lucrative revenue stream. The organisation planned to import and process large quantities of cocaine, with shipments of up to 1,000 kilograms. In parallel, LTD3_N served as a legal façade for an extensive illicit enterprise. Although its CBD extraction activities had limited operational capacity, internal projections estimated annual revenues of approximately EUR 11 million from the purportedly legitimate component of the business. These projections highlight both the scale of the intended cannabis operations and the anticipated profit margins derived from leveraging pharmaceutical infrastructure for illicit cultivation and processing.

This case illustrates a multilayered financial process in which illicit capital is progressively transformed through successive **cycles of legitimisation**. Initial proceeds from cartel activities entered Spain via the formal declaration of cash and investment gold, enabling the introduction of criminal funds into the legal economy as apparent lawful capital. These resources were then channelled through deliberately loss-generating operations, such as the rapid purchase and resale of high-value properties (i.e. house flipping), designed to reduce traceability by subjecting funds to controlled financial erosion. Once completed, these cycles produced capital with a substantially reduced risk profile, suitable for investment into legal or semi-legal ventures. Through this process, the organisation embedded itself within legitimate economic structures, creating a durable financial presence capable of sustaining long-term criminal activity while remaining partially insulated from detection mechanisms.

5. Harms caused by Case November

Harms to individuals

At the level of individual harm, Case November illustrates profound consequences for both victims and participants. The corruption of a previously high-performing police officer not only ended his career but also caused emotional and institutional harm, described by one expert as akin to 'taking a colleague away'. Moreover, members of the criminal network were not insulated from harm. Its principal leader, C3_N, carried the trauma of cartel violence in Mexico, where a relative had been killed. He operated with the awareness that his choices offered only two plausible outcomes: death or imprisonment. Mexican workers brought to Spain were subjected to conditions bordering on **coercive control**, including restrictions on their freedom of movement and daily living. They were reportedly forbidden to leave the farm, partly because their appearance, heavily marked by marijuana cultivation, could attract attention and because they might inadvertently disclose operational details. These circumstances indicate elements of labour exploitation.

Harms to other businesses

Criminal infiltration into sectors such as luxury car sales, CBD pharmaceutical production, and real estate distorted market conditions and placed legitimate enterprises at a **competitive disadvantage**, particularly where criminal organisations benefited from VAT fraud and an uninterrupted flow of undeclared cash. These illicit advantages enabled criminal entities to operate outside normal cost structures, undermining competition and eroding market integrity. Moreover, the complicity of gatekeepers, including lawyers, consultants, and other professionals, further undermined the credibility of professions that depend on public trust and compliance with legal standards. When such actors facilitate money laundering, identity fraud, or corporate manipulation, the resulting harm extends beyond economic distortion to the integrity of the professional frameworks themselves.

Harms to public institutions

The impact on public institutions was severe and multifaceted. The corruption of a police officer, particularly one embedded in central services, caused substantial reputational harm to law enforcement and contributed to a broader **erosion of public confidence** in State institutions. The judicial system also revealed structural and operational limitations in dealing with the scale and transnational complexity of Case November. The investigation was assigned to an investigating judge operating within a local court whose capacity was constrained by heavy caseloads and limited resources. These constraints contributed to delays in authorising certain investigative measures, the early closure of specific lines of inquiry, and difficulties in processing international cooperation requests to Mexico, Switzerland, and Portugal.

Asset management procedures likewise faced difficulties. Although legally grounded, the decision not to authorise the interlocutory sale or provisional use of seized luxury vehicles and jewellery resulted in the unintended depreciation of high-value assets while in custody, with some vehicles deteriorating significantly. This illustrates how structural constraints can affect the preservation of assets that might otherwise have generated revenue for the State.

Harms to the social environment

The scale and nature of the operation reveal significant harm to the wider social environment. The network contributed to the spread of drug addiction, the escalation of violence associated with arms trafficking, and an erosion of public trust following the corruption of law enforcement officers. Its activities also affected workers and local communities, including social groups linked to traditional agriculture whose livelihoods were disrupted by criminal activities and governance. Beyond these direct effects, the network undermined the wider systems intended to safeguard the social environment. Its activities weakened financial and regulatory controls, while extensive money laundering and tax fraud demonstrated the network's ability to exploit legitimate economic and institutional structures. The resulting strain on the judiciary further contributed to delays in the effective enforcement of the law. Moreover, the network's ambition to import fentanyl precursors and methamphetamine posed a potential threat to public health in Europe, given the severe impact synthetic opioids have had elsewhere.

Annex 5.O – Case Oscar: Chinese Connections and Criminal Cashflows

1. Criminal network involved in Case Oscar

The criminal organisation demonstrated exceptional adaptability and specialisation, operating not through a rigid top-down hierarchy but via autonomous yet **interconnected functional groups**. The first group was responsible for cash generation, producing undeclared cash through opaque commercial trade and the sale of counterfeit goods. The second group handled collection and custody, centralising and securely storing substantial volumes of illicit cash in clandestine depots. The third group focused on cash extraction and logistics, coordinating the movement of funds out of Spain. This group used overland routes with trucks fitted with hidden compartments to other European countries, exporting an estimated EUR 2 million weekly, as well as air routes involving couriers carrying cash-filled luggage to China, moving around EUR 1 million per week. The network also served external criminal groups

through a crime-as-a-service model, providing value transfer, cash logistics, and financial laundering for drug traffickers, human trafficking operations, and businessmen concealing undeclared profits.

A **familial trust structure** consistent with Guanxi social norms unified a related pyramidal group within the ecosystem, further reinforcing operational security.[89] The network's success relied on a core structure supported by specialised, independent, interchangeable, and compartmentalised groups. These groups provided various criminal services in short cycles before disappearing. When dismantled or exhausted, they were rapidly replaced to maintain the resilience of the main network. The network itself can be seen as an isolated and interchangeable criminal cell within a broader criminal ecosystem that has only suffered a partial setback and is expected to recover with relative ease. Its links to other groups, such as 'Emperador' and 'Draconarius', among others, appear evident. The lack of cooperation from Chinese authorities, who provide no evidence regarding the role of their territory and citizens in the criminal scheme, reinforced the broader framework of impunity underpinning the perceived prospects of prosperity of Chinese criminal networks.

2. Legitimate businesses involved in Case Oscar

The organisation embedded itself in the legal economy through a dense corporate infrastructure of approximately **forty companies**, primarily headquartered in Cobo Calleja. Ostensibly, these businesses focused on the legal import and wholesale distribution of Chinese goods across the EU. They operated across several legal subsectors, conducting legitimate **imports of unregulated merchandise** for Chinese convenience stores and e-commerce platforms, exploiting lawful marketing channels to facilitate customs fraud, TBML, and VAT evasion. Retail outlets in the public sphere functioned as collection points, generating substantial volumes of undeclared cash through the sale of legal and counterfeit goods. The proceeds were ultimately reinvested in real estate assets.

Structurally, the network operated as an integrated international holding company, internalising logistics and intermediary invoicing to reduce its reliance on (potentially unreliable) external collaborators and maintain strict operational security. To adapt to evolving commercial trends and preserve digital opacity, a significant share of the network's sales was shifted to **online platforms** such as Amazon, Miravia, and AliExpress. This enabled the network to exploit the EU's 'One-Stop Shop' (OSS) regime, which simplifies cross-border business-to-consumer VAT compliance. By registering for the OSS in a single Member State, the entities paid VAT there for all European sales, deliberately limiting the visibility of transactions to tax authorities in destination countries such as Spain and making enforcement largely dependent on identifying the individuals operating the central logistics hubs. As these activities were conducted without physical storefronts and relied on parcel delivery services, the e-commerce platforms themselves incurred no legal liability.

To maintain both digital and physical opacity, the network employed a highly specialised three-tiered **hierarchy of legal entities**, each assigned a specific role in the fraud chain. The three tiers consisted respectively of producing or exporting companies based in China, importing companies located in the EU, and missing trader companies fronted by strawmen (cf. *infra*).

[89] 'Guanxi' is a fundamental concept in Chinese culture, referring to an effective system of personal networks and social connections based on mutual trust, reciprocity, and the exchange of favours. It extends beyond friendship, encompassing a network of obligations that facilitates business transactions and bureaucratic procedures.

3. Crime script based on Case Oscar

Motivation – Purpose

The network's primary monetary objective was the systematic repatriation of substantial illicit euro **cash flows** from Europe back to China. This process aimed to cleanse funds derived from large-scale fiscal fraud. In addition, through a crime-as-a-service model, the network provided cross-border value transfer, cash logistics, and money laundering services to external criminal networks engaged in drug trafficking, human trafficking, and prostitution.

Preparation

The network meticulously prepared its operational architecture by exploiting **Spain's strategic position** as a European commercial gateway to Eastern Asia. It established a physical base of forty companies in Cobo Calleja and built a multilayered trust network involving Chinese, Ukrainian, and Spanish nationals. Furthermore, the Cobo Calleja logistical hub, as a geographical element, provided the level of insulation and protection required by criminal enterprises.

The network's operational flow relied on a **strategic geographic triangle**, exploiting systematic weaknesses, including the practical impossibility of inspecting the overwhelming number of shipping containers, the absence of real-time law enforcement access to the Virtual Information Exchange System (VIES), and the lack of automated transport document records.

- **Manufacturing base** (China): China served as the primary source of the physical goods and the ultimate destination of laundered funds.
- **Entry points** (EU, Greece, Hungary): These strategic jurisdictions facilitated the introduction of goods into the EU while enabling the exploitation of intra-Community VAT exemptions. Chinese criminal networks specifically targeted porous customs gateways where they had access to logistics providers from their own country, as well as companies registered with an Economic Operator Registration and Identification (EORI) in the Member State of entry, a mandatory requirement for importing and exporting goods within the EU. These companies subsequently channelled the goods through VAT fraud schemes. The network also exploited the practical impossibility of inspecting every container entering the EU, given the scale of international trade. In addition, it benefited from the difficulties faced by police and customs authorities in detecting fraud during the transport of goods to distribution warehouses, where the principle of free movement of goods applied. The use of disposable documentation, including invoices and CMR consignment notes, further complicated detection, highlighting the importance of robust control systems based on automated electronic CMR (e-CMR) records.[90]
- **Commercialisation hub** (Spain): Spain functioned as the final destination, where the organisation carried out reception and distribution functions.

[90] The CMR is the standard consignment document used in international road freight transport. Real-time access to the Virtual Information Exchange System (VIES) for law enforcement remained notably inadequate.

Pre-activity or enabling conditions

Logistical preparations included the establishment of clandestine cash depots and the acquisition of modified vehicles. Moreover, the scheme required a continuous flow of undeclared imports and a stable client base of criminal actors willing to pay commissions for laundering services. The operation's success depended on the strategic use of strawmen to absorb legal liability and distance the *de facto* leadership from illicit activities. The deliberate, forensic-level separation between the documented movement of goods and the actual flow of financial capital served as the primary **shield against law enforcement**. Strict security protocols governing courier behaviour, communications, and cross-border transfers were essential to maintain the network's operational security. When Spanish tax authorities occasionally detected irregularities, the organisation relied on associated networks to rapidly generate false invoices and documentation to artificially justify the commercial activity, reflecting the systemic impunity of the ecosystem.

Activity

The activity phase involved the physical **importation of goods**, which entered Europe through the Port of Piraeus in Greece. These goods were documentarily transited via shell companies in Eastern Europe and ultimately transported directly to Spain. While maintaining an appearance of legality through a façade of legitimate warehousing and retail operations, the network operated clandestinely, ensuring that the actual movement of goods and generation of illicit cash remained shielded from fiscal oversight.[91] Retail sales generated substantial volumes of undeclared cash, which collection teams centralised in clandestine depots using forty seized cash-counting machines.[92] To ensure security during illicit transactions, the network developed sophisticated authentication protocols, including the use of torn halves of banknotes as verification tokens during cash handovers. The extraction group physically smuggled an estimated EUR 2 million weekly by land and over EUR 1 million by air. Funds were processed through Fei Qian value transfer systems and transferred to China, Hong Kong, and Dubai, coordinated via secure communications channels such as Telegram.

To maintain both digital and physical opacity, the network employed a highly specialised three-tiered **hierarchy of legal entities**, each assigned a specific role in the fraud chain.

- The first tier consisted of complicit **producing or exporting companies** based in China. These entities possessed genuine manufacturing capabilities but were complicit in the fraud. They facilitated the scheme by accepting non-commercial payment routes, such as transfers from third-party shell companies with no documented commercial relationship to them. In terms of documentation, they provided falsified invoices for EU customs, misrepresenting both the quantity of goods and the identity of the actual clients to reduce the initial fiscal footprint.

[91] On the rare occasions when the Spanish Tax Agency detected irregular operations, the criminal network relied on associated groups to generated false invoices and documentation to artificially justify or regularise the commercial activity, thereby allowing sufficient time to complete the process.

[92] The retail storefronts served as the primary collection points for illicit cash. These establishments maintained a legitimate physical presence while reporting turnover and tax footprints that were near-zero or significantly lower than actual commercial activity, enabling the accumulation of substantial volumes of undeclared cash.

- The second tier consisted of **importing companies** located in the EU, particularly in regions such as Greece and Hungary. These entities managed the entry of goods into the EU and frequently exploited the Economic Operator Registration and Identification (EORI) system by registering in one Member State while operating in another. To facilitate VAT evasion, they declared sales to a third company in a different Member State, thereby invoking VAT exemptions for intra-Community transactions. This created a layer of complexity that significantly hampered cross-border investigative efforts.
- The third tier consisted of **missing trader companies**. These were instrumental entities fronted by strawmen and designed to concentrate tax liabilities within disposable structures. Under the domestic model in Spain, they were registered in the country of final sale to accumulate substantial VAT liabilities that were never settled. Under the multi-country EU model, these entities generated transport documents and invoices solely to provide a legal veneer for the physical movement of goods to Spain. These documents were not declared to any tax administration, allowing goods to enter the black market immediately upon arrival. To execute their evasion mechanisms and avoid tax settlement, these companies either rapidly disappeared by liquidating and replacing the entity before audit cycles or engaged in simulated purchase operations through a network of *ad hoc* entities, generating false invoices to artificially compensate for VAT liabilities or declare artificial losses.

The network also implemented a notably innovative laundering mechanism involving **Ukrainian refugees**, whereby humanitarian regulatory frameworks were exploited by instructing refugees to declare illicit cash as personal savings and deposit them into Spanish banks. The refugees subsequently reimbursed the network using their own legitimate resources, thereby obscuring the illicit origin of the funds and disrupting financial traceability.[93] In addition, the network orchestrated a subsidy fraud scheme involving complicit **Spanish wineries**: illicit cash was provided to an intermediary, the winery claimed EU and government subsidies for simulated wine promotion programmes in China and subsequently transferred the combined funds via bank transfer to the Chinese exporter, generating a net profit for the winery.

Upon reaching the destination countries, the expatriated cash was fully integrated into the formal financial system through bank deposits and transfers, often through **shell companies** in jurisdictions perceived as having weaker anti-money laundering controls (such as Hungary and Slovakia), via falsified sales used to pay the original Chinese manufacturers. Finally, the laundered funds were reinvested in tangible assets, such as luxury vehicles and real estate, completing the transformation of illicit capital into apparent legitimate wealth.

[93] Following the Russian invasion of Ukraine in 2022, exceptional financial measures enabled refugees to enter Spain with significant amounts of cash and to access the banking system more easily. The criminal network exploited this humanitarian framework to facilitate money laundering and disrupt financial traceability.

Post-activity or post conditions

The investigation into Case Oscar, launched in 2021 by the Central Operational Unit (UCO) of the Guardia Civil with the support of the State Tax Administration Agency (AEAT), represents a paradigmatic example of a highly sophisticated transnational **criminal investigation**. The operation involved extensive multi-agency collaboration, including the Madrid Regional Customs Surveillance Area, the Labour and Social Security Inspectorate, and the Tax Agency's Fraud Investigation Unit (ONIF), as well as international partners from Portugal, Germany, Romania, Belgium, and Hungary within a dedicated Operational Task Force coordinated by Europol and Eurojust. More than two hundred officers were deployed across at least ten Spanish provinces, executing more than forty searches targeting private residences, business premises, and warehouses linked to approximately forty corporate entities.

The investigation exposed a complex criminal infrastructure characterised by a high degree of organisational compartmentalisation, transnational logistical coordination, and the systematic 256exploitation of vulnerabilities in customs control. These features not only facilitated large-scale illicit activity but also significantly hindered judicial and law enforcement responses, as strict internal segmentation often resulted in the loss of evidentiary continuity. Consequently, coordinated legal action proved exceptionally difficult, underscoring **structural limitations** in the capacity of local courts to manage highly complex cross-border cases. Notably, the dismantling of the network in Case Oscar relied on the discovery of documentary evidence directly establishing criminal liability. In the absence of such evidence, comparable Chinese networks frequently evade detection due to their operational opacity and sophistication. This case therefore highlights a broader systemic vulnerability: the persistence of highly adaptive criminal organisations capable of distorting market competition and undermining regulatory frameworks.

Despite these challenges, the operation led to the **arrest** of thirteen individuals, primarily Chinese nationals, alongside Ukrainian and Spanish suspects, with an additional three persons placed under investigation. Among those apprehended were key organisations and business figures reportedly operating from major commercial hubs such as Cobo Calleja. The dismantling of the network resulted in the **seizure** of nearly EUR 7 million in cash, the freezing of multiple bank accounts, and the confiscation of 25 real estate assets.

4. Financial profile of the criminal network involved in Case Oscar

Financing sources and start-up capital

Although no formal start-up capital was documented, the scale and maintenance of forty companies required substantial financial resources.

Payment methods and arrangements within the network

Transactions relied almost exclusively on cash, facilitated by Fei Qian underground banking systems and sophisticated authentication protocols (e.g., split banknotes). While not central to Case Oscar, cryptocurrencies were used in associated networks for peer-to-peer value transfers via stablecoins.

Costs of business operations

Operational expenses included modified vehicles, courier logistics, maintenance for corporate infrastructure, and personnel remuneration.

Revenues and proceeds

Revenue was generated from two principal sources: illicit commercial activities, including undeclared imports and counterfeit sales; and crime-as-a-service commissions, whereby the network provided high-volume laundering services to third-party criminal groups. The primary criminal network laundered an estimated EUR 3 million per week, while a related structure processed approximately EUR 1 million per day.

5. Harms caused by Case Oscar

Harms to individuals

The criminal network laundered proceeds derived from prostitution and human trafficking, thereby facilitating and sustaining the exploitation of victims. Moreover, money mules were exposed to criminal liability, while vulnerable individuals, including refugees, were manipulated.

Harms to other businesses

Legitimate enterprises in Cobo Calleja experienced significant competitive disadvantages as a result of counterfeit sales and tax evasion by network-affiliated businesses. Following enforcement actions, some businesses reported sales drops of 60 to 70 percent.

Harms to public institutions

Major crimes against the Public Treasury resulted in significant tax revenue losses. Moreover, the operation required over two hundred agents from multiple agencies, placing a substantial burden on public resources, and intensive judicial cooperation through Europol, Eurojust, and OLAF.

Harms to the social environment

Repeated large-scale operations caused reputational harm and contributed to the entrenchment of a criminal climate. The network's organisational adaptability facilitated rapid operational regeneration, further contributing to the erosion of the social and commercial environment in Cobo Calleja.

Annex 5.P – Case Papa: Banking on Fame

1. Criminal network involved in Case Papa

The network in Case Papa was characterised by a high degree of complexity, a hierarchical structure, and diversified activities, and has operated internationally since at least 2017. It was allegedly led by **three individuals**. C1_P, a television producer, exploited his public profile and credibility as a 'business card' to gain the trust of financial institutions and secure funding, often through purported film and television projects. He was the principal beneficiary of the proceeds. C2_P and C3_P specialised in banking and corporate operations, acquiring and concealing companies, appointing nominee directors, and using these entities to obtain financing from financial institutions.

With regard to its **crime-as-a-service** model, the network diversified its criminal activities, acting as a facilitator or service provider for other criminal groups, particularly in money laundering.

- **Narcotrafficking laundering** involved the use of the network's corporate structure of over seven hundred companies to launder proceeds for third-party organisations from drug trafficking by simulating fictitious commercial activity to legitimise substantial cash inflows. A separate organisation, allegedly led by drug trafficker C4_P, exploited the same structure for this purpose.
- The criminal structure relied on essential external collaborators and **corrupt professionals**, including bank employees who actively or passively facilitated operations in exchange for remuneration (such as commissions, cash, or in-kind benefits including high-end mobile phones, televisions, a Roomba vacuum, or apartments). They either ignored the fact that the leaders controlled companies without formal directorship or directly participated in the operations. The structure also involved legal professionals, including notaries and financial managers, notably a notary 'on the payroll' who assisted in the formalisation and validation of fraudulent documents and transactions.
- Approximately 58 of the newly indicted individuals acted as **figurehead administrators** for the companies (i.e., strawmen), attending bank offices to submit fraudulent documentation prepared by the leaders.

2. Legitimate businesses involved in Case Papa

The criminal use of the legitimate economy in Case Papa was extensive and sophisticated, centred on the **creation and concealment of corporate entities** to facilitate fraud and money laundering. With regard to corporate entanglement, the organisation established an intricate structure comprising more than seven hundred commercial companies, the vast majority of which were shell entities. In many cases, these companies had no genuine economic activity and served primarily to simulate solvent commercial operations and legitimate business relationships.

3. Crime script based on Case Papa

Motivation – Purpose

The scheme was primarily driven by the pursuit of **illicit financial gain** through the systematic acquisition of substantial funding from financial institutions and private investors, achieved via deception and abuse of the credit system. A secondary but equally significant objective was the **laundering of proceeds** derived both from internal fraudulent activity and external sources, in particular drug trafficking operations.

Preparation

The network exploited numerous structural opportunities with a high degree of premeditation. C1_P's public profile functioned as a form of **symbolic capital**, facilitating access to financing channels that would otherwise have been unavailable. This reputational leverage operated as a *de facto* credentialing mechanism within financial contexts. In parallel, an extensive corporate framework of more than seven hundred shell entities provided the infrastructure for the layering and concealment of illicit financial flows. The deliberate recruitment of corrupt intermediaries, including bank managers, legal professionals and notaries, further enabled the circumvention of institutional safeguards and the formalisation of fraudulent transactions.

The network's criminal activities affected several key sectors of the legal economy by exploiting structural vulnerabilities.

- The **financial and banking** sector was the primary target and most severely affected, with the network directly defrauding numerous banking institutions and 'societies of reciprocal guarantee' (in Spanish: *Sociedades de Garantía Recíproca*) through the abuse of the credit system to obtain financial products such as confirming, factoring, discount lines, bank loans, and credit policies. The scheme also targeted public funds, including ICO (Official Credit Institute) loans guaranteed by the State during the COVID-19 pandemic.
- The **audiovisual and entertainment** sector was instrumentalised by the network, with C1_P leveraging public recognition to present fictitious or inflated cinematographic and television projects to secure financing, thereby creating an appearance of legitimate commercial activity and corporate solvency.
- The **legal, accounting, and notarial** sectors were also implicated, with the network relying on the active complicity of professionals, including lawyers, financial managers, and a notary 'on the payroll', whose involvement was essential to sustain the operation, avoid detection by internal banking control systems, and validate fraudulent operations.
- The **public administration and taxation** sector was likewise affected, as the network defrauded the Public Treasury (AEAT) through tax evasion and efforts to conceal illicit proceeds.

Pre-activity or enabling conditions

Prior to the execution of criminal activities, several enabling conditions were established. Central among these was the creation and systematic concealment of **corporate entities** designed to project an appearance of legal solvency and commercial legitimacy, often with minimal share capital. In addition, fictitious or significantly inflated audiovisual and cinematographic projects were developed as a pretext to justify large-scale financing requests. The network also recruited personnel, including strawmen and specialised collaborators, who were instrumental in operationalising the fraudulent schemes.

Activity

The operational phase of the scheme was characterised by multiple interrelated practices. Fraudulent financing was obtained through ostensibly legitimate companies, leveraging the producer's name and supported by falsified commercial documentation and simulated economic activity. The network fostered the **appearance of genuine commerce** by simulating business relationships and issuing fictitious invoices across its constellation of companies. It further engaged in systematic cheque rotation (including the rotation of cheques and promissory notes), involving the continuous and rapid exchange of commercial instruments among affiliated entities to artificially construct and inflate liquidity and transactional volume, thereby projecting financial health and deceiving banks into extending credit.

Concurrently, substantial quantities of illicit cash – often transported by couriers using concealed compartments in vehicles – were introduced into the financial system with the assistance or acquiescence of corrupt banking personnel, who either facilitated deposits or ignored indicators of suspicious activity. These funds, together with proceeds from fraud, were then redistributed through a complex and prolonged circuit of inter-company transfers designed to obscure the funds' traceability and dissociate them from their illicit origin. The **laundered proceeds** were subsequently transferred to foreign jurisdictions (e.g., Panama, the Maldives, and Switzerland) or invested in luxury assets, vehicles, and real estate, as well as used to sustain ongoing fraud schemes, including the financing of earlier debts with newly obtained loans.

Post-activity or post conditions

Finally, the network's leadership was alleged to have actively obstructed enforcement mechanisms, including debt recovery and asset seizure procedures, conduct giving rise to the offence commonly referred to as 'frustration of execution'. The investigation into Case Papa was initiated in 2018 and executed in June 2021 by specialised units of the Spanish National Police and Civil Guard. Led by the National High Court, the **criminal proceedings** focused on dismantling a highly complex criminal organisation. A judicial proposal has been issued to proceed to trial against 55 individuals, including the principal figures identified in the scheme. The charges under consideration include participation in a criminal organisation, continued fraud in conjunction with the falsification of commercial documentation, money laundering, commercial corruption, obstruction of enforcement, frustration of execution, and tax-related offences attributed to specific defendants.[94]

4. Financial profile of the criminal network involved in Case Papa

Financing sources and start-up capital

The financial configuration of the network reflects a structured and resource-intensive model, combining elements of corporate proliferation, corruption, and illicit financial integration. Although precise figures regarding initial capitalisation were not specified, the establishment of the scheme necessarily required significant upfront investment. This included the incorporation of an extensive network of over seven hundred **corporate entities**, each requiring minimum statutory capital. In parallel, resources were allocated to the cultivation of corrupt relationships, including the payment of bribes and commissions to bank employees, notaries, and legal or financial advisors whose involvement was instrumental in circumventing institutional controls.

Payment methods and arrangements within the network

The network's internal functioning relied on a combination of formal financial instruments and informal arrangements. Cheques and promissory notes were systematically employed to simulate transactions and create the appearance of liquidity within the corporate structure. Payments to collaborators, particularly those facilitating access to the banking system, took **multiple forms**, including cash, consumer goods, and access to luxury services. At the same time, the network exploited a range of legitimate financial products (such as factoring, confirming, credit lines, ICO loans, and discount

[94] At the time of writing, the case remained in the intermediate phase of abbreviated proceedings, during which the prosecution and private parties were entitled to submit formal accusations or request additional investigative measures. The forensic examination of extensive documentary and digital evidence was ongoing and expected to play a significant role in substantiating the evidentiary basis for trial and potential asset recovery. Parallel civil proceedings, including judgements ordering restitution to affected investors, were also likely to inform claims for civil liability within the criminal proceedings.

facilities) as mechanisms for extracting funds. A further defining feature was the integration of large volumes of cash, primarily derived from drug trafficking, into the financial system through the complicity or acquiescence of banking personnel, corresponding to the placement stage of the money laundering process.

Costs of business operations

The costs of maintaining the operation were substantial and recurrent, including the administrative and legal burdens of sustaining a large corporate network, ongoing expenditure on corrupt facilitation, and operational costs associated with the movement and handling of illicit cash. In addition, the deliberate non-repayment of fraudulently obtained credit generated legal and financial exposure, often resulting in civil claims and criminal proceedings, including charges relating to obstruction of enforcement actions. Further **operational expenditure** was incurred in sustaining intermediaries such as strawmen and cash couriers.

Revenues and proceeds

Revenue generation within the network derived from **multiple streams**. The primary source consisted of fraudulently obtained financing amounting to more than EUR 50 million from financial institutions and private investors. In addition, the network appears to have generated income through the provision of money laundering services to third-party criminal actors, although the precise magnitude of these proceeds remains undetermined. A related civil judgement ordering the restitution of approximately EUR 35 million to an investor further indicates the scale of diverted or misappropriated funds.

5. Harms caused by Case Papa

Harms to individuals

At the individual level, private investors suffered significant economic harm after investing in projects presented as legitimate but ultimately not realised. Moreover, collaborators and workers involved in the projects were left with outstanding payments, directly transferring financial risk to individuals within the production chain.

Harms to other businesses

The impact on other businesses was equally significant. Banks and mutual guarantee societies incurred substantial losses from the non-repayment of fraudulently obtained credit facilities, including those backed by public guarantees such as ICO loans. Beyond the direct financial harm, the use of corruption to facilitate the entry of illicit funds into the financial system undermined institutional trust and weakened perceptions of integrity and reliability in financial markets.

Harms to public institutions

Public institutions were also adversely affected. The tax authority incurred losses from tax evasion and fraudulent practices, with estimated damages amounting to several million euros across multiple fiscal periods. State-backed financial instruments, particularly ICO credit lines, were also misused, thereby exposing public funds to the scheme. Furthermore, the scale and complexity of Case Papa, involving hundreds of corporate entities, transnational financial flows, and extensive digital evidence, placed a significant burden on judicial resources. This required the involvement of specialised investigative bodies, including UDEF, UDYCO, and UCO, as well as the jurisdiction of the National Court.

Harms to the social environment

Within the broader social environment, Case Papa contributed to a marked deterioration in the public image of those involved, particularly C1_P. More broadly, it illustrates how organised economic crime can exploit reputational capital and complex organisational structures to infiltrate legitimate markets, distort commercial practices, and erode public confidence in both the economy and the rule of law.

ANNEX 6

PARIS

DETAILED CASE STUDIES

Annex 6.Q – Case Quebec: The Luxury Laundering Loop

1. Criminal network involved in Case Quebec

The analysis of the judicial file and hearings of the various defendants revealed a **highly structured transnational criminal network** operating between Latin America, Europe, and the Middle East since at least 2012. The network was directed and supervised from Lebanon by C1_Q, identified by the US Drug Enforcement Administration (DEA) and the French Central Office for the Repression of Major Financial Crime (OCRGDF) as the organisation's supervisor and mastermind. Acting as a '*saraf*' (or broker), he centralised global accounting and settlement operations and was closely assisted by an inner circle.[95] C2_Q, an employee and close associate of C1_Q, served as logistics coordinator, issuing instructions to European teams, organising cash collections, and contacting intermediaries. C3_Q was a key fund provider, supplying cash in Europe and arranging settlements through the covert system. C4_Q, operating under the guise of an entrepreneur, acted as an intermediary for C1_Q and C2_Q, handling communications and supporting the network's logistical operations.

On European soil, the organisation relied on collection and conversion managers who operated trusted **family- and friendship-based sub-cells**. Initially, C5_Q served as a key collector and intermediary in Europe. Following debt accumulation and management failures, he was removed from the organisation by the Lebanese leadership and replaced by C6_Q as the network's principal collector and client. C6_Q established a highly closed organisation centred on family members, including his wife, brother, and stepson. He laundered over EUR 14 million through large-scale purchases of luxury watches.

To facilitate the integration and export of illicit proceeds via watches and vehicles, the network relied on **intermediaries** embedded in the legitimate economy. C7_Q, a restaurateur, acted as an intermediary in the luxury-watch trade and participated directly in the collection and counting bundles of cash amounting to tens of thousands of euros. C8_Q, a car dealer, used C1_Q's network to obtain substantial amounts of cash in Europe to purchase vehicles for export to Africa and the Middle East. C9_Q, a freight forwarder, facilitated customs fraud by shipping empty watch boxes and cases separately to Lebanon, enabling the network's accomplices to wear the watches across borders without arousing suspicion.

Intercepts and witness statements highlighted the network's high degree of **professionalism**. Members used dedicated phone fleets exclusively for criminal activities and, on C1_Q's instructions, employed coded language to conceal meeting locations. For example, Belgium was referred to as 'the oven' and the Netherlands as 'the mill'. The network also benefitted from insider complicity at Beirut airport, facilitating the secure and fraudulent importation of watches and capital.

[95] In (international) covert banking networks, a ***saraf*** (broker) coordinates fund collection on the sending side and identifies clients requiring cash downstream.

2. Legitimate businesses involved in Case Quebec

The **trade in high-end vehicles** served as the network's primary mechanism for justifying financial flows and converting collected cash. Several defendants, including C1_Q and C8_Q, presented themselves as vehicle traders or managers of automotive companies. C8_Q claimed to manage a company in Lebanon, earning a monthly salary of USD 10,000 to USD 15,000 and owning a fleet of seven luxury vehicles. The network relied on import-export and transport companies to move funds and goods across Europe. For example, C5_Q operated a transport company in which C1_Q had invested approximately USD 250,000.

3. Crime script based on Case Quebec

Motivation – Purpose

The principal motivation of the network's actors (i.e., collectors, *bureau de change* managers, and coordinators) was personal enrichment through commissions or margins on illicit financial operations. The network operated at a large scale, **laundering** several million euros. Its objective was to place, conceal, and convert cash in order to obscure its illicit origin and reintegrate the funds into the economy or return them to the principals. These financial operations were directly linked to international **drug trafficking**, in particular cocaine importation. Investigations established that the laundered funds originated from Colombian drug cartels. The European laundering network, coordinated from Lebanon, negotiated 'collection contracts' with known traffickers responsible for shipping cocaine containers to Mexico and Europe.

Preparation

The network heavily targeted the used-car sector, particularly in Germany, a jurisdiction characterised by the flexibility of cash-based vehicle transactions. Several members presented themselves as car traders. To reinforce this cover, they travelled with vehicle purchase orders and registration documents. **High-value luxury goods**, which concentrate substantial value in a small volume, were identified as an effective means of converting and transporting funds. Illicit funds were used to purchase designer bags (e.g., cash transactions at Louis Vuitton stores on the Champs-Élysées) and high-end watches (e.g., Rolex, Patek Philippe, Concord). A recent survey (2021-2022) revealed that some luxury-sector professionals, particularly in watchmaking and automotive retail), still lack a clear understanding of their due diligence obligations, including client identification and suspicious activity reporting. Criminal actors exploit these gaps, as well as the possibility of settling large cash transactions under the pretext of 'foreign clientele' (despite very strict legal thresholds in France: EUR 1,000 for residents and EUR 15,000 for non-residents).

By purchasing luxury watches and claiming customs tax refunds upon exiting the EU, the network not only laundered capital but also generated an **additional financial gain** through the recovery of VAT by the State. The high value added of watches and leather goods enabled the absorption of large cash sums into small-volume items, significantly facilitating their transport compared with cash-filled suitcases. Given the scale of international maritime trade, it was difficult for shipowners and customs authorities to monitor the purpose and origin of the funds used to acquire used vehicles exported to West Africa or the Middle East.

Moreover, the network primarily exploited weaknesses in the global financial system by relying on **hawala-type structures**. Rather than using conventional banking channels, it relied on Lebanese *bureaux de change*, enabling the transfer of drug proceeds from Europe to Latin America without formal cross-border banking movements. To facilitate settlements in Europe, companies linked to the diamond and jewellery sector were instrumentalised. This included, for example, a jewellery company in Antwerp (Belgium), whose manager – regularly in contact with members of the organisation – received funds and assisted in counting cash to facilitate laundering. The network targeted the Schengen Area by fragmenting its operations to exploit the specificities of national economies: cash collection in Spain, Italy, or the Netherlands, the use of Belgium for transfers via the diamond trade, and transit through Germany to justify cash flows through automotive import-export activities.

Pre-activity or enabling conditions

The network's members owned or used pre-existing legitimate commercial structures, including import-export companies, freight forwarders (e.g., LTD1_Q), and car-trading businesses. The organisation benefited from strategic **complicity** at borders, notably at Beirut airport. A senior official, the head of the airport's intelligence bureau, alerted traffickers to the presence of inspectors and facilitated the passage of couriers carrying luxury goods. To create an appearance of legality for their cross-border movements, members submitted cash declaration forms to customs, falsely presenting themselves as legitimate traders.

In the watchmaking sectors, collectors purchased **luxury watches** (worth several tens of thousands of euros) in France using drug proceeds. To avoid customs duties and airport scrutiny, the items were disassembled: the cases (boxes) were entrusted to freight companies (e.g., LTD1_Q) for separate shipment, while the watches were worn on the wrist or concealed (e.g., wrapped in tissues or hidden against couriers' bodies) during air travel. At airports, couriers presented the watches to fraudulently obtain tourist tax refunds. Once in Lebanon, the watches were reunited with their original packaging and reintroduced onto the legal market for resale. Unconverted funds were physically transported across borders (to Germany or Belgium), concealed in clothing bags or hidden compartments.

The *modus operandi* in the automotive sector involved individuals presenting themselves as **car traders** (such as C8_Q) targeting high-end vehicles (e.g., Mercedes, BMW) in Europe. To circumvent regulatory scrutiny, payments were often split: a cash deposit, drawn from illicit collections, was made within authorised or tolerated limits, while the remaining balance was transferred from accounts in Lebanon to legitimise the transaction. The purchased vehicles were subsequently shipped via ports (including in Belgium) for export by sea freight to Africa or the Middle East, on behalf of Lebanese companies.

Some managers of logistics companies acted with full **knowledge** of their clients' irregular activities. For example, the manager of LTD1_Q agreed to regularly ship empty luxury-watch boxes to Lebanon, while aware that the watches themselves were being transported across borders by passengers. Other providers, such as the Belgian companies LTD2_Q (handling customs documentation) and LTD3_Q (a maritime carrier), functioned primarily as logistical intermediaries and were not aware of the criminal origin of the funds used to finance the exported vehicles. Large retail outlets on the Champs-Élysées and high-end watch resellers accepted substantial cash payments (e.g., EUR 4,700 for a bag) without systematically verifying the origin of the funds, thereby providing the network an efficient conversion channel.

Activity

The network's core criminal activity was large-scale **international money laundering**, operating as a covert financial services platform for Colombian drug cartels. Its function was to collect the substantial cash proceeds generated by cocaine importation and distribution in Europe, and to reinject these funds into the legal economy or transfer them to principals in Latin America. To do so, the organisation fully bypassed the traditional banking system and its traceability controls, relying instead on informal hawala-type settlement mechanisms. Its activities included the physical collection of cash, clandestine cross-border transportation, and the large-scale conversion of funds through the purchase of high-value goods intended for export.

The network's activities were confined to the post-offence phase of drug trafficking, following the importation and sale of drugs in Europe. Drug proceeds were physically collected from local traffickers across several European countries (e.g., France, Belgium, Spain, Italy, Germany, and the Netherlands). Collectors gathered large cash sums and transported them in vehicles equipped with concealed compartments (e.g., under floor mats or near the wiper system) to avoid police or customs detection. To obscure their activities, logisticians used dedicated phones and coded communications. Cash was circulated covertly via hawala-type settlement mechanisms, with the involvement of certain merchants and jewellers in Europe, as well as *sarafs* based in Lebanon. To complete the **laundering process** and return value to the cartels, the illicit funds were converted into luxury goods and merchandise. The case files notably record the purchase of luxury cars and watches subsequently exported abroad.

Post-activity or post conditions

The exploitation of legal economic circuits by the criminal organisation occurred over an extended period. According to the offence periods established by the courts, the network operated continuously from 2012 until January 2016, immediately preceding the arrests. Investigators found that the cell led by C6_Q purchased luxury watches with illicit funds exceeding EUR 14 million from 1 January 2014.

Several indicators and **red flags** demonstrated the network's infiltration into legitimate commercial sectors, including the systematic use of large cash volumes to acquire luxury goods. Rather than relying on traceable bank transfers for international trade, the network used a hawala-type settlement system, operated by *sarafs*. Collectors, who sometimes presented themselves as traders, transported concealed cash sums. In one instance, customs intercepted vehicles carrying nearly EUR 500,000 hidden within concealed compartments. The separation of goods for cross-border transport was a strong indicator of fraud: empty watch boxes were shipped via official freight channels, while the watches themselves were transported clandestinely by passengers.

The dismantling of this 'multinational' laundering network required **large-scale international coordination** under the supervision of the Paris Specialised Interregional Court (JIRS). Upstream, investigators conducted extensive telephone intercepts. Analysis of these communications enabled authorities to determine each member's role, identify coordinators based in Lebanon, and trace cross-border cash-collection operations throughout Europe (in France, Belgium, Germany, the Netherlands, Italy, and Spain). Customs authorities also carried out roadside checks leading to the seizure of cash in transit. The coordinated arrest operations were executed simultaneously in France, Italy, Belgium, and Germany, taking advantage of the arrival of several network leaders on French soil. C1_Q was arrested at Paris Charles-de-Gaulle airport alongside one of his intermediaries. This arrest was followed the

same evening by the detention of other key members in Paris. The following day, on the basis of international arrest warrants issued by the French investigating judge, the German authorities arrested several additional members, while the Italian authorities apprehended another network associate. Searches conducted during these operations led to the seizure of multiple collection phones, cash, and personal luxury items. The defendants were subsequently brought before an investigating magistrate, charged, and placed either in pre-trial detention or under strict judicial supervision, including bail conditions ranging from EUR 40,000 to EUR 150,000, confiscation of passports, and travel bans.

4. Financial profile of the criminal network involved in Case Quebec

Payment methods and arrangements within the network

The organisation's financial profile was closely aligned with the underground economy of international drug trafficking. It functioned as a financial services provider to South American drug cartels under so-called 'collection contracts', enabling the repatriation of profits generated through the import and retail distribution of cocaine in Europe. The network's inputs were exclusively fiduciary in nature, described by the defendants as **'cash-to-cash' operations**. During seizures by customs, the judicial authorities and German notaries confirmed that the transported funds consisted almost entirely of small-denomination banknotes, a typology typically associated with retail drug proceeds.

To evade the traceability of the traditional banking system, the network relied on a covert **settlement mechanism based on hawala**, allowing value transfer without physical cross-border movement of cash. Cash integration into the legal economy was achieved on a large scale through the use of front companies and complicit garages for vehicle acquisition, as well as through the purchase of high-value luxury goods, which concentrate substantial monetary value in compact form. Transactions frequently involved tens of thousands of euros per item, including cash payments of up to EUR 195,000 for a single watch.

Costs of business operations

The organisation operated according to a **business logic**, including structured profits, profit margins, and the management of bad debts. Its profitability was based on a global commission paid by the traffickers in exchange for laundering services, subsequently distributed between coordinators and 'sarafs' in Lebanon. At the lowest level of the logistics chain, 'collectors' (who assume the criminal risk during clandestine transport) received a fixed fee of EUR 2,000 to EUR 5,000 per trip.

The model also absorbed 'operational losses' arising from customs interceptions. The case files illustrated such losses through the seizure of nearly EUR 500,000 concealed in vehicle driven by network members in Germany. Covert accounting was maintained with strict discipline by the network leader, and any financial shortfall was met with severe sanctions. For instance, collector C5_Q was dismissed by the Lebanese supervisor C1_Q after being accused of having spent 'money that did not belong to him', leaving him with a personal debt of EUR 100,000 to the organisation.

Revenues and proceeds

Analysis of the judicial files revealed a money laundering infrastructure of macroeconomic scale. The organisation handled tens of millions of euros over its established period of activity (2012 until early 2016). A settlement actor operating initially in Amsterdam (the Netherlands) testified to laundering EUR 13 to 15 million per month on a regular basis, illustrating the intensity of the financial flows. At the operational cell level, the volumes handled indicate rapid cash turnover. The network managed by collector C5_Q, for example, accumulated over EUR 5 million within seven months. Similarly, collector C10_Q processed approximately EUR 1.8 million across seven collection operations between March and July 2015, with individual transfers ranging from EUR 200,000 to EUR 500,000 per trip.

5. Harms caused by Case Quebec

The analysis of the transnational laundering network involved in Case Quebec, operating at the crossroads of Europe, Latin America, and the Middle East, reveals a range of direct harms. Although **money laundering** is inherently designed to remain invisible and does not necessarily involve an immediate physical victim, its direct effects can nevertheless significantly undermine institutional integrity, public safety, and macroeconomic stability.

Harms to other businesses

The network instrumentalised sectors of the real economy, including high horology, car dealing, and international freight, to facilitate its settlement operations. This infiltration distorted market conditions, as front companies operated without conventional commercial objectives and prioritised the rapid liquidation of illicit funds over legitimate funds. This created an unfair competitive advantage over law-abiding businesses, which were sometimes knowingly and sometimes unknowingly drawn into the criminal scheme, exposing them to criminal liability and reputational harm.

Harms to public institutions

By leaning on the informal hawala system and unlicensed money changers (‘*sarafs*’), the criminal organisation circumvented public controls on anti-money laundering (AML) and counter-terrorist financing (CTF). Injecting tens of millions of euros outside the regulated banking system undermined financial traceability and, consequently, the effectiveness of the European financial architecture. Furthermore, the network’s cross-border logistics involved the compromise of public officials. The case file refers to the collusion of the head of Beirut Airport's intelligence bureau, who facilitated the movement of couriers and cash while circumventing customs controls. This undermined both State sovereignty and the integrity of public institutions responsible for national security.

Annex 6.R – Case Romeo: Pakistani Forgery and Money Laundering

1. Criminal network involved in Case Romeo

Analysis of the case material indicated the existence of a structured **Pakistani criminal organisation**, primarily based in Val-d'Oise, engaged in document fraud, facilitation of irregular residence, and large-scale money laundering. The network operated through a clearly defined familial and operational hierarchy, as presented in Table 16. Two brothers, C1_R and C2_R, coordinated its activities under the cover of LTD1_R. C1_R, a national of France, oversaw the organisation's administrative and commercial operations, while C2_R, who held a valid residence permit, exercised a leadership role and was responsible exclusively for issuing financial instructions. C1_R had an extensive criminal history. In 2017, he was implicated in offences including organised-gang undeclared work, organised-gang employment of foreign nationals without authorisation, facilitation of irregular residence, and aggravated money laundering. He had previously been arrested in 2009 for facilitating the irregular entry of a minor into national territory. Nevertheless, C1_R remained able to operate the network, highlighting deficiencies in post-conviction monitoring.

Table 16
Overview of the core members of the criminal network involved in Case Romeo (Paris)

Member	Role
C1_R	Principal organiser; *De facto* manager of LTD1_R
C2_R	Principal organiser; Financial leader
C3_R	Operational coordinator; Distributor of forged documents
C4_R	Logistics and financial coordinator
C5_R	Supplier of forged documents
C6_R	Secondary financier
C7_R	Client of the network; Potential smuggler
C8_R	Associated third party; Opening of bank accounts
C9_R	Associated third party; Opening of bank accounts
C10_R	Associated third party; Opening of bank accounts
C11_R	Official front-man manager of LTD1_R

C3_R served as the network's principal intermediary, overseeing the receipt and **distribution of forged documents**, including Italian passports sold for EUR 900 and French residence permits, while executing the financial instructions issued by C1_R and C2_R. He used at least four aliases to open 25 bank accounts. C4_R acted as a logistics and financial coordinator, managing both fund transfers and the distribution of forged documents. In February 2020 alone, he arranged the transfer of approximately EUR 30,000 to Pakistan via courier services. He used nine false identities to open 54 bank accounts. He was previously known to the authorities for forgery of administrative documents and use of forged documents, and did not hold a valid residence permit. C5_R, who held a valid Italian residence permit, acted as a logistics facilitator for the distribution of forged documents. He received parcels from Pakistan and redistributed them through his network of contacts. He operated with a high degree of

caution, frequently changing telephone numbers and systematically verifying the identity of those with whom he communicated.

C6_R, who held a Spanish residence permit, used twelve false identities to open 59 bank accounts, with estimated monthly withdrawals of approximately EUR 100,000. Furthermore, C7_R was known to the authorities for fraud and did not hold a French residence permit. He received transfers from various companies into a bank account, indicating his involvement in the money laundering scheme. Telecommunications intercepts and geolocation data showed regular contact with foreign numbers (e.g., Italy, Romania, Poland, the Netherlands, Austria) and suggested a possible role in the facilitation of migrant movement from Italy. C8_R, C9_R, and C10_R completed the network's banking structure.

2. Legitimate businesses involved in Case Romeo

Analysis of the criminal proceedings showed that several **construction-sector companies** had served as fronts for illicit activities. Companies such as LTD1_R were formally registered for painting, glazing, and electrical work, while operating from business centres that provided only a registered address and no genuine business presence. Operating through approximately twenty entities linked to LTD1_R, the network used these structures as financial conduits, with more than 25 bank accounts identified within its core operations. Pre-employment declarations (in French: *Déclaration Préalable à l'Embauche*) (DPAE) were occasionally submitted to create an appearance of regulatory compliance: C2_R was registered by LTD1_R, whereas C1_R, the company's *de facto* manager, was not. The criminal network relied on **frontmen** to manage these corporate structures. Although C11_R was the registered manager of LTD1_R, the company was effectively controlled by C1_R, who oversaw its daily administrative and commercial operations, as confirmed by phone taps.

3. Crime script based on Case Romeo

Motivation – Purpose

The network's activities were primarily driven by **financial gain**, derived from the exploitation of both administrative vulnerabilities and the construction sector. It generated revenue through the sale of forged documents, including Italian passports sold for approximately EUR 900 each. These counterfeit identity cards, residence permits, and European driving licences enabled clients in an irregular situation to open bank accounts, obtain credit, and move within the Schengen Area. The network's ultimate aim was to divert proceeds from undeclared construction work by cashing company-issued cheques and subsequently converting the funds into cash or transferring them to Pakistan. In this context, the network engaged in a range of interconnected criminal activities (cf. *infra*).

Preparation

Analysis of the proceedings revealed the systematic exploitation of the **construction sector** by the criminal network. The sustained demand for labour in painting, glazing, and electrical work enabled the (clandestine) employment of undocumented migrants by the network. [96] For example, C3_R worked on construction sites for C1_R without a residence permit and under multiple false identities. At the same time, the complex flow of transactions between contractors and subcontractors facilitated the

[96] In this context, one company (LTD2_R) was flagged for the use of undeclared labour and the criminal use of corporate assets. None of the individuals receiving transfers from construction companies had been registered through a DPAE declaration.

commingling of legitimate and illicit funds. Transfers received into fraudulent accounts – opened with forged European documents – were disguised as wage payments from third-party construction companies. The scheme further benefited from the ease with which very small enterprises (VSEs) could be established and dissolved in the sector, allowing the multiplication of legal entities and the dilution of regulatory oversight.

In parallel, the network exploited opportunities arising from its **corporate front structures**. LTD1_R and its associated entities enabled the opening of 154 bank accounts and the acquisition of consumer edit, which was immediately withdrawn in cash. Their legal existence also provided supporting documentation, including accommodation certificates and occasional DPAE registrations, facilitating identity verification procedures at financial institutions. Furthermore, the apparent legitimacy of DHL and FedEx was used to import consignments of forged documents from Pakistan, Turkey or Greece, disguised as professional shipments. High-quality European identity documents (Italian, Spanish, Greek), including look-alike documents, enabled the network's financial integration before detection. Moreover, the presence of a Pakistani community in the Val d'Oise construction sector provided a readily available pool of frontmen managers (such as C11_R at LTD1_R) and labour, which further insulated the network's true organisers from direct scrutiny and investigation.

Pre-activity or enabling conditions

The *modus operandi* consisted of the acquisition of **forged European passports**, either as look-alike documents or wholly falsified. These documents were produced abroad (in Pakistan, Turkey, or Greece) and sent to France via DHL or FedEx, concealed in packaging of white paper and blue carbon paper, a camouflage method likely standardised by the same upstream supplier. Parcels were received by C5_R under multiple recipient identities and at addresses across different French departments. The documents were subsequently stored in discreet locations (e.g., vehicles or basements) in Argenteuil.[97] Meetings were arranged in public spaces (e.g., Gare du Nord, Rue Marx Dormoy, La Chappelle Metro) for the handover of documents in exchange for bundles of banknotes. Ultimately, the fraudulent documents were used to open over 150 bank accounts under false identities. These accounts received **fictitious wage-disguised transfers** from complicit construction companies without any corresponding pre-employment declaration (DPAE). The funds – estimated at approximately EUR 175,000 per month for C4_R and EUR 100,000 per month for C6_R – were then rapidly withdrawn in cash, transferred by courier to Pakistan, or remitted via money-transfer services. In parallel, the network facilitated migrant transit, including minors, from the United Kingdom (via Dunkirk).

The use of the legitimate sector was not marginal but **systemic**, with more than twenty construction companies identified as issuers of fraudulent transfers. LTD1_R and its associated structures were entirely controlled by C1_R and C2_R, who dictated financial decisions despite the presence of formal managers. The entities had no genuine economic activity consistent with their declared corporate purpose. The twenty construction companies issuing fraudulent transfers exhibited varying degrees of complicity or compromise.

[97] Argenteuil is a commune in the northwestern suburbs of Paris and a sub-prefecture of the Val-d'Oise department.

Activity

The network operated through **multiple vectors**: the trafficking of forged administrative documents from Turkey, Greece, and Pakistan via DHL and FedEx; facilitation of irregular residence and illegal employment on construction sites; money laundering through a network of shell companies; and banking fraud through the opening of accounts under false identities. LTD1_R and LTD2_R provided a façade of legitimacy. C1_R oversaw the administrative and commercial aspects of the scheme, assisted on a daily basis by his brother, C2_R, who issued direct financial instructions. C3_R acted as the central intermediary for the distribution of documents and the execution of withdrawal orders. C5_R managed the reception of numerous Pakistani parcels via DHL. Undocumented foreign nationals were employed on construction sites, generally without any formal declaration.

Post-activity or post conditions

Financial investigations established that the network had operated in a structured manner since at least 2017, when the first money laundering activities linked to undeclared work were detected. During the network's operational period, several **indicators of infiltration** were identified. These included significant banking anomalies, with more than 150 accounts opened by a small group of individuals under multiple false European identities. Financial flows appeared incoherent, as alleged 'wage' payments from construction companies were received without any corresponding pre-employment declarations (DPAE). In addition, credited funds were systematically and immediately withdrawn, with no balances retained. Monthly withdrawals were estimated at approximately EUR 175,000 for C4_R and EUR 100,000 for C6_R. Logistic activity also appeared suspicious, with approximately fifty parcels sent from Pakistan since May 2020, addressed under varying identities to multiple locations across different departments in France, and consistently linked to female sender identities. An intensification of account openings and the use of forged documents was observed between January and October 2020. Furthermore, the organisational overview indicated a potential connection to a parallel proceeding involving the same individuals, although – at the time of writing – the precise relationship between the two matters remains to be established.

The **investigation** into the network was triggered by an anonymous tip received by the Central Office for the Suppression of Irregular Immigration and the Employment of Foreigners Without a Permit (in French: *Office Central pour la Répression de l'Immigration Irrégulière et de l'Emploi d'Étrangers sans Titre*) (OCRIEST). The case was referred to the OCRGDF for the money laundering aspect. Investigative measures included technical intercepts on several French and Italian mobile lines, with successive extensions, as well as physical surveillance and tracking. Cooperation with DHL enabled the interception and lawful opening of suspect parcels. Urban video surveillance and surveillance of the Fréjus tunnel cameras were also used, alongside the geolocation of telephone lines. The investigation ultimately led to a request for the opening of a judicial investigation, together with a recommendation to place the five principal remaining targets under interception and geolocation measures.

4. Financial profile of the criminal network involved in Case Romeo[98]

With regard to revenue sources, the network relied on **three interdependent financial pillars**:

- The sale of forged documents, which generated immediate direct income (approximately EUR 900 per Italian passport);
- Credit fraud, involving consumer loans obtained under false identities, immediately withdrawn and never repaid;
- The concealment of construction-related profits, as the network's companies systematically under-declared their actual earnings, a practice ongoing since at least 2017.

5. Harms caused by Case Romeo

Harms to individuals

People in precarious situations were forced to pay substantial sums (EUR 900 for a forged passport) to access employment or a substitute identity. Workers employed at the network's sites operated outside the legal framework, without insurance, pension rights, or occupational health protection. The network was also involved in the movement of three Pakistani children, although the available evidence does not indicate that they were intended to be integrated into the network. Instead, they were referred to child-protection services.

Harms to other businesses

The use of 'look-alike' documents, consisting of genuine documents belonging to physically resembling third parties, sometimes reported stolen in Spain, exposed the legitimate holders to potentially serious administrative and judicial consequences. Moreover, by employing undeclared labour and avoiding social contributions, the network's companies were able to offer lower rates than legitimate businesses. The criminal use of the construction sector also undermined trust between principals and subcontractors. Finally, DHL and FedEx had their infrastructure used for the clandestine transport of fraudulent materials, exposing them to legal risks and increased control costs.

Harms to public institutions

Alongside its effects on the social security system, prefectural authorities, and the judicial system, the proliferation of forged documents undermined the integrity of legal identity and complicated administrative checks. The network's presence across multiple regions created pockets of an underground economy beyond State oversight. By providing logistical support and prospects for undeclared employment, the network also facilitated clandestine migration routes across Europe.

[98] The Paris City Report contained no information regarding financing sources or start-up capital, payment methods and internal arrangements within the network, or the costs associated with business operations.

Annex 6.S – Case Sierra: Taxi Licence Laundering Scheme[99]

1. Criminal network involved in Case Sierra

The transnational criminal network involved in Case Sierra, specialising in drug trafficking, had been active for more than fifteen years. It comprised at least ten members, organised around a **core group of three brothers**. C1_S, the network's leader and second son, was incarcerated in Spain and directed import operations from prison via telephone. Previously convicted for trafficking offences in the 2000s, he had escaped custody at the end of the 2010s. His partner, C2_S, managed a substantial part of the laundering activities. C3_S, the first son, oversaw international transport operations and part of the laundering, while C4_S, the third son, ran the Île-de-France sales outlets. To maintain its position within the regional drug trade, the network routinely resorted to violence. Investigators and media reports documented conflicts over the control of dealing locations, at times involving military-grade firearms, including Kalashnikov-type assault rifles.

2. Legitimate businesses involved in Case Sierra

LTD1_S was a **taxi passenger-transport company** formally registered in Paris's fifth arrondissement, although its registered address was effectively no more than a mailbox. Established in November 2006, it was initially owned and managed by C5_S, the family patriarch at the centre of the network. Upon his death in March 2020, the business, valued at EUR 120,000, passed to his spouse and seven children through succession proceedings. C3_S subsequently acquired 60 shares for EUR 6,000 but resigned shortly thereafter. In May 2020, management was transferred to C6_S, who had no established familial links to the family. In March 2022, the company's capital structure was reorganised through a series of intra-family share transfers. C2_S was appointed manager and acquired a 50% stake, while the remaining shares were divided equally between C3_S and his son, C7_S.

Moreover, three additional companies were involved in financing the taxi licences:

- **LTD2_S**, registered as a short-distance road freight transport business, had no employees and operated from a fictitious registered office. Over a 19-month period (January 2022 – August 2023), its sole bank account recorded exceptionally high transaction volumes (EUR 3.46 million in credits and EUR 3.46 million in debits), consistent with the layering of illicit funds.
- **LTD3_S**, formally chaired by a frontman (a Moldovan national) who also received undeclared wages from a plastering company, was in practice controlled by another individual known to law enforcement. Over an eleven-month period, its bank account recorded more than EUR 1.039 million in credits and EUR 1.039 in debits. The company financed the acquisition of four taxi licences and one taxi for LTD1_S through eight cashier's cheques totalling approximately EUR 324,500.

[99] This case study was based on access to the judicial file, as well as interviews with the journalist who covered the case and with a financial investigator involved in the proceedings.

- **LTD4_S**, a Nice-based heating and insulation company operated by two brothers, financed EUR 140,000 of one taxi licence through a cashier's cheque and transferred a further EUR 356,000 to LTD2_S. Several of its bank accounts recorded transactions amounting to several million euros, consistent with the layering of illicit funds.

3. Crime script based on Case Sierra

Motivation – Purpose

The network had been involved in drug trafficking (cannabis, cocaine, and synthetic drugs). Its criminal use of a business to launder criminal proceeds served a dual purpose: protecting illicit funds from both rival theft and police seizure, and generating legitimate income through licence leasing that could be transferred more easily to Spain or Tunisia, the leaders' country of origin.

Preparation

The network exploited several vulnerabilities within the **private transport sector**. First, its familiarity with the industry – derived from the family's long-standing involvement – facilitated access to taxi licences and enabled the continued use of the deceased father's (C5_S) company and bank account. Second, the sector's continued acceptance of cash payments allowed illicit cash to be integrated into legitimate business turnover. More importantly, the acquisition of taxi licences provided an effective laundering mechanism. By purchasing licences with illicit funds, the network converted criminal proceeds into legitimate business assets while exploiting a regulatory weakness of the Paris system. Taxi licences were administrative authorisations issued by the police prefecture and could be transferred directly between drivers without mandatory notarial involvement or verification of the origin of the funds, unlike real-estate transactions.

Pre-activity or enabling conditions

Between February 2022 and April 2023, LTD1_S acquired ten parking authorisations for a total of EUR 1.49 million and became co-owner of thirteen taxis between September 2021 and August 2023. This rapid expansion was disproportionate to the company's underlying economic activity. LTD1_S's accounts were funded primarily through payments from individuals and corporate entities, which appeared to correspond to the leasing of licences and/or vehicles, amounting to approximately EUR 245,000.

The degree of culpability of the structure appeared to be total, as LTD1_S had effectively been set up for money-laundering purposes. In particular, the financing of the taxi licences raised significant concerns. Of the EUR 1.49 million invested, only around EUR 245,000 originated from the company's own resources through reinvested rental income. The remaining funds were provided by at least three companies with no apparent economic connection to the passenger transport sector.

Activity

In practice, the purported licence lessees were untraceable or fictitious. The companies involved had few or no clients, employed little or no staff, and maintained suspicious financial records. Funds were channelled through the taxi companies' accounts, returned to the leasing company, and subsequently transferred to Spain or reinvested in other legitimate commercial activities. Audio intercepts corroborated the laundering scheme and the use of frontmen. Moreover, the network had been

involved in drug trafficking (of cannabis, cocaine, and synthetic drugs) for at least fifteen years and operated within a dense distribution network.

Post-activity or post conditions

The leasing scheme operated for approximately two years before **judicial intervention**. Without investigation, no signs of infiltration had been apparent.[100] Nevertheless, the courts linked the acquisition of licences by traffickers with no identifiable legitimate income to rental payments ultimately transferred to Spain. On the night of 4-5 February 2023, following a tip-off and a vehicle pursuit, the police seized 330 kilograms of cannabis from a car, together with fuel receipts from a Spanish station, two sets of licence plates, and a GPS tracker. On the night of 7-8 February, the network broke into the vehicle pound and recovered a further 550 kilograms of cannabis that investigators had overlooked in one of the seized vehicles.

The preliminary investigation also established that C1_S had used a borrowed identity and his father's bank accounts to finance vehicle purchases and rentals between France and Spain. The leader's ability to evade arrest, resist law enforcement, orchestrate the burglary of a vehicle pound, and sustain a long-running transnational network, combined with its use of violence, diversified money laundering methods, local and political connections, and capacity to corrupt public officials, underscored the organisation's **high level of sophistication** and dangerousness. Following the arrests, the prosecutor referred the case to the Specialised Interregional Court (JIRS), and the asset investigation was subsequently assigned to the Interministerial Investigation Group (GIR; *Groupe Interministériel de Recherche)* of Essonne. In 2024, approximately fifteen individuals aged 20-40 were charged with drug trafficking, drug exportation, criminal conspiracy, and money laundering. According to the most recent available information, seventeen taxi licences had been seized by 2026, representing an estimated total value of approximately EUR 2.65 million. This figure excluded future rental income, estimated at approximately EUR 2,000 to EUR 3,000 per licence per month.

4. Financial profile of the criminal network involved in Case Sierra

Payment methods and arrangements within the network

The deceased father's accounts, which had never been closed, were actively used, recording around EUR 68,800 in credits and EUR 69,700 in debits on one account, and EUR 56,730 and EUR 56,750 respectively on the other. These accounts were funded by LTD1_S and LTD2_S and used to pay for vehicle rentals, air travel, and accommodation in Spain. The financial structure thus relied on shell companies handling substantial flows of funds (several million euros each), cashier's cheques, and cross-transfers designed to obscure the origin of the money, alongside a systematic externalisation of funds towards Spain, Tunisia, and Morocco.

[100] According to investigators, the company's growth over its first twelve months was highly anomalous. Within a year, it had acquired ten taxi licences worth approximately EUR 1.5 million and a joint ownership interest in thirteen taxis. Although licence prices had fallen by around 40% since 2014 following the emergence of VTCs, the company acquired its licences at the lower end of the market (EUR 80,000 to EUR 140,000). The purchase price of EUR 80,000 was considered substantially below market value, reinforcing the hypothesis that an additional cash payment had been made to the sellers.

Analysis of one seller's bank account revealed a series of **cash deposits** coinciding with the transfer of a taxi licence, amounting to approximately EUR 29,000 between March and April 2022. This finding supported the hypothesis that part of the purchase price had been paid in cash. Overall, cash deposits totalled approximately EUR 43,000. A discrepancy of approximately EUR 452,500 out of EUR 1.49 million remained unexplained by the bank transactions obtained, with two individuals additionally contributing EUR 44,000 and at least EUR 25,000 circulating in cash. Neither the authorities nor the banks filed any suspicious transaction reports. The inherited nature of the original licence appeared to have 'primed' the flow of rental income, lending it an outward appearance of legitimacy.

Costs of business operations

LTD2_S paid EUR 304,000 towards the acquisition of four taxi licences by LTD1_S, while also transferring EUR 195,000 and EUR 84,000 to French accounts linked to the family, EUR 72,000 in purported wages to C2_S despite having no employees, EUR 12,000 in school fees, and EUR 40,000 in holiday expenses. Furthermore, LTD3_S financed the acquisition of four of LTD1_S's taxi licences and one taxi through eight cashier's cheques, totalling approximately EUR 324,500. LTD4_S financed EUR 140,000 of a single licence via cashier's cheque and also credited LTD2_S with around EUR 350,000. Several of its accounts recorded transaction flows amounting to several million euros, consistent with the dilution of funds.

Revenues and proceeds

Between October 2022 and February 2023, the organisation is believed to have carried out at least eight 'go-fast' runs, transporting Moroccan cannabis to Île-de-France via Spain. The consignments were valued at approximately EUR 12 million to EUR 20 million at French wholesale prices. The network resold the drugs to semi-wholesalers and at retail level, while also sourcing cocaine in the Netherlands for onward resale in the Paris Region and in the Loiret (Orléans). Moreover, revenues were derived from the leasing of fictitious licences. As each licence generated EUR 1,500 to EUR 2,000 per month, ten licences yielded a monthly income of approximately EUR 15,000 to EUR 20,000.

The network's financial profile combined substantial illicit income with a near-total absence of declared income among the individuals involved. C1_S submitted no tax declaration and held no bank accounts or property in his name. C3_S and C4_S similarly declared no income or assets, relying partly on reported gambling winnings at the *Française des Jeux* (FDJ) and PMU Betting, totalling up to EUR 63,900.

5. Harms caused by Case Sierra

Beyond the resulting patrimonial harm, Case Sierra reveals distortions in the private-transport market, linked to the use of illicit capital, as well as institutional harm arising from shortcomings in prefectural oversight and established police corruption. It also contributed to the territorial consolidation of a violent network, resulting in broader social harm.

ANNEX 7

SOFIA

DETAILED CASE STUDIES

Annex 7.T – Case Tango: The Hammers

1. Criminal network involved in Case Tango

The criminal network involved in Case Tango was a highly **structured and hierarchical** organisation primarily involved in drug trafficking and distribution, as well as in violence, extortion, robbery, and intimidation. The organisation comprised more than thirty – predominantly Bulgarian – members, spread across various levels with separate roles and limited knowledge of the broader network structure, and many of them were linked to the 'Levski Sofia Zapad' football supporters' faction. The network's leader (C1_T) did not directly participate in or manage street-level drug sales, but exercised strategic oversight, resolved internal conflict, and intervened in serious matters affecting the network. Only four individuals were allowed to have direct contact with C1_T, reflecting the strict separation between leadership and mid-level operatives.

The network relied on a defined **division of labour**, enhancing both resilience and operational efficiency. Area managers were responsible for distributing drugs to lower-level dealers across designated regions in Sofia or in drinking establishments across the city. Dealers communicated exclusively with their superiors, from whom they received drugs and to whom they returned profits. Warehouse staff stored and packaged narcotics, whilst cashiers collected the revenues on a weekly basis, maintained financial records, and reported directly to senior management. In addition, a specialised 'punishment unit' – known as 'Chukovete' or 'The Hammers' – enforced discipline through abductions, beatings, and severe bodily harm, and was also authorised to distribute drugs. The network demonstrated its capacity to continuously recruit new members who all contributed to a shared objective of generating profit from drug trafficking and related criminal offences.

Interventions by law enforcement authorities from 2008 onwards resulted in charges, arrests, and the seizure of drugs, cash, and digital evidence. However, the network's upper echelons proved difficult to disrupt, with C1_T evading arrest in Dubai and successfully avoiding extradition despite an Interpol Red Notice. Subsequently, mid-level members were acquitted on appeal and allegedly remained active in the nightlife entertainment sector (Mediapool, 2017). Following intensive police investigation into the C1_T and his immediate subordinate, who acted as operational commander, the company's manager assumed leadership responsibilities in 2009.

2. Legitimate businesses involved in Case Tango

The legitimate business at the centre of Case Tango is a limited liability company (**LTD1_T**) that was formally active in Sofia's nightlife and entertainment sector. Although best known for operating major nightclubs, it was registered to carry out a wide range of additional activities, including construction and infrastructure services, domestic and international trade, hotel and tourism services, logistics and warehousing, leasing, consultancy, various production activities, and technical services related to beverage vending machines. According to the case files, its status in the public register remained 'active' throughout the relevant period. Between 2007 and 2009, the company itself employed between 30 and 42 people and reported a turnover of BGN 534,000 (EUR 273,000) in 2008 and BGN 28,000 (EUR 14,000) in 2009.

LTD1_T was a **limited liability company** (LLC) and, from 2012 onwards, a single-shareholder LLC. Importantly, the recorded owner and manager appeared in several other companies linked to the criminal group and co-owned or partnered with family members of the network's leader (C1_T). This overlap between legal ownership and criminal hierarchy created structural vulnerabilities that facilitated the blending of lawful and unlawful activities. The fact that a high-ranking member owned or controlled the company constituted a key enabling condition, both operationally and financially. Overall, the information in the case files suggested that the company was not merely a legitimate business but formed an integral part of the criminal network's operations, providing infrastructure, cover, and revenue channels that were essential to its activities.

Even after the network had been dismantled, its **legitimate business operations** continued. The companies no longer managed clubs in Sofia but shifted the focus of their main operations to the Black Sea Coast, where they also managed similar establishments. The businesses also adjusted their ownership structure, and the shareholders who were the subject of a criminal investigation were replaced by new shareholders (Mediapool, 2017). The business model in which nightclubs are used as distribution channels for drugs also persists and is actively employed by other criminal networks, as evidence by targeted police raids on nightclubs in Sofia (Stanchev, 2024).

3. Crime script based on Case Tango

Motivation – Purpose

The primary motives for using the legitimate business were to provide a legitimate façade for the network's criminal activities, to facilitate and expand its drug trafficking operations, and to launder illicit proceeds. Nightlife establishments owned or controlled by network members (particularly those under LTD1_T) enabled direct and routine access to a large customer base, providing an ideal environment for the distribution of narcotics. The purpose of exploiting the business was therefore twofold: to conduct **drug sales** within a high-traffic and low-surveillance setting, and to **launder the proceeds** of criminal activities by mixing them with the lawful turnover generated by the venues. The legitimate business (LTD1_T) was directly linked to the network's organised crime activities in the distribution and money laundering stages of the criminal process. It provided a platform for the distribution of drugs at retail level and served as a conduit through which illegal proceeds could be channelled into the network's structured accounting system.

Preparation

The nightlife sector in Bulgaria has traditionally attracted criminal finance since the early 1990s, with a significant level of criminal use of the sector.[101] Many popular clubs have been associated with notorious criminal figures and criminal network, whilst nightlife venues have been identified as favoured channels for the distribution of drugs, particularly cocaine and amphetamines (CSD, 2020). However, there is no publicly available information that allows to assess the extent to which legitimate

[101] In total, the hospitality sector in Sofia comprises 2,777 licensed restaurants and entertainment venues, of which 307 are registered as bars and nightclubs. Around 45% of the businesses in this sector are based in Sofia due to the high purchasing power of the capital's population, which amounts to approximately EUR 1.25 to 1.4 billion. Nightlife venues account for around 10 to 15 percent of the sector's turnover, or between EUR 175 million and EUR 200 million (Goranova, 2018).

businesses in this sector are being used for criminal purposes, or whether this is increasing or decreasing.

The nightlife establishments offered **numerous opportunities** which the criminal network deliberately targeted. First, they enabled its members to interact with customers in a natural and discreet manner, thereby leveraging the anonymity and dense crowds that characterise such venues. Furthermore, the company's businesses – already under the ownership or management of senior network members – provided an operational advantage by removing the need for external infiltration. The broader economic subsector exhibited similar characteristics: limited oversight, high cash turnover, and an environment conducive to blend lawful and unlawful revenue streams. These characteristics made nightlife venues particularly suitable for covert drug distribution and the laundering of small-scale proceeds.

Pre-activity or enabling conditions

The degree of criminal use of the legitimate business was substantial. The case files show that high-ranking members both facilitated drug distribution and directly received revenues generated within the nightclubs. Lower-level members were formally employed in these establishments, providing additional cover and enhancing the network's ability to conceal its activities. This suggests that the company was deliberately established by the network's leaders to facilitate criminal activities, functioning not merely as a passive setting but as an **integral component** of their operations.

Activity

During periods of active criminal use, the legitimate business (LTD1_T) formed part of the network's broader management structure. Drug distribution within the nightlife establishments followed its **hierarchical command structure**, with area managers supplying dealers and overseeing regional territories. Dealers sold drugs exclusively to customers within their allocated territories and handed over all their profits to their supervisors. At an operational level, the network initially used distinctive holographic packaging ("VIP" or "ORIGINAL") to brand its products but subsequently switched to untraceable packaging in response to pressure from LEAs. The *modus operandi* was based on communication with customers, either in person, by telephone or via intermediaries, using code words and passwords to specify the type of drug involved.[102] Profits were transferred weekly from higher-level dealers to designated cashiers, who maintained written records and reported to the leadership. Furthermore, the 'punishment unit' maintained discipline through violence and intimidation, thereby ensuring compliance at all levels. The management and *modus operandi* within the legitimate business thus mirrored the broader organisational structure, characterised by centralised leadership, strict reporting channels, and clearly defined territorial control.

Post-activity or post conditions

The case files suggest that the legitimate companies owned by high-ranking members were used for criminal purposes throughout the network's period of operation (2007-2010). **Indicators** of criminal use were evident in the overlap between ownership structures and the criminal hierarchy, the use of employment contracts for lower-level members, and the flow of illicit proceeds through business-linked channels. Law enforcement intervention intensified from 2008 onwards. After being charged

[102] The criminal use of legitimate businesses facilitated the commingling of legal and illegal revenue streams, although the case files provided no further detail on specific laundering methods or investments.

with establishing and leading the criminal network, the leader (C1_T) withdrew from visible leadership and went into hiding. Subsequent **investigative actions** resulted in search and seizure operations, the arrest of several members, and the confiscation of drugs, cash, digital devices, and written records. Arrest warrants were issued, several members were declared wanted, and others were convicted. Although substantial evidence was gathered, key figures (including C1_T) evaded arrest and remained beyond the reach of extradition, preventing the network's complete dismantling. Moreover, the group's legitimate business structures remained intact, continuing to operate after the network's dismantling through changes in ownership and the relocation of their principal business activities to the seaside. The underlying business model also appeared to persist, although the links between legitimate commercial activity and criminal operations became increasingly obscured, making detection and evidentiary proof considerably more difficult.

4. Financial profile of the criminal network involved in Case Tango

Financing sources and start-up capital

The origin of start-up capital was not explicitly stated in the case file, although it suggested it was likely derived from the leaders' existing legal or criminal businesses.

Payment methods and arrangements within the network

LTD1_T generated significant legitimate turnover, as it operated several popular nightlife venues in Sofia and at the Black Sea Coast. As a substantial proportion of the legitimate payment transactions were made in cash, this provided an easy avenue for blending licit and illicit cash and laundering the proceeds of drug trafficking. Revenue collection followed a hierarchical process, with higher-level dealers transferring weekly profits to designated cashiers responsible for maintaining written accounts, auditing drug quantities, and reporting directly to senior leadership. One of the witnesses stated that he collected all proceeds, kept detailed financial records, and passed the money on to the operational commander (the second-in-command within the network's hierarchy), who personally checked the accounts and corrected any errors. Financial transactions were primarily conducted **in cash**.

Costs of business operations

The case file indicated that costs associated with the network's activities were **unspecified**, with no information on formal financial outlays or operational expenditure beyond general references to payments such as salaries for members of the 'punishment unit'.

Revenues and proceeds

The financial aspects of the criminal network, as described in the case files, reveal the existence of a structured and centralised system for generating, collecting, and managing illicit revenues. The primary source of income was **drug trafficking**; the case files state that in 2008 alone, the network sold approximately two kilograms of cocaine per month at a price of BGN 85 per gram (EUR 43), which generated approximately BGN 170,000 (EUR 87,000) per month from cocaine sales. This figure reflects only part of the network's narcotics portfolio, which also included amphetamines, cannabis, and heroin. During searches, law enforcement authorities recovered a metal safe containing approximately EUR 6960, as well as drugs, notebooks with coded financial information, and digital devices, including a computer, flash drive, and compact disc containing data relevant to the network's operations. Asset confiscation and seizure formed part of the financial investigation; however, the case files provide no further information on the broader process of tracing, recovering, or freezing assets.

5. Harms caused by Case Tango

Harms to individuals

The criminal use of nightlife establishments caused several forms of harm to individuals frequenting these venues. The widespread availability of drugs increased the risks of addiction, overdose, and drug-related physical harm, while contributing to the normalisation of substance use. Customers, often unaware of the extent of the underlying criminal activities, were thereby exposed to heightened vulnerabilities. Moreover, individuals were indirectly exposed to the network's violent enforcement methods, including beatings, intimidation, and, in some cases, severe bodily harm.

Harms to other businesses

Other businesses within the nightlife sector were also negatively affected. The involvement of the network's clubs in large-scale drug distribution risked damaging the reputation of legitimate venues operating in the same subsector. The association of nightclubs with criminality and drug trafficking contributed to repeated police raids, discouraged patrons, generated distrust, and undermined the commercial viability of businesses not involved in illicit activities.

Harms to public institutions

Although the case file provides no evidence of direct harm to public institutions, the criminal activities placed an indirect strain on law enforcement and institutional capacity, requiring extensive investigative efforts, resource-intensive operations, and cross-border coordination in relation to arrest warrants and extradition.

Harms to the social environment

The integration of drug trafficking into mainstream nightlife venues contributed to the normalisation of criminal behaviour in public entertainment spaces. The ease of access to narcotics in these settings likely increased drug use, influenced social norms, and fostered an environment in which criminal activity became embedded in everyday leisure contexts. This blurring of the boundaries between licit and illicit activity further strengthened the criminal network's presence and influence within the local nightlife scene.

Annex 7.U – Case Uniform: Quick Credits

1. Criminal network involved in Case Uniform

The criminal network involved in Case Uniform operated on the basis of a clearly defined division of responsibilities, spread across six functional roles. The **leader** exercised overarching oversight and provided a legitimising presence, appearing at key confrontations to reinforce his hierarchical authority. His role was primarily supervisory, serving as a source of symbolic authority across the network of offices rather than engaging in operations. The leader was assisted by a number of '**operational managers**' who oversaw day-to-day operations in the four offices. They served as the primary point of contact for debtors, managing telephone-based intimidation, coordinating visits to homes and workplaces, overseeing loan origination, and directing enforcement activities.

Furthermore, several individuals acted as '**enforcers**', directly subjecting debtors to violence in remote locations, including physical assault, electric shocks, and degrading treatment. They were typically deployed as a last resort when financial pressure and verbal threats proved ineffective. The enforcers were formally employed as credit consultants by LTD1_U. One also served as the company's registered owner, through which the lending operation was conducted. The network further included a '**recruiter**' and intermediary who, although not formally employed by LTD1_U, referred financially vulnerable individuals from the local community to the lending office. His presence during at least one violent incident further suggests that he acted as an informant, relaying information about debtors' circumstances to the network.

The investigation further revealed the involvement of '**administrative support members**' who were formally employed as credit consultants, responsible for handling paperwork, filing contracts, and making routine reminder calls to clients. Although apparently removed from direct violence, their role provided the administrative legitimacy that lent credibility to the operation. The legitimate business structure mirrored the criminal hierarchy, with office managers serving as group leaders and employees formally designated as credit consultants while, in practice, performing enforcement functions for coercive debt collection. Taken together, the network integrated legal incorporation, operational management, coercive enforcement, administrative legitimacy, and community-level recruitment into a cohesive predatory lending enterprise in which legitimate business functions and criminal enforcement were inseparable.

2. Legitimate businesses involved in Case Uniform

The network involved in Case Uniform established and operated several legitimate businesses to facilitate loansharking and extortion under the disguise of a **payday lending business**, operating under the brand "Quick Credits". The brand was used by multiple franchisees providing short-term consumer credit in Bulgaria.[103] It was not a legal entity and was not registered in neither Bulgaria's Commercial Register nor the National Bank Register. Although the brand was used across several locations, its presence was largely confined to Sofia and the surrounding region. One such franchisee, **LTD1_U**, operated offices at four locations in Sofia. Open-source information suggests that at least three additional companies used the "Quick Credits" brand. None held licences from the National Bank to operate as financial lenders, and the franchisor of Quick Credits was a licensed non-bank financial company based in Pernik. The franchisor's level of culpability remains unclear, as does its awareness of franchisees' involvement in extortion.

The legitimate arm of LTD1_U was registered in 2023, with a single individual formally listed as owner. The company operated as a single-member LLC. The owner and three associates collectively managed **four Quick Credits offices** – located in Lyulin, Nadezhda, and Bozhurishte, with a main office in Obelya – in Sofia, each overseeing one site. These four core members of the network served as 'office managers' across the locations, responsible for daily operations, including financial management and

[103] '**Fast credits**' or 'payday loans' are forms of unsecured, small-value lending typically provided to individuals requiring immediate financial assistance. In Bulgaria, approved funds are disbursed within a matter of hours of the application, either in cash or directly into the borrower's bank account, with loan approval generally processed rapidly. As in other countries, payday loans are typically sought by individuals seeking to cover essential monthly expenses, such as food and household bills, when regular income is insufficient to meet their financial obligations (TREND – Research Centre, 2023). This issue becomes particularly pronounced during periods of austerity, high inflation, and cost-of-living crises (Booth, 2018).

debt collection. Their duties included securing loan repayment through intimidation, coercion, and, where necessary, violence. One victim identified a different core member as the *de facto* leader of the network, despite formal ownership of the business being attributed to another of the four. The network employed at least ten employees, with an unknown number of credit consultants. Like other providers of payday loans, Quick Credits' franchisees provided quick 'fast credits' with minimal paperwork, few questions askes, abnormally high interest rates, and associated high risks for potential clients. However, its offices had attracted particular notoriety due to their association with the use of violence in the collection of issued loans. The Quick Credits office in the Obelya residential district of Sofia served as a notable example of this criminal activity.

3. Crime script based on Case Uniform

Motivation – Purpose

The primary motivation of the criminal network involved in Case Uniform was **profit**. Violence and extortion were not ends in themselves but a means to that end. However, direct income from short-term lending was not the sole driver, as the structuring of the criminal operation around a legitimate business entity provided additional advantages, including a credible façade for criminal activity, reduced exposure to law enforcement scrutiny, and a vehicle for integrating illicit funds into the legitimate economy. There is no indication that the network sought to exercise territorial control or that the cohesion among its members was based on shared social, cultural, or ideological ties.

Preparation

By franchising Quick Credits offices, criminal networks operating under the guise of legitimate businesses, such as LTD1_U, gain significant opportunities for illicit profit. The operational structure and functioning of the **payday lending sector** provide criminal networks with opportunities to exploit it for illicit gain, effectively disguising loansharking as legitimate money lending while preserving its core elements, including debt entrapment through excessive and escalating interest rates, coercive debt collection, and the financial exploitation of vulnerable borrowers (Kojouharov & Rusev, 2015).

According to police officers familiar with the criminal use of legitimate financial institutions, payday lenders such as Quick Credits can facilitate the **laundering of proceeds** from other criminal activities, including drug trafficking. A common method for 'laundering via loans' involves criminal actors posing as clients of credit providers. For example, a drug dealer may obtain a formal loan using fraudulent documents or a shell company, and subsequently repay it with 'black cash' obtained through illegal activities, thereby rendering the illicit funds ostensibly legitimate. Alternatively, payday lenders may be established as front businesses, issuing fictitious loans to legitimise illicit funds. In this way, criminal networks can also function as providers of 'laundering-as-a-service' to other criminal actors. However, as noted by several interviewees, these aspects of Quick Credits franchisee operations were not specifically examined in the pre-trial investigation.

A major vulnerability in Bulgaria's payday lending sector arises from the systematic use of opaque and **misleading contract terms**, combined with weak and largely ex-post enforcement mechanisms. Payday lenders characterised by little regulatory oversight, minimal scrutiny by LEAs, and significant legislative loopholes provide opportunities to take advantage of financially vulnerable individuals (cf. *infra*). Although loans typically range from EUR 250 to EUR 500 with stated interest rates of 12-20%, contracts often obscure or conceal additional terms, including excessive processing fees and punitive charges for

late payment. Consumers are often unable to understand or meaningfully assess these terms at the point of signing. By entrapping borrowers through short-term, high-interest loans, debtors may ultimately repay 150-300% more than the original loan amount. Exorbitant default interest and punitive late-payment charges are common, generating substantial profits for 'fast credit' providers such as Quick Credits. Such coercive enforcement typically involves beatings, harassment, and threats of arson, rape, and death.

Bulgaria's **consumer protection law** prohibits unfair terms in principle, but the protection of customers against such clauses is complicated by two interrelated factors. First, legislators in Bulgaria have been slow to respond to emerging abusive practices. Many concealed clauses in payday loan agreements undermine consumer rights and are reinforced by misleading promotional messaging. Some estimates suggest that up to 90% of fast loan providers breach consumer protection rules (BNT News, 2023). Second, in cases of outright illegality, enforcement bodies such as the Bulgarian Consumer Protection Commission lack the authority to immediately invalidate abusive clauses or suspend their application through administrative action (Georgieva, 2025). Instead, it must rely on fines and lengthy court proceedings, which often occur only after consumer harm has materialised. This regulatory design incentivises non-compliance, allowing lenders to continue unlawful or borderline practices while sanctions are delayed, contested, or absorbed as a cost of doing business. The result is a structural imbalance in which borrowers bear immediate financial risk, while legal remedies remain slow, uncertain, and inaccessible to many affected individuals.

Another opportunity for both the legitimate businesses themselves and the wider subsector of non-bank financial lenders is the significant number of individuals in **economically precarious situations** who may be in need of urgent financial support. As noted above, individuals with poor credit histories or an urgent need for finance may be unable to obtain bank loans, either because applications are processed too slowly or are rejected due to unstable incomes or adverse credit records. Payday lenders are therefore particularly attractive to lower-income borrowers. In Bulgaria, payday loan providers are widely criticised for exploiting individuals with gambling or substance use disorders, as well as those from socioeconomically vulnerable communities (Kandilarov, 2025). The continued presence of such vulnerable groups therefore presents another significant opportunity for criminal networks.

Despite the vulnerabilities provided by the sector, the provision of 'fast credit', including payday loans, is lawful in Bulgaria and regulated by the Bulgarian Law of Consumer Credit Protection.[104] However, the legislation contains a significant loophole that can be exploited by criminal networks. Specifically, loans with a term of less than three months and a value not exceeding BGN 400 (approximately EUR 200) fall within this **regulatory gap**. Up to 2026, loans falling within these thresholds fell outside the scope of the Bulgarian Law of Consumer Credit Protection. As a result, they were not subject to interest rate caps, constraints imposed by the Consumer Credit Act (2010), or strict licensing requirements, and offered minimal consumer protection (Trifonov Law Office, 2012). This legal loophole created significant scope within the legitimate economy for criminal networks and predatory lenders to

[104] As of February 2026, the non-bank financial sector in Bulgaria comprised 262 companies (BNB, 2026). Compared with 190 firms in 2025 and 174 in 2024, this indicates continued **sectoral expansion**. Many of these companies are situated in Sofia. Collectively, they hold approximately BGN 8.6 billion in assets (around EUR 4.3 billion). Just over half of these assets are owed by households, amounting to roughly BGN 4.875 billion (approximately EUR 2.46 billion), of which BGN 4.718 billion consists of consumer loans (approximately EUR 2.41 billion) (Kostov, 2025).

operate, often using ostensibly legitimate businesses as cover for extortion. In combination with extortion, violence, and 'crime-as-a-service' operations, this constitutes a significant case of criminal infiltration of Sofia's licit economy. The adoption of the Law on Credit Servicers and Credit Purchasers in June 2025 closed this loophole. However, some existing companies appear to have continued predatory lending practices by issuing part of their loans without formal contracts (GlasNews.bg, 2026).

In Sofia, the payday lending sectors appears to be of more importance than elsewhere in the country. Most notably, larger and more densely populated areas generate greater demand for such services, and Sofia's large economy intensifies competition among service providers for potential clients. Furthermore, the higher cost of living in Sofia, elevated inflation, and more competitive labour markets are likely to increase households' demand for short-term loans to meet urgent needs. Another factor that increases the **importance of this subsector in Sofia**, and thus its appeal to potential clients (and victims), is the capital's demographic composition. Sofia has the lowest median age of any city in Bulgaria and a population with greater variation in income stability. Owing to their comparatively precarious economic circumstances, young people are more vulnerable to high-cost lenders and loan sharks, a trend that has been further exacerbated by the effects of the COVID-19 pandemic. Indeed, the number of individuals under the age of thirty obtaining loans from unlicensed lenders via social media is increasing, a trend that extends well beyond Bulgaria (Evans, 2021).

Pre-activity or enabling conditions

The significant opportunities for criminal use within the broader economic subsector naturally create scope for criminal networks to exploit legitimate businesses operating in the sector. The unregulated and often exploitative practices associated with many payday loan operators represent one form of problematic economic activity in Bulgaria. However, as demonstrated by the Quick Credits franchisee network, ostensibly legitimate businesses within this sector may also be appropriated for entirely criminal purposes. In this case, the franchise companies operating the offices – particularly the Obelya office – were established primarily to facilitate criminal activities and functioned largely as **front companies**. The legitimate business structure mirrored the internal organisation of the criminal group: the office manager simultaneously served as the group's leader, while employees performed operational and enforcement roles within the broader criminal scheme.

The brand recognition of "Quick Credits" and the use of legitimate and widely recognised services as part of the process provided criminal actors associated with the franchisee network with a veneer of legitimacy. The opportunities outlined above (cf. Preparation) represent key enabling conditions for the criminal operations that have infiltrated companies such as Quick Credits. However, such infiltration would not have been possible without a **degree of culpability** on the part of legitimate, licensed payday loan organisations. It is believed that Quick Credits operators knowingly granted franchise rights to individuals engaged in criminal activity, or to persons known to have links to organised crime, allowing them to establish and manage franchise offices (Safe News, 2024).

Activity

The criminal network's activities were systematically embedded within and concealed by a nominally legitimate fast-loan operation, in a manner intended to place them outside the scope of the Consumer Protection Act. During its period of active criminal operation, the network functioned in a manner analogous to legitimate Quick Credits payday loan franchises, with its offices formally operating under a lending licence held by a registered parent lending company, and LTD1_U acting as a cooperation partner responsible for managing the physical premises. This arrangement provided a **veneer of legality**: clients signed written loan agreements, repayments were processed through a standard payment platform using reference codes, and employees were engaged under formal labour contracts with associated social security contributions.

However, these legitimate business functions served as a direct **vehicle for criminal activity**. Loan arrangements with clients were generally initiated through verbal agreements conducted at the office. Following an identity verification check, the terms of agreement were formalised in a written contract, which clients were subsequently required to sign. However, the credit consultant role provided access to borrowers' personal data, with identity documents being photographed and retained without copies being provided to clients. Furthermore, these written contractual terms systematically diverged from verbal agreements, imposing substantially higher and more frequent repayment obligations than those disclosed during the initial discussions.[105] Once this process was completed, office employees would travel by car to the client's registered address to conduct address verification, after which the agreed loan amount was delivered to the client. Clients rarely received a copy of the signed agreement.

Repayments of loans were typically collected through "Easypay" (a Bulgarian financial payment service) using the company's CIN number, although some clients were reportedly instructed to transfer payments directly to the personal identification numbers (Uniform Civil Number; EGN) of individual employees, outside the company's official payment structure. When a repayment was missed or delayed, the office typically contacted the client by phone to issue an initial reminder. The network employed a structured **escalation model for debt collection**. This began with persistent, often abusive phone calls to the debtor. If these failed to secure payment, contact was extended to family members, friends, and employers, while physical visits to the debtor's residence were also undertaken.[106]

When these measures proved ineffective, the group escalated to **systematic violence**, including beatings, abduction, psychological abuse, and threats of rape, arson, or murder. The severity of the abuse increased as repayment delays became more prolonged. The consistency of these methods across multiple offices indicated coordinated operational practices aimed not only at securing financial gain but also at deterring victim from cooperating with law enforcement authorities. By incorporating violence into its business model, the network caused severe physical, psychological, and economic harm to victims, while simultaneously undermining public trust in institutions and contributing to the

[105] A typical **contractual arrangement** used by the Obelya office involved a weekly interest rate of 10%. For example, a EUR 300 loan incurred an additional EUR 30 in weekly interest, with no defined repayment term beyond the requirement that "the interest is paid". Larger loans involved weekly repayments of several hundred euros (e.g., EUR 250 per week on a principal amount of EUR 2,500). These arrangements often differed from the terms verbally agreed with office employees. Nevertheless, clients were pressured into accepting the written agreements or complied due to their financial circumstances.
[106] In one documented case, employees visited a victim's mother's apartment, persuaded her to contact her son, and arranged a meeting under false pretences. In another case, a pregnant partner was threatened over the phone with being 'cut up', after which individuals arrived at the couple's residence, forcing her to contact emergency services.

normalisation of coercive practices within the lending market. Debt entrapment through excessive and escalating interest rates, combined with extortion and violence, therefore constituted an integral component of the enterprise's business strategy.

Post-activity or post conditions

The legitimate business had operated since at least 25 August 2023, the date on which the franchisee company was registered. This indicates approximately 13-14 months of documented criminal activity prior to the initiation of the criminal proceedings in October 2024. The systematic nature of the group's *modus operandi*, reflected in the consistency of practices across four office locations, standardised debt-collection escalation procedures, and coordinated use of violence, suggests that these activities had been in place since the network's inception.

The criminal use of the legitimate franchisee company exhibited several distinct **indicators of illicit activity**. The most immediate and apparent indicator concerned the discrepancy between written contracts and verbal agreements, which were imposed on clients through coercive means. While legitimate fast-credit providers operating in Bulgaria may employ aggressive contractual terms within the boundaries of the law (including through the exploitation of existing loopholes), the deliberate creation of two divergent sets of obligations – one documented for the purposes of nominal compliance and another enforced through coercion – suggested a calculated criminal design. The network's operational structure provided a further indicator. Although the four 'core members' each managed individual locations with apparent autonomy, the coordination of enforcement activities involving multiple 'enforcers' indicated a level of organisational sophistication beyond what the decentralised structure might initially suggest. Furthermore, the ambiguity surrounding the network's ultimate hierarchy – particularly the contrast between witness accounts and formal ownership records – may have reflected a deliberate attempt to obscure command structures and lines of responsibility.

Another indicator of the criminal exploitation of this structure is evident in the **financial practices** employed by the network. The use of personal identification numbers (EGNs) for direct payments to employees in certain cases demonstrated the diversion of funds outside formal accounting channels, while the use of legitimate Easypay systems may have served to reinforce an appearance of legitimacy. These practices, combining the use of legitimate financial services with transfers to personal accounts via EGNs, suggested systematic efforts to obscure financial flows and potentially facilitate money laundering. Furthermore, the consistent approach to escalating **violence and intimidation** not only indicated deliberate criminal infiltration but also demonstrated the tactical use of coercion to suppress victim cooperation with law enforcement.

Despite these efforts, **criminal proceedings** against the network were formally initiated by the Sofia Directorate of Internal Affairs on 1 October 2024, under the supervision of the Sofia District Prosecutor's Office. The case was opened under Article 213a of the Bulgarian Penal Code, which addresses extortion through the use of force or threats to obtain financial benefit. This legal classification reflected the assessment that the conduct in question extended beyond aggressive debt collection and constituted criminal extortion, highlighting the organised and profit-driven nature of the enterprise.

The investigation revealed several significant **enforcement challenges**. First, as noted previously, the legal framework governing the fast-credit sector in Bulgaria contains regulatory loopholes that create opportunities for criminal exploitation while making it difficult for law enforcement authorities to distinguish between aggressive, yet lawful, lending practices and organised criminal exploitation. For example, intimidating phone calls to borrowers could be interpreted merely as harassment arising from an alleged debt default rather than as evidence of extortion. As a result, enforcement action is often delayed. A further challenge arose from the network's systematic intimidation of victims. As discussed above, the Consumer Protection Commission lacked the authority to initiate proceedings proactively against coercive or exploitative lending practices. The network exploited this limitation by using explicit threats of escalating violence to discourage victims from reporting offences or cooperating with law enforcement. Such intimidation extended beyond borrowers themselves to their family members, creating additional disincentives to lodge formal complaints.

Despite these challenges, the police were ultimately able to intervene to a limited extend. Following requests for permission, officers conducted **searches** of the offices associated with the enterprise, as well as searches of the accused individuals. These searches yielded evidence that enabled investigators to reconstruct the network's operations, including incriminating material recovered from the suspects' mobile phones (e.g., videos). Aside from these searches of the premises and individuals connected to the scheme, there were no reported instances of direct confrontation with law enforcement.

4. Financial profile of the criminal network involved in Case Uniform

Financing sources and start-up capital

According to interviews and the judicial files, the network's declared start-up capital amounted to BGN 200 (approximately EUR 100), shared equally between the two officially registered owners. The investigation did not examine the origin of the company's working capital or establish whether it derived from a demonstrably lawful source.

Payment methods and arrangements within the network

Interviews indicated that 'credit consultants' employed by Quick Credits received a monthly salary of approximately EUR 1,250. However, the remuneration of branch managers remained unclear, and the available evidence did not indicate whether members of the network received bonuses or other financial incentives for activities involving the intimidation or assault of debtors.

Loan amounts issued by Quick Credits were distributed exclusively **in cash** rather than through traceable banking channels. Repayments, including interest and associated charges, were typically made via Easypay, with clients referencing their full name, personal identification number (EGN), and the relevant loan instalment. However, there were also reported instances in which payments were directed through the personal EGNs of individual employees rather than to the Quick Credits offices, thereby obscuring financial flows. Written contracts were deliberately structured to create the appearance of compliance with consumer protection legislation, while the actual lending arrangements were governed by verbal agreements imposing excessive interest rates and coercive repayment obligations.

Revenues and proceeds

The primary motivation underpinning the network's activities was **financial gain**. Revenue was derived principally from excessive interest rates imposed on loan agreements and enforced through the threat or use of violence. According to the case file, the standard interest rate was 10% per week, although this appears to have increased where repayments were delayed. Violence and intimidation were also used to coerce victims into taking out additional loans, thereby generating further revenue through continued interest payments. In addition, arbitrary fees were imposed on an *ad hoc* basis, often following missed repayments or the filing of complaints with the police. These practices further increased the network's profits.

5. Harms caused by Case Uniform

Harms to individuals

The clearest harms arising from the criminal operation were inflicted on seeking fast credit from the "Quick Credits" offices managed by the franchisee. Violence and other forms of abuse formed a structural part of the operation, with the harms inflicted on victims escalating in a calculated manner to secure timely repayment. This typically began with psychological and emotional intimidation, including threatening phone calls and visits to clients' homes intended to cause stress and unease. When these measures proved ineffective, threats were extended to family members, friends, or employers, including banging on doors and the placement of stickers. These measures reinforced the perception that violence could be enacted at their homes and further intensified the psychological pressure.

When threats and intimidation failed to secure repayment, creditors from Quick Credits escalated to systematic physical violence. Documented tactics included abduction, beating, humiliation, torture, and the recording of abuse, as well as the use of tasers and coercion into degrading acts. Victims were also warned against contacting police, threatened with further increases in their debt, and subjected to threats against family members, including arson, rape, and murder. The violence followed a consistent and controlled pattern across cases, suggesting an organised enforcement strategy rather than opportunistic abuse. Taken together, the network used systematic form of coercion intended to enforce repayment through harassment, intimidation, and violence.

Harms to other businesses

The reinforcement of debt cycles and accumulation of further debt among citizens of Sofia may also have affected local economy by reducing disposable income available for other expenditure. The network's activities may have further damaged the reputation of the non-bank lending sector, potentially discouraging the public from using such services. Moreover, the systematic use of intimidation and violence within a formally legitimate business context blurs the boundary between lawful economic activity and criminal coercion, which increases the risk that similar practices spread within the informal and semi-formal lending sector. Together, these effects contribute to a broader climate of fear and insecurity and may make Sofia a less attractive location for investment.

Harms to public institutions

The activities of the criminal network resulted in the erosion of public trust in the institutions of Sofia. Despite instances in which LEAs acted in accordance with the law, their perceived failure to disrupt the network's extortion activities may have weakened public confidence in their ability to protect citizens and maintain law and order. In particular, instances in which individuals visited a victim's apartment but left before the police arrived may have further contributed to perceptions of limited institutional effectiveness.

Harms to the social environment

The activities of the criminal networks also contributed to a broader climate of fear and the normalisation of violence. Media coverage of violent incidents extended their impact on direct victims and may have contributed to perceptions that Sofia is unsafe and that LEAs are ineffective. This, in turn, may have discouraged victims and potential witnesses from cooperating with the authorities, further weakening civic engagement. The social harm was also reflected in the vulnerability of the individuals targeted by the network's lending scheme. People in precarious financial situations, including those facing gambling or substance-abuse problems or unexpected financial pressures, were particularly exposed to exploitative lending practices. Rather than alleviating financial difficulties, these loans often reinforced cycles of debt and insolvency through hidden costs or forced entry into new loan agreements. The limited ability of State institutions to protect vulnerable groups and help individuals escape such cycles may have further undermined public confidence in those institutions.

Annex 7.V – Case Victor: Lords of the Dust[107]

1. Criminal network involved in Case Victor

The criminal network operating within Sofia's construction waste sector was organised around a **central intermediary** (C1_V) responsible for coordinating illegal dumping operations. He owned three legally registered companies officially engaged in the transport and disposal of excavated soil and construction activities. Through lease agreements with landowners, he secured access to unused land on Sofia's outskirts and coordinated with transport company owners, site managers, and allegedly complicit municipal officials to facilitate the illegal disposal of excavated soil and construction waste (ACF, 2024). C1_V also ensured a steady flow of waste into this parallel disposal system, while the construction sector's reliance on multiple layers of subcontracting enabled the scheme to operate with limited scrutiny. To conceal the illegal dumping, he further attempted to create a veneer of legality by forging a land-reclamation permit purportedly issued by the Ministry of Agriculture.

The other key members of the network were **transport company operators** who controlled truck fleets and maintained contractual relationships with construction companies. Investigative findings indicated that many companies involved in the removal of rubble and construction waste from building sites in Sofia were involved in the illegal dumping scheme (ACF, 2024). Although no official statistics exist on the number of companies providing such services, the Sofia Municipality Inspectorate estimated that approximately 10-15 such operators were active in the city. These actors coordinated with the organiser

[107] The analysis of Case Victor draws on an extensive media investigation conducted by a Bulgarian civil society watchdog organisation specialising in anti-corruption, supplemented by interviews with representatives of the Sofia Municipal Inspectorate.

to divert waste away from the authorised 'Vrazhdebna landfill' towards unregulated dumping sites on the western outskirts of Sofia. Drivers transported and unloaded waste at locations leased from **landowners** who, in many cases, paid little regard to the subsequent use of their land. Some further contributed to the appearance of legitimacy by declaring that the excavated soil was intended for land levelling.

Rather than operating as a unified hierarchical organisation, the illegal dumping system consisted of a **flexible network** of interconnected actors, including waste disposal and transport companies (cf. *infra*), landholders, and facilitators, linked by shared economic interests and sustained by continuous construction demand. This structure enabled operational resilience over an extended period and facilitated the continuous generation of illicit profits. The scheme's operation across hundreds of unregulated dumping sites spanning Gorubljane, Suhodol, Botunez, Lyulin, Bistritsa, Bankya, and Pancharevo demonstrates its geographic reach and organisational sophistication, effectively functioning as a parallel waste management system serving a substantial segment of Sofia's construction sector (ACF, 2024).

2. Legitimate businesses involved in Case Victor

The legitimate businesses at the centre of Case Victor were **waste transport and disposal companies** operating within Sofia's construction sector.[108] These companies were registered to provide excavation, transport, and waste disposal services for residential and commercial construction projects. Their lawful role was to collect excavated soil and construction waste from building sites and transport it to the 'Vrazhdebna landfill', the only authorised disposal facility within the Sofia Municipality. There, disposal fees were calculated according to the weight of the waste, creating a transparent but relatively costly regulatory framework.

3. Crime script based on Case Victor

Motivation – Purpose

The primary objective of the network was **profit generation**. By avoiding mandatory disposal fees at Sofia's authorised Vrazhdebna landfill, the organiser enabled transport companies and construction clients to reduce operating costs while generating substantial illicit profits. In doing so, the network established a parallel waste disposal market involving multiple actors, including transport operators, construction companies, and allegedly complicit municipal officials (ACF, 2024). The scheme further demonstrated how criminal networks can exploit legitimate business sectors, capitalise on institutional weaknesses, and systematically generate illicit revenue.

[108] The network organiser (C1_V) had registered three limited liability companies over the years, all with similar stated scopes of activity. At least two of these companies were used to facilitate the illegal disposal of construction waste. One of them, established in 2009, had already been sanctioned by the Sofia Municipality in 2014 for the illegal dumping of excavated soil in the Suhodol district.

Preparation

Over the past years, Sofia has experienced a sustained **construction boom**. The number of completed dwellings increased by 27.3% to 15.415 units in 2021, growing to 22,649 units in 2023 (Stoykova, 2023). According to the National Statistical Institute (2025), the number of construction projects initiated annually rose from just thirteen in 2004 to 522 in 2023. This sustained expansion has generated unprecedented volumes of excavated soil and construction debris requiring disposal, while property market dynamics have further reinforced this growth trajectory. Consequently, demand for waste collection and disposal services has increased substantially, placing sustained pressure on waste management infrastructure and creating predictable, high-volume waste streams, which were also exploited by the criminal network involved in Case Victor. Transport companies were able to plan routes, allocate resources, and coordinate with corrupt officials (cf. *infra*), thereby maintaining operational continuity over multiple years.

These conditions have provided criminal networks with recurring opportunities to exploit vulnerabilities within the waste management system. As a result, Sofia's waste collection and disposal sector has become heavily affected by **organised criminal activity**. In particular, offences involving the unauthorised disposal of excavated material (soil), the illegal dumping of hazardous waste, and fraud relating to the transportation and disposal of household waste constitute persistent and serious challenges. Under the current regulatory framework, all construction waste and rubble must be transported to the Vrazhdebna landfill, where disposal charges are levied according to the weight of each load. These mandatory disposal fees impose significant cost pressures on construction and transport companies, creating a strong financial incentive to seek alternatives to regulatory compliance. This incentive is further reinforced by the limited enforcement of sanctions for non-compliance. As a result, the identification of more than 240 **unauthorised dumping sites** across Sofia Municipality indicates the existence of a large-scale parallel waste disposal system operating outside the regulatory framework.

Although the unauthorised dumping of construction waste carries substantial fines for both drivers and transport companies, **enforcement** has remained **weak**. Municipal inspection capacity proved insufficient to monitor and regulate the sector's rapid expansion, leaving extensive areas of Sofia's periphery effectively beyond routine oversight. Furthermore, the existing penalty structure weakened the deterrent effect of regulatory enforcement. Although regulations allowed for fines of up to EUR 25,000 for transport companies, penalties imposed under the previous inspectorate leadership were frequently set at the minimum applicable level. Where fines were issued, they typically represented only a small proportion of the profits generated through avoided disposal fees, thereby making non-compliance economically attractive from a business perspective. Moreover, the absence of criminal sanctions for large-scale illegal dumping meant that administrative penalties remained the primary enforcement mechanism. Consequently, repeat offenders faced neither the prospect of imprisonment nor the revocation of business licences, regardless of the scale or duration of their illicit activities.

The illegal dumping scheme in Sofia involved the majority of **transport companies** responsible for removing rubble and construction waste from construction sites, illustrating the extent to which the criminal network had systematically infiltrated the legitimate waste management sector. These companies represented attractive targets for criminal co-option, as they possessed the operational infrastructure required to facilitate both lawful and illicit activities, including fleets of heavy-duty

vehicles, licensed drivers, access to construction sites, and established contractual relationships with developers and subcontractors. Moreover, their legitimate legal status, professional appearance, and routine presence within construction environments afforded a degree of legitimacy and concealment that reduced the likelihood of detection. By diverting waste streams from the authorised Vrazhdebna landfill to unregulated disposal sites, transport operators were able to offer construction clients substantially lower disposal costs while retaining a significant proportion of the avoided landfill fees as illicit profit. As a result, these companies were well positioned to function as dual-use entities, simultaneously conducting legitimate commercial operations and facilitating systematic environmental crime.

The construction waste management sector in Sofia exhibited several structural vulnerabilities that were systematically exploited by the criminal network involved in Case Victor. First, the **fragmented organisation** of construction project delivery, characterised by complex subcontracting chains, facilitated the operation of the scheme. Construction firms routinely outsourced waste collection and disposal to third-party transport and waste management companies, thereby diffusing responsibility among construction investors, principal contractors, and waste transport operators. This organisation arrangement enabled construction clients to benefit from lower disposal costs. The criminal network capitalised on this structural feature by operating a parallel waste disposal system alongside the legitimate regulatory framework, while minimising the risk of detection by the companies generating the waste.

Moreover, the availability of **unused arable land** provided the physical infrastructure necessary for the operation of the scheme. Many landholders owning agricultural plots in the vicinity of Sofia do not actively cultivate their land but instead seek to have its designation changed to urbanised territory in order to increase its market value. However, the process of changing land-use status is often lengthy, complex, and, in some cases, impossible due to regulatory and legal constraints. Consequently, some landholders prefer to lease their plots without closely monitoring the activities undertaken by tenants, as long as they receive their rent. This created opportunities for the criminal network to exploit otherwise underutilised land for illegal waste disposal.

Pre-activity or enabling conditions

- **Degree of criminal use of the legitimate business(es);**
  The waste disposal and transport companies involved in Sofia's illegal dumping network operated according to dual business models that blurred the boundaries between legitimate and criminal activity. These firms maintained formal business registrations, held the required licences for waste transportation, and sustained contractual relationships with construction companies, thereby operating within the established legal framework. At the same time, however, they conducted systematic parallel disposal operations, diverting construction waste away from authorised facilities towards unregulated dumpsites.

This did not constitute opportunistic or sporadic criminal behaviour but rather involved deliberate planning, logistical coordination across multiple sites, and the sustained repetition of illegal activities over several years. As a result, transport companies occupied a critical intermediary position between legitimate construction activity and organised environmental crime. The exploitation of these businesses was **comprehensive**: the same trucks, drivers, organisational structures, and client relationships that supported lawful waste collection were systematically repurposed to facilitate illegal dumping operations. Overall, the available evidence suggests that these transport companies were not merely passive service providers but functioned as active logistical enablers within a large-scale illegal waste disposal market. Their legitimate status, operational capacity, and integration into mainstream construction processes provided the criminal network with essential cover, infrastructure, and financial channels, thereby enabling the sustained continuation of long-term illicit activities.

- **Culpability of companies;**
  The available evidence indicates the deliberate and **systematic misuse** of legitimate business structures rather than inadvertent compliance failures or isolated misconduct by individual employees. The company responsible for securing the illegal dumping sites, together with the transport company operators involved, demonstrated sophisticated knowledge of municipal inspection procedures, including the timing of enforcement activities and geographic patterns of regulatory oversight.

- **Opportunities enabling criminal activity;**
  Alongside the structural opportunities present within Sofia's construction waste management sector (cf. *supra*), the network was sustained through **systemic protection mechanisms** embedded within municipal inspection structures. The Head of the Construction Pollution Control Sector, who held this position since 2011, was exposed as having supported the scheme for several years and as being willing to pay EUR 255,000 to secure the position of Inspectorate Director within the municipal administration. Evidence further indicates that municipal inspection officials provided advance warnings of forthcoming inspections to operators of illegal dumping sites, applied sanctions selectively, and tolerated repeated violations. In some instances, inspection vehicles reportedly remained stationary for hours, apparently providing violators with sufficient time to conceal breaches, while imposed fines were often limited to the minimum applicable levels. This degree of foreknowledge suggests the existence of sustained communication channels between the criminal network and municipal officials, indicating active collusion rather than merely the exploitation of enforcement weaknesses. Such institutional infiltration and **corruption** within oversight institutions substantially reduced operational risks for the network, allowing it to sustain its activities over several years (ACF, 2024).

Activity

The illegal dumping operation in Sofia functioned as a **networked criminal enterprise**, coordinated by a central organiser (C1_V). He facilitated cooperation among multiple categories of actors (including transport companies and individual drivers), managed access to dumping locations, and secured the involvement of complicit public officials providing protection and intelligence from within municipal institutions. This organisational structure provided the network with considerable operational resilience: the removal or disruption of individual participants did not undermine the wider system, as other actors were able to maintain the continuity of waste disposal services for construction clients. For instance, the replacement of the Head of the Construction Pollution Control Sector within the Sofia Municipality Inspectorate, who had facilitated lenient oversight of the network's activities (cf. *supra*), did not significantly disrupt the scheme. Instead, the network rapidly adapted by exploiting a legal loophole that enabled transport companies to avoid paying imposed administrative sanctions (ACF, 2024).

The criminal operation itself followed a recurring operational **cycle** that was seamlessly integrated into legitimate construction waste management processes.

- **Step 1: Waste collection**
  The cycle began with the collection of waste from construction sites under standard commercial contracts. Transport companies dispatched vehicles to construction projects across Sofia to collect excavated soil and construction debris, documenting these activities through delivery notes and waste manifests that created the appearance of lawful service provision. At this initial stage, the operation was virtually indistinguishable from legitimate waste transport, with drivers adhering to standard procedures for loading and departing from construction sites.

- **Step 2: Diversion and illegal disposal**
  The critical criminal activity occurred during the transport phase, when drivers diverted waste loads from the authorised Vrazhdebna landfill to illegal dumping sites. Rather than being *ad hoc*, these diversions were centrally coordinated by the network organiser (C1_V), who instructed drivers on the selection of disposal sites based on factors such as available site capacity, recent enforcement activity, and proximity to the originating construction project. Site selection was therefore guided by a combination of operational efficiency and risk management, minimising transport time and distance while avoiding locations that had recently attracted regulatory attention or were expected to be subject to inspection (ACF, 2024).

  The timing of illegal dumping operations was strategically managed to minimise the risk of detection. Waste deliveries to unauthorised disposal sites typically took place during the early morning hours or late evening, when municipal inspection activity was limited and visibility was reduced. At the disposal sites, unloading was carried out rapidly, with drivers depositing waste and leaving immediately to minimise the time spent at unauthorised locations. Repeated use of particular sites gradually resulted in the emergence of established dumping locations, forming a stable component of the network's operational model.

A critical component of the network's operational security was the provision of advance warnings by compromised municipal officials (cf. *supra*). Individuals within the Inspectorate supplied information on planned inspections, including their timing and target locations. This intelligence enabled transport companies to suspend activities at high-risk sites or redirect vehicles to alternative disposal locations. In documented instances, municipal inspection vehicles reportedly remained stationary near illegal dumping sites for extended periods, apparently allowing operators sufficient time to conceal evidence before formal inspections commenced. This coordination between criminal actors and comprised public officials effectively neutralised the deterrent effect of enforcement, transforming inspections into manageable operational events that could be anticipated (ACF, 2024).

- **Step 3: Revenue generation and profit distribution**
  The operational cycle concluded with the generation and distribution of illicit profits. By diverting waste to illegal disposal sites rather than the municipal landfill, transport companies avoided disposal fees while continuing to invoice construction clients for waste collection and disposal services, often at prices slightly below prevailing market rates to maintain a competitive advantage. The difference between the fees charged to clients and the costs actually incurred – largely limited to fuel and driver wages – constituted substantial illicit profit. Over the course of hundreds of waste deliveries spanning several years, this business model generated considerable criminal proceeds. These profits were distributed among the network organiser (C1_V) responsible for controlling access to dumping sites, the owners of the transport companies, and corrupt municipal officials who received payments in exchange for protection and advance intelligence (ACF, 2024).

The cyclical nature of the operation, repeated daily across dozens of active construction sites, gave rise to a stable criminal business model. The continuous generation of waste by construction projects created a predictable demand for disposal services. The network was able to meet this demand reliably and at competitive prices, and with limited disruption caused by regulatory enforcement. These conditions enabled the network to function as a **parallel waste management system** operating alongside Sofia's legitimate disposal infrastructure (ACF, 2024).

Post-activity or post conditions

The illegal dumping network in Sofia operated over an extended period. The available evidence suggests that the criminal exploitation of legitimate construction waste transport and disposal businesses persisted for approximately five to ten years. The earliest documentation indication of C1_V's criminal activities dates to 2014, when one of his companies was sanctioned by Sofia Municipality for illegal dumping in the Suhodol district. This estimated timeframe is further supported by several additional indicators, including the discovery of hundreds of unregulated dumping sites across Sofia, the extent of institutional infiltration within the Municipal Inspectorate, and investigative findings indicating that senior officials had occupied positions capable of facilitating the scheme since 2011 (ACF, 2024). At the same time, the longevity of the criminal network was facilitated by clear **indications** of institutional infiltration at multiple levels of municipal oversight (cf. *supra*).

Meaningful intervention against the network did not commence until 2024, following investigative reporting by media organisations and anti-corruption advocates. These investigations documented the scale of the illegal dumping operation and exposed the alleged involvement of municipal officials, generating substantial public attention. The resulting external pressure prompted a series of institutional responses across multiple levels of government. Two **pre-trial proceedings** were initiated in relation to the illegal waste disposal scheme: one by the Sofia City Prosecutor's Office and another by the Sofia District Prosecutor's Office. However, both investigations were subsequently suspended, and no criminal charges were brought owing to legislative gaps, as the large-scale deposition of excavated soil is not classified as a criminal offence under the Bulgarian Criminal Code (ACF, 2024).

Following the media investigation, the corrupt official of the Sofia Municipality Inspectorate who had facilitated the disposal of waste at illegal dumping sites was removed from office. However, illegal dumping continued, as administrative sanctions had proven insufficient to deter perpetrators. Although documented violations could result in fines of up to EUR 2,500 for drivers and EUR 25,000 for companies, the enforcement of **administrative penalties** remained ineffective, with only a limited proportion of imposed fines being collected due to legislative loopholes and procedural obstacles.

At the **municipal level**, a series of administrative reforms was introduced following changes in the leadership of the Sofia Municipal Inspectorate. The new management initiated a systematic mapping of illegal dumping sites, issued more than ninety penalty notices during its first months in office, and substantially increased the level of fines compared with previous enforcement practices. Disciplinary proceedings were also initiated against inspectorate employees implicated in the scheme. However, some individuals relied on administrative mechanisms, including sick leave and trade union protections, to delay or prevent disciplinary action. In addition, the newly elected Mayor of Sofia announced that the municipality would submit a formal complaint to the Prosecutor's Office concerning the alleged abuse of official position and corrupt practices by inspectorate employees, thereby escalating the matter to the level of a criminal investigation.

At the **national level**, legislative initiatives were announced to strengthen the existing legal framework. Proposed amendments to the Penal Code sought to establish large-scale illegal dumping as a distinct criminal offence, thereby addressing shortcomings in the environmental legislation, which relied primarily on administrative sanctions.[109] The Ministry of Environment and Water provided technical support by mapping illegal dumping sites through satellite imagery and coordinating with municipal authorities to identify remediation priorities. In parallel, environmental monitoring programmes were strengthened to track progress in site remediation and reduce the risk of new unauthorised dumping locations emerging.

Meanwhile, continued scrutiny from civil society and the media has maintained pressure for institutional accountability. Investigative reporting and NGO advocacy have highlighted new illegal dumping sites, called for stronger enforcement, and demanded greater transparency regarding remediation efforts and the accountability of implicated officials. Despite these interventions, **significant challenges** remained. The financial resources required to fully remediate the situation, estimated at several million euros, exceed the capacity of available municipal budgets. Many waste

[109] The Bulgarian Parliament adopted the amendment of the Criminal Code on 19 March 2026.

transport companies implicated in the scandal continued to operate legally while investigations were ongoing, and the decentralised nature of the criminal network complicated efforts to dismantle it comprehensively. Moreover, the persistence of strong market incentives, high legal disposal costs, and sustained construction demand, suggests that – without fundamental structural reforms to oversight and enforcement mechanisms – pressure towards illegal dumping is likely to continue.

4. Financial profile of the criminal network involved in Case Victor

The financial information on this criminal network, as reflected in investigative reporting, suggests that its operations were designed to mirror those of legitimate waste transport businesses while systematically **generating illicit profits** through regulatory circumvention. Revenue generation, cost management, and profit distribution followed patterns typical of construction service providers, particularly construction waste management companies. However, these operations also incorporated distinct criminal adaptations that clearly differentiated the network from its law-abiding counterparts.

Financing sources and start-up capital

Start-up capital was likely obtained through conventional business formation mechanisms. The transport companies involved in these activities were also likely established as formally registered businesses before engaging in systematic illegal dumping.

Payment methods and arrangements within the network

Payment arrangements followed standard construction industry practices, exploiting the infiltration of legitimate sectors to conceal criminal proceeds. Payments for waste removal services were typically made through **conventional channels**, such as invoicing and bank transfers, making these transactions appear indistinguishable from legitimate business operations. The criminal element – primarily the non-payment of the substantial disposal fees at the Vrazhdebna landfill – remained off the books. Consequently, no specialised financial mechanisms were required, as the proceeds simply remained in the transport companies' accounts as apparently legitimate profits.

Costs of business operations

The network's cost structure likewise resembled that of a legitimate business, with expenditure primarily relating to vehicle operation and maintenance, driver wages, administrative overheads, and fuel. Its assets were similarly indistinguishable from those of a legitimate enterprise, including fleets of heavy-duty trucks, office facilities, and long-standing relationships with construction companies. These assets served both legal and illegal activities, eliminating the need for specialised criminal infrastructure. Protection payments to **corrupt municipal officials** constituted an additional operational cost of the scheme. Reported conversations indicated that the former Head of the Construction Pollution Control Sector at the Municipal Inspectorate collected payments from the transport companies and intended to pay EUR 255,000 in bribes to secure appointment as Director of the Municipal Inspectorate. This suggests that substantial financial resources were allocated to maintaining institutional protection and facilitating the continuation of the illegal activities. To avoid detection and financial scrutiny, these payments were likely made in cash and kept outside the companies' official accounts.

Revenues and proceeds

Proceeds largely remained within the legitimate economy without requiring extensive money laundering. Revenue entered company accounts as apparently legitimate income from construction clients, enabling operators to maintain conventional banking practices, report income to the tax authorities, and make standard business investments. Consequently, integration within an ostensibly legitimate business provided an inherent money laundering mechanism, without requiring separate financial infrastructure.

Estimating the network's total revenue is challenging, as it would require calculating the disposal fees avoided across all documented instances of illegal dumping. In the Pancharevo district alone, illegal landfill activities reportedly cost the Sofia Municipality approximately EUR 2,500 per day. Given the multiple affected districts and the hundreds of illegal dumpsites operating over several years, annual losses to the Municipality – and corresponding profits for the criminal network – are likely to have reached **several million euros**.

5. Harms caused by Case Victor

Harms to other businesses

The economic burden falls heavily on public resources and law-abiding businesses. The clean-up, regularisation, and remediation of illegal dumpsites impose substantial costs on municipal budgets, ultimately borne by taxpayers. The Bulgarian Anti-Corruption Fund documented losses of millions of euros to Sofia's budget, with costs continuing to accumulate (ACF, 2024). At the same time, legitimate waste transport companies face unfair competition from criminal operators offering artificially low prices, while construction firms complying with disposal requirements incur higher costs than those using illegal system. This distorts competition and disadvantages responsible businesses.

Harms to public institutions

The scheme also caused significant institutional harm by undermining public trust in municipal governance. Where illegal dumping operates as a business model allegedly protected by municipal officials, confidence in regulatory institutions may be weakened. The normalisation of systematic lawbreaking, particularly in the context of alleged complicity at senior levels of inspection services, may further undermine perceptions of equal enforcement and institutional integrity. These effects extend beyond the waste management sector, potentially affecting broader perceptions of governance effectiveness and the rule of law in Sofia Municipality.

Harms to the physical environment

Environmental degradation represents the most immediate and visible impact of Case Victor. Soil contamination and degradation caused by construction waste alter ground composition, rendering land unsuitable for agriculture or future use as green space. The location of many dumpsites near ravines and riverbeds further increases the risks of fire, flooding, and erosion. During the summer months, fires may pose an immediate threat to the health and safety of nearby residents, while heavy rainfall can cause landslides and contaminated runoff, spreading pollutants into waterways, destabilising slopes, and obstructing natural drainage. Moreover, the systematic conversion of farmland and undeveloped municipal land into waste repositories results in a permanent loss of productive and recreational space for Sofia's residents (Rusev et al., 2026).

ANNEX 8

STOCKHOLM

DETAILED CASE STUDIES

Annex 8.W – Case Whiskey: Children in the Care of Criminals

1. Background: foster care in Sweden

In Sweden, municipalities – through their social welfare committees – have the ultimate responsibility for assessing children's needs for protection or support (SOU, 2025). This includes decisions on placement and responsibility for monitoring the quality of care provided. Municipalities may provide care directly or procure services from private providers. Regardless of whether care is provided publicly or privately, responsibility for placement decisions and oversight formally remains with the municipality. When a child needs to be placed in a new home, social services will first seek to place the child with relatives or other people known to them. Where this is not possible, they may turn to so-called "**Familjehem**" (foster homes): private households that provide care to children or young people in a family setting, broadly comparable to foster care in the Anglo-Saxon context. The caregivers are not professionally trained staff but individuals or couples providing care in their own homes. In principle, they must be approved and supervised by social services. According to interviewees and sector representatives, however, this has not always been the case in practice.

Where a child requires more intensive care, they may be placed in a "**Hem för Vård eller Boende**" (HVB), which translates literally as "Home for Care or Residence". These are residential facilities providing professional care and support to children, adolescents, or adults. Since 2017, the operation of HVB-homes has been subject to licensing requirements. Both owners and key personnel, including managers and staff, must demonstrate appropriate professional competence and undergo a suitability assessment as part of the licensing process administered by the Health and Social Care Inspectorate (IVO). In 2024, the police published a previously confidential report revealing that numerous individuals linked to criminal networks owned or worked in HVB-homes (Brå, 2025; NOA, 2024b). These revelations prompted public concern and government action, including a government inquiry recommending reforms to the HVB-system (SOU, 2025). IVO subsequently refused licences to several homes linked to criminal networks. However, revoking or preventing licences has proved challenging.[110] Approximately three-quarters of children in Sweden who are placed outside their family home are placed in foster homes, followed by around one-fifth in HVB-homes, while a small proportion are placed in state-run secure treatment centres (SOU, 2025).

During the 2015-2016 refugee influx, **private consultancy firms** providing foster care services expanded rapidly. These firms recruit and match suitable foster homes for children and young people and provide guidance and support to foster carers. At the time, Swedish municipalities lacked the administrative and practical capacity to accommodate the larger number of unaccompanied minors arriving in the country (Savona & Riccardi, 2018; SOU, 2025). The regulatory framework also placed fewer restrictions on establishing such consultancy businesses or arranging different forms of foster care, without requiring licensing or prior authorisation. Although foster homes were formally subject to municipal approval and supervision, in practice this supervision was often delegated to consultancy firms acting on behalf of municipalities.

[110] Most recently, the Administrative Court overturned IVO's decision to revoke the licence of an HVB-provider identified by the police as having links to criminal networks. The court found the identified shortcomings insufficient to justify revocation and held that IVO should have specified the measures required to address them.

Since 2017, consultancy firms that both place children in foster homes and provide guidance have been subject to **licensing requirements and restrictions** on who may operate them. Owners, managers, and certain staff must demonstrate appropriate competence and undergo a suitability assessment when applying for a licence from IVO. However, firms that provide only placement or only guidance are not subject to oversight by IVO, creating a regulatory gap. Moreover, IVO does not conduct regular inspections of licensed consultancy firms. Instead, supervision is largely reactive and based on reports or complaints from municipal social workers or members of the public. Many consultancy firms also hold licences to operate HVB-homes or operate separate family homes. While this is not inherently problematic, such arrangements may create opportunities for exploitation by criminal actors. In addition, some consultancy firms – including those examined in Case Whiskey – place children in family homes that effectively operate as HVB-homes without the required licences or oversight. In such cases, care is provided by employed staff rather than by foster carers, contrary to the applicable rules.

2. Criminal network involved in Case Whiskey

C1_W, C2_W, C3_W, and C4_W formed a criminal network and were also connected to an established **criminal group**, possibly through having grown up in the same neighbourhood, according to an interviewee. However, there is no indication that the criminal group was directly involved in establishing the consultancy forms, foster homes, or HVB homes. C1_W, C2_W, and C3_W have been involved in both economic and drug-related crime and have established or been involved in several companies across a range of sectors, including financial services, real estate, transport, and welfare services. An individual associated with LTD2_W also appears to have provided a work certificate for a family member of one of the criminal group's leaders. Table 17 provides an overview of the core members of the network.

The case files focus on relatively narrow economic offences committed by the consultancy companies and do not examine potential wider criminal activities, despite a municipal interviewee's assessment that "criminal use permeates everything they do". Interrogations documented in the case files suggest that many employees of the companies were unaware of the owners' criminal connections. One employee described the owners as "sweet guys at heart that got a bit greedy". While this account may be viewed as wilfully naïve or self-serving, it remains possible that many employees were genuinely unaware of these connections.

Table 17
Overview of the core members of the criminal network involved in Case Whiskey (Stockholm)

Member	Role	Gender
C1_W	Beneficial owner of LTD1_W and LTD2_W; Managing logistics for the criminal network	Male
C2_W	Beneficial owner of LTD1_W and LTD2_W	Male
C3_W	Unclear	Male
C4_W	CEO of LTD4_W and LTD5_W	Male
C5_W	Strawmen; Relative of C4_W	Male
C6_W	Board member of LTD6_W and LTD7_W; Worked for the municipality in a role involving children	Female
C7_W	Part-owner of LTD2_W for a period	Female
C8_W	Unclear	Male
C9_W	Deputy CEO of LTD2_W	Male

3. Legitimate businesses involved in Case Whiskey

All companies involved in Case Whiskey were **limited companies**. All companies appear to be of a similar size, employing between ten and twenty staff (excluding staff or 'parents' in family homes) and generating annual revenues of approximately SEK 15 to 50 million, depending on the year.

- **LTD1_W** was established as a consultancy company to facilitate the placement of unaccompanied children in foster homes during the height of the 'refugee crisis' in the mid-2010s. According to the case file, the beneficial owners (C1_W and C2_W) were based in an area near Stockholm.
- **LTD2_W** was established in the mid-2010s by C1_W and C2_W for the same purpose as LTD1_W. All individuals involved have been accused of serious tax and accounting offences. C4_W and C7_W also served as board members of LTD2_W for certain periods.
- **LTD3_W** was established by C4_W in the mid-2010s. C4_W had a background in social work and healthcare, including positions at both municipal and national level, and had previously held various positions in several companies. C3_W was also involved in some capacity and may have acted as a link between LTD2_W and LTD3_W.
- **LTD4_W** was established by C4_W before the other companies, but appears to have become operational only several years later, when LTD3_W was being inspected by IVO. C4_W subsequently sold the company to a relative, while LTD3_W provided a loan to finance LTD4_W's establishment. IVO later concluded that LTD4_W was effectively operated by C4_W, with some involvement of C3_W. C4_W was primarily responsible for contacts with social services and family homes, but also handled invoicing and financial matters. C3_W was responsible for finances, systems, and documentation. In the early 2020s, IVO revoked LTD4_W's licence for 'consultant-supported family home care' after receiving information that individuals involved in LTD3_W were also active in LTD4_W.
- **LTD5_W** was established in the early 2020s, with C4_W as a board member.
- **LTD6_W** was established with financial involvement of LTD5_W and C5_W as a board member. C5_W had previously worked for a municipality. LTD6_W received a licence in the late 2010s, which was revoked several years later, partly due to its connections to C4_W. Since then, several new companies have been established involving similar constellations of board members.

4. Crime script based on Case Whiskey

Motivation – Purpose

Based on interviews with police and municipal personnel, **financial gain** appears to be the primary motivation. Operating consultancy firms, foster homes, and HVB-homes can be highly lucrative, as discussed below. Payments range from approximately EUR 300 to EUR 3,000 per child per day, while costs and oversight may be relatively limited. Interviewees also identified other potential, albeit secondary, motivations. One was the use of the business as a form of '**cover for action**': having legitimate-looking companies may help individuals appear economically active and reduce scrutiny

from government authorities, particularly as enforcement against undeclared income and tax evasion has increased.

In this context, police interviewees also speculated that residential facilities could potentially be used to conceal weapons or drugs, with responsibility subsequently attributed to the young people residing there, or that company vehicles could be used for smuggling. A further possible motivation was the use of the facilities as **recruitment** grounds for criminal networks, including for the recruitment of young people as low-level offenders or drug dealers. Two interviewees also pointed to possible motivations related to control, power, and prestige, suggesting that gaining control over a legitimate market and employing large numbers of people could provide **status** and influence.

Preparation

Several characteristics of the subsector make it vulnerable to exploitation by criminal networks. First, concerns have been raised within the healthcare sector about vulnerabilities arising from, among other factors, strict patient confidentiality, which may also make criminal activities more difficult to detect. More broadly, there is growing concern – and emerging evidence – that the **increasing sophistication** of criminal networks in using companies as vehicles for criminal activity, combined with the privatisation of welfare services and relatively low barriers to establishing and operating limited companies, may increase the risk of criminal in healthcare and the welfare sector more broadly (Brå, 2025; NOA, 2025).

Furthermore, official statistics from the Swedish National Board of Health and Welfare indicate that almost 6,000 children and young people are placed in HVB-homes each year. According to interviewees, IVO remains a relatively small institution and is still developing its capacity to oversee the complex landscape of HVB-homes and consultancy companies. Municipalities, meanwhile, rely on consultancy firms to arrange placements for many children but do not always have the resources or capacity to adequately monitor either the firms or the homes in which children are placed. A further challenge concerns the **assessment of the quality of care**. Although municipalities pay substantial amounts to consultancy firms and care providers for the placement and care of children, there are limited mechanisms for defining and measuring what constitutes ‘good care’ for vulnerable children.

Additionally, several interviewees noted that new companies can be **established relatively easy** when an existing company is denied a licence. As one interviewee explained, HVB-homes are relatively straightforward to investigate because IVO has regulatory authority over them and information on the companies and their employees is available. Foster homes, by contrast, are more difficult to monitor because IVO has less information about them. By contrast, representatives of private companies in the HVB and foster care sectors noted that obtaining licences to operate consultancy firms and HVB-homes has become more demanding in recent years. IVO has increased its requirements for suitable physical premises, and the licensing process can now take up to a year. According to these representatives, this has made the sector less attractive to illicit actors. Nevertheless, establishing foster homes remains relatively easy, while oversight and supervision by municipalities and IVO remain limited.

According to the interviewees, several **other vulnerabilities** may make the subsector attractive to criminal actors. The risk of direct consequences is relatively limited, as the main sanction is the loss of a licence, while revocation procedures can be lengthy and subject to appeal. At the same time, municipalities may have difficulty finding suitable placements, particularly for children with complex needs or criminal backgrounds, increasing their reliance on consultancy firms. Information-sharing and oversight are also constrained by confidentiality rules intended to protect children. Municipalities may therefore lack a complete overview of how many children are placed in individual homes, creating a risk that homes accommodate more children than intended. Although IVO has introduced a registry of companies whose licences have been denied or revoked, it remains unclear whether all municipalities make effective use of it. The system also relies heavily on staff and managers reporting concerns, with serious cases referred to IVO. This creates a vulnerability where those responsible for identifying or reporting misconduct are themselves involved in concealing it. Finally, several interviewees noted a potentially problematic assumption that individuals with a history of criminal involvement are particularly well placed to help young people disengage from crime, even though some may remain involved in criminal activities or relapse.

Pre-activity or enabling conditions

LTD1_W was established by an investment company of dubious nature as a consultancy firm for placing unaccompanied children in foster homes during the height of the '**refugee crisis**'. According to the Business Register at the Swedish Companies Registration Office, its board of directors changed several times in quick succession. LTD2_W was established for the same purpose, with C1_W, C2_W, C4_W, and C7_W registered as board members. Although the ownership of LTD1_W remained unclear, extensive transactions between the board members of the two companies led investigators to conclude that they had the same beneficial owners. As discussed above, the consultancy and HVB-home subsector was subject to limited oversight before 2017 but has since undergone significant regulatory changes, including new licensing requirements. From 2017 onwards, LTD3_W and LTD4_W applied for licences from IVO to provide consultancy services and, when a licence was revoked, quickly established or switched to another company.

The business model required access to suitable properties for family homes, municipal contracts, and individuals who could act as foster carers. According to a representative of the municipality, these carers sometimes included serious criminal actors or so-called '**renting fathers**': men who formally appeared able to care for the children but in practice left them largely unsupervised with a small allowance. In some cases, the facilities presented as family homes were effectively residential institutions requiring employed staff, while documentation was used to present them as family homes and avoid regulatory oversight and inspections. The criminal network also needed a steady supply of children to place, which appears to have been readily available. As one interviewee noted: "They take in difficult children, sometimes criminals, that no one wants." The difficulty municipalities face in finding placement for children with complex needs therefore creates a favourable position for providers.

Furthermore, although some family homes recruited by the consultancy were legitimate and may have been unaware of the consultancy's criminal ties, the children placed in these homes did not receive the compensation and support to which they were entitled. One interviewee from the municipality reported indications that some foster carers (and, in some cases, staff members rather than foster parents) were **recruited from within the network**'s existing circle of friends and acquaintances. The extent to which these individuals were themselves involved in criminal activities or otherwise connected to criminal networks remains unclear. Nevertheless, given the social circles from which they were recruited, it is possible that some of them were aware of the network's criminal ties.

Another important 'enabling condition' that facilitated the identification of children was that some individuals involved in the companies had **connections** to a Swedish authority that enabled the companies to identify and recruit children for placement in their preferred foster homes more easily. All of the companies discussed in the context of Case Whiskey had several key individuals with connections to such authorities, either through current employment or previous positions. These connections may not only have facilitated access to children, but could also have made it easier to establish consultancy companies by providing knowledge of how the system operated and a degree of institutional legitimacy. Moreover, LTD3_W and LTD4_W each had a board member who was employed by a municipality in a role involving children. This dual role had not been disclosed to the municipality and, at the very least, constituted a conflict of interest.

Activity

LTD1_W and LTD2_W both **operated family homes** and placed children in family homes on behalf of the municipality. The exact number of children they placed across the various homes is unknown, but during its busiest periods, LTD2_W seemed to have been responsible for more than 150 children and young people, operated a number of family homes, and employed approximately a dozen staff members. The investigations revealed a consistent pattern of **financial misconduct** across several companies involved in Case Whiskey. The owners of LTD1_W and LTD2_W repeatedly failed to declare their income for tax purposes, while LTD3_W and LTD4_W exhibited similar patterns of financial irregularities. Across all four businesses, false invoices were used and addressed to both known and unknown recipients. Undeclared wages were paid to staff and owners, while funds were also withdrawn for personal use. Significant bookkeeping offences included the deduction of millions in unsupported or otherwise incorrect costs, including substantial expenses for which no receipts were available.

Moreover, fundamental **irregularities** – such as invoices without VAT and invoices bearing incorrect organisation numbers – were systematically overlooked. The misconduct also involved the misallocation of costs, as well as a failure on the part of those responsible for certification, bookkeeping, and auditing to address these apparent irregularities. At the same time, following the introduction of licensing requirements in 2017, considerable efforts appear to have been made to create a legitimate façade around LTD3_W and LTD4_W. LTD3_W, for example, recruited a well-respected and prominent individual as CEO and board member, who also worked for the company for a brief period. Based on the available information, this individual was likely unaware of the network's criminal connections.

There were also **shortcomings** in the **day-to-day operations** of LTD3_W and LTD4_W. On several occasions, the police or municipality found that children were not present at the address at which they were officially registered, or that they were residing at a different location from the one reported to the authorities, without the company informing the relevant authorities as required. Despite these indications, the response from the relevant authorities was slow. In general terms, the companies appear to have shared a similar *modus operandi* as well as similar organisational and administrative shortcomings. Considerable effort and sophistication went into identifying and placing children in HVB-homes that were presented as 'family homes'. At the same time, however, the companies appeared to lack long-term strategies and basic administrative capacity, and their accounting practices were characterised by a lack of care and oversight. Rather than investing in the effective operation and administration of their existing companies, they appeared to prioritise establishing new companies and repeatedly applying to IVO for new licences.

Post-activity or post conditions

Signs of criminal use were present from the outset, but weak oversight, inadequate procedures, and limited inter-agency cooperation meant that these warning signs were often missed or overlooked. Reports, including from whistle-blowers, were made to both the police and municipalities at an early stage, raising concerns about the **neglect of children**. However, as the number and seriousness of reported incidents increased, the authorities began to take action. Investigations had been initiated into the financial activities of LTD2_W and, to a lesser extent, LTD1_W. Both companies were subsequently declared bankrupt. Furthermore, there are indications that both LTD3_W and LTD4_W involved **children in criminal activities**. These included instances in which children were reportedly transported by the company together with known criminals for the purpose of transporting drugs. The names of children placed in their care, as well as those of owners and employees, have appeared in encrypted communications primarily used by criminal networks. Despite these indications, however, enforcement action against the companies focused primarily on economic and financial misconduct.

IVO rejected LTD3_W's application for a licence to operate as a 'consultancy company' because of concerns regarding both C4_W, who was deemed unsuitable on the grounds of economic misconduct, and C3_W, who had an extensive criminal record and held a leading position within the company. The latter was particularly problematic given that individuals convicted of serious offences are prohibited from working with young people. However, once the licences were revoked, new companies were brought in to replace them. In the case of LTD4_W, the organisation continued to operate in several municipalities even after its licence had been revoked. In the newly established companies LTD5_W and LTD6_W, connections to the criminally involved individuals (C3_W and C4_W) remained, but were less readily apparent.

5. Financial profile of the criminal network involved in Case Whiskey

Financing sources and start-up capital

The case file contains evidence that LTD2_W was financed with capital from LTD1_W, while funds from LTD2_W were subsequently used to finance several other businesses. Similarly, capital from LTD3_W was used to finance LTD4_W, which in turn provided financing to LTD5_W and LTD6_W, either in the form of loans or through partial ownership. However, it is unclear whether these funds originated from legitimate activities or whether they also included proceeds from illegal activities. Throughout the period in which the companies were operational, all of them received a steady stream of income from the placement of children in care, with the associated costs being paid by the municipalities.

Payment methods and arrangements within the network

Based on the available information, no clear picture of the financial arrangements within the network emerges. Nevertheless, the investigation into the financial transactions of LTD2_W, and to a lesser extent LTD1_W, uncovered a large number of **suspicious transactions**. In particular, the investigation revealed extensive use of company funds for private expenditure by C1_W and C2_W. The investigations further indicate that C1_W and C2_W each failed to declare approximately a few million SEK in income in a particular year. C2_W also repeatedly provided incorrect information in the company's employer tax returns. In one year alone, contribution bases exceeding SEK 10 million were omitted from the reported figures, creating a risk that more than a few million SEK in employer contributions were unlawfully withheld from the public authorities. In addition, LTD2_W acquired an expensive private residential property, which was subsequently transferred to C2_W for use as his private residence. False purchase documentation was used in connection with the transaction, and the property was transferred for an amount below its market value.

Costs of business operations

The costs of establishing a company in this sector were relatively low, particularly when companies were able to avoid the costs associated with applying for the required licences. However, as the network expanded into subsectors subject to licensing requirements, repeated refusals or revocations by IVO increased the costs of maintaining its operations. The companies employed between approximately ten and twenty full-time employees and maintained facilities for their own operations, as well as for foster families and staff working in the "supposed foster homes but actual HVB-homes". These arrangements likely involved substantial operating costs.

It is unclear how much the companies paid the family homes for providing care. According to a municipal employee, there are also indications that some children may have been given a small amount of money to live independently at an address that did not correspond to their actual place of residence. LTD4_W additionally offered training courses on childcare. The purpose of these courses remains unclear: they may have been intended to enhance the company's legitimacy, strengthen its relationships with foster families, reduce scrutiny, or serve other purposes.

Revenues and proceeds

The available data do not allow for a precise estimate of the companies' total revenues. Publicly available annual accounts provide only partial snapshots and may not fully reflect their actual financial activities. Nevertheless, LTD2_W reported annual revenues ranging from approximately SEK 13 million to more than SEK 50 million, while LTD3_W and LTD4_W each reported annual revenues ranging from SEK 20 million to more than SEK 50 million. It is unclear to what extent these revenues were transferred to or otherwise benefited the criminal network. However, given the financial flows between the companies and the broader network, the possibility that some of these revenues contributed to financing other criminal activities cannot be excluded.

6. Harms caused by Case Whiskey

Harms to individuals

Children placed in residential homes are particularly vulnerable, often have experienced trauma, drug addiction, and a need for special care, guidance, and structure. Instead, they may be left with little or no supervision, sometimes in impoverished and highly unhygienic situations. In some cases, children have reportedly been exposed to or encouraged to engage in criminal activities, including through placement in homes where weapons and drugs were stored or through contact with criminal associates. In the most serious cases, children placed in family homes by this type of consultancy companies have reportedly been both perpetrators and victims of murder.

Harms to other businesses

According to the police analysis report, criminally connected actors are endemic in the sector, which may have made it more difficult for legitimate businesses to establish themselves (NOA, 2024b).

Harms to public institutions

The State and municipalities incurred considerable money that ultimately benefited criminal actors and their networks. Although service quality is difficult to assess, the available evidence suggests that public authorities did not receive services consistent with the resources allocated. Moreover, the companies and individuals involved did noy pay the applicable taxes and fees, resulting in tax losses of several million kronor. The involvement of criminal networks in operating HVB-homes has received considerable media attention, prompting action by the authorities. Nevertheless, significant challenges remain, potentially undermining trust in key institutions. As one police employee noted, placing children in compulsory care that provides worse conditions than those at home represents a fundamental failure of the State.

Harms to the social environment

The forced placement of children in criminal environments constitutes a significant social harm and may increase their risk of involvement in criminal activities. Even without direct links to criminal networks, placement in HVB-homes may expose children to criminal influences (Brå, 2023). Individuals who were later recruited into criminal networks described HVB-homes and youth homes as meeting places where they established contacts with other young people involved in crime.

Annex 8.X – Case X-Ray: Construction and Cash Compensation

1. Criminal network involved in Case X-Ray

According to interviewees, the actors involved in Case X-Ray were part of a wider criminal network than was visible from the case file, as well as of a broader **Russian-speaking community**, despite their different national backgrounds. The main actors were considered sufficiently harmful by the authorities to warrant a multi-agency response. Interviewees assessed the capacity of this criminal environment as high, citing its ability to create and use large numbers of false identities, obtain welfare payments fraudulently, and operate efficiently, particularly in the construction sector. Several investigative reporters have also documented the wider Russian-speaking community, its use of online platforms, and the *modus operandi* of criminal networks within it (Alexandrova-Zorina, 2023, 2025; Fyrk, 2020).

These broader patterns were reflected in the case file, which contained evidence of false passports, identity misuse, falsified COVID-19 test results, and fictitious income registrations. In encrypted chats, the main actor (C1_X) and one of his associates discussed opportunities to obtain government contracts abroad and potentially participate in public procurement in the construction sector in Sweden. This suggests that their activities extended beyond financial management and crime-as-a-service to direct involvement in **construction activities**. Notably, all three principal actors had backgrounds in the construction sector.

According to an interviewee, and supported by several indications in the case material, the scheme appeared to have emerged from a network's need for **money-laundering services**. These indications included the connections between C1_X, C4_X, and C5_X and the client companies, their backgrounds in construction rather than financial management, and their discussions about obtaining construction contracts. At the same time, the network also appeared to operate as a facilitator by providing money-laundering services to other criminal networks on a crime-as-a-service basis.

In Case X-Ray, it is particularly difficult to determine where one network ends and another begins. Rather than a clearly bounded network, the case appears to involve a **broader criminal environment** in which different alliances formed around economic crime in the construction sector. The focus on economic crime, which is structured differently from more traditional forms of organised crime such as drug trafficking and fraud, may also help explain why comparatively little is known about these types of networks. Table 18 provides an overview of the core members involved in Case X-Ray. None held formal positions within the companies used by the network, but they exercised control over them through various arrangements. No minors appeared to be involved as company owners or account holders.

Table 18
Overview of the core members of the criminal network involved in Case X-Ray (Stockholm)

Member	Role	Gender	Born between	Nationality
C1_X	Organiser; Leader of the network's subset	Male	1974-1993	Swedish (and other)
C2_X	Administrator	Female	1974-1993	Eastern European
C3_X	Employee at 'the office'; Taking orders from client companies	Female	1974-1993	Eastern European
C4_X	Coordinating orders from a large number of client companies	Male	1974-1993	Eastern European
C5_X	Coordinating orders from a large number of client companies	Male	1974-1993	Swedish (and other)
C6_X	Recruiting strawmen; Registering companies and bank accounts	Male	1974-1993	/
C7_X	Involvement in hawala business	Female	1954-1973	Eastern European

- **C1_X** was the most prominent actor and appeared to be responsible for running the operation. He was contacted when critical decisions had to be made. He also received substantial declared income from several client companies, although the amounts varied considerably. An interviewee confirmed that C1_X was the leader of the operation under investigation, while noting that he was not considered a prominent figure within the wider criminal environment. There were indications that he had been running the operation for almost four years, although the preliminary investigation covered only the 21 months preceding the suspects' arrests. The case file also contains some indications that C1_X had taken over the operation from an individual who had left the network.

- **C2_X** appeared to control most of the bank transactions, as well as the digital banking credentials of the strawmen. She acted on C1_X's instructions but appears to have operated with considerable independence. The two were described as having a close relationship.

- **C3_X** worked within the scheme under C1_X's direction. Her tasks included answering calls and messages, relaying instructions concerning cash and invoices, and maintaining local accounts. She regularly recorded updated balances in chats and kept notes on the transactions. Although she did not have a formal employment contract, she was paid for her services. The available information suggests that these payments may have originated from illicit funds.

- **C4_X** was described as a facilitator or intermediary between the cash compensation scheme and some of its client companies. He was a friend of C1_X and also received what appeared to be fictitious income from one or more client companies, providing him with a legitimate-looking source of income on paper.

- **C5_X** was described as having a similar role and was well acquainted with C4_X, although he had been introduced to the wider group through C1_X. He also had loans that were repaid by a company used in the scheme.

- According to an interviewee, **C6_X** was a successful recruiter of strawmen and appeared in several investigations. He had previously been convicted of similar offences in another case. His activities included registering companies and applying for business bank accounts using strawmen or misappropriated identities.

- **C7_X** appeared to be closely involved in the hawala activities and in collecting funds for humanitarian purposes. The chat messages suggest that she was genuinely concerned about victims of the conflict and sought to provide assistance. In one conversation, C1_X discussed the conflict with a friend in a manner suggesting that he supported the opposing side to C7_X, although he was nevertheless willing to facilitate the transactions for financial gain. This may indicate that C7_X had limited knowledge of, or contact with, the wider network and was primarily involved in this 'secondary' activity. This may also help explain why she was ultimately not charged: there was insufficient evidence linking her to the network's more apparent money-laundering activities.

In addition, the preliminary investigation identified approximately **twenty strawmen**, although additional names appeared in the case file without being linked to specific identities. Some of these were suspected to have been created using falsified passports, including cases in which genuine names were combined with photographs of other individuals. The strawmen were generally adults, with relatively few under the age of 25 and many aged around 40 or older. Both men and women were recruited. Although men were often approached initially, they were sometimes encouraged to refer their partners. The available information suggests that recruitment extended across different social groups.

2. Legitimate businesses involved in Case X-Ray

Case X-Ray revolves around a **'crime-as-a-service' hub** that provided payment and money-laundering services to criminal networks, primarily in the construction sector. The operation was described as an 'invoice factory', using multiple companies to facilitate money laundering. All companies involved were limited companies. Most of them were registered as construction businesses, although some operated in other sectors vulnerable to illicit labour and criminal infiltration, including groundworks and gardening, cleaning, taxi services, and hospitality. The client companies purchasing these services operated across an even broader range of sectors. Some of these client companies appeared to be legitimate businesses that used the network's services only occasionally, possibly to obtain illicit labour on a temporary basis, according to an interviewee. Others appeared to be linked to actors from the same Russian-speaking community, or potentially to the wider network itself, and may have supplied illicit workers as part of a separate scheme.

According to the case file, the money-laundering companies functioned as **shell companies**, formally registered in the names of strawmen but effectively controlled and administered by the members of the core group (C1_X, C2_X, C3_X, C4_X, C5_X) in accordance with their interests and instructions. The convictions concerned the use of just over twenty companies, although the preliminary investigation identified additional companies linked to the scheme. The companies were not formally connected through an ownership structure. However, their links became apparent through financial transactions, invoice orders directed to multiple companies, and the repeated use of the same strawmen across different combinations of companies.

Furthermore, the money-laundering companies were based in different parts of Sweden, and also made transactions to companies in other countries. In addition, one member of the network lived in another EU country and appeared to operate similar services from there, while one strawman was offered a position on the board of a company in a third country. Taken together, these findings suggest that the scheme formed part of a broader, internationally connected structure.

3. Crime script based on Case X-Ray

Motivation – Purpose

The companies investigated were established to primarily provide **money-laundering services**, particularly in the construction sector. The scheme was designed to disguise illicit transactions in a way that allowed the companies' accounts to withstand superficial scrutiny, and potentially even a formal audit. The suspects were reportedly paid a fee of at least 15% of the amounts moved or laundered, totalling at least SEK 400 million. This provided a substantial financial incentive for operating the scheme. The network's underground banking services, including hawala and cryptocurrency services, provided an additional source of income and attracted a broader range of clients. These included migrants without access to conventional banking services, as well as drug-trafficking actors seeking to move or store funds outside the formal banking system.

Preparation

The construction sector is widely recognised as being particularly vulnerable to economic crime and is frequently associated with organised crime (Brå, 2011, 2025; Fair Play Bygg, 2025; SOU, 2025). Brå's (2025) research also identified construction as one of the sectors in which the largest number of individuals with known links to **criminal networks** had held company board positions over the preceding five years. Moreover, interviewees emphasised that the sector is characterised by numerous examples of criminal activity, involving substantial sums of money. Although profit margins in the sector are relatively small, the overall transaction volumes are high. Furthermore, entry into the sector is relatively easy, as many activities require only common or basic qualifications. This creates opportunities to reduce costs and increase margins through the use of low-paid or exploited foreign workers and by evading taxes. Interviewees also pointed to the avoidance of workplace safety and environmental regulations as further means of reducing costs.

Furthermore, the infrastructure required to facilitate economic crime is relatively **easy to establish** in Sweden. New companies can be set up with limited barriers, and existing companies with an established business history can be acquired and placed in the names of strawmen. Such companies can then be used to issue invoices, maintain bank accounts, and otherwise create the appearance of legitimate business activity. The individuals involved in Case X-Ray also used several false or misappropriated identities as strawmen on company boards or as authorised bank signatories.

There is a market for cash compensation schemes, driven by the extensive use of illicit labour in the construction sector. In Stockholm, numerous large-scale construction projects are underway, and Ekobrottsmyndigheten (2025) reports growing interest among criminal networks in participating in such projects. As delays in construction projects can result in substantial penalties, contractors have an incentive to use **illicit labour** on a temporary basis. The widespread use of temporary workers and consultants through subcontractors reduces transparency and enables companies to be used both to supply illicit labour and to issue fraudulent invoices. At the same time, actors involved in large-scale criminal activity in the sector need ways of paying these illicit workers and moving funds outside the formal banking system and its anti-money laundering controls. The network involved in Case X-Ray therefore provided a service for which other criminal actors had a clear demand and were willing to pay. By outsourcing the handling of cash, payments, and fictitious invoicing, clients could shift part of the risk of detection and the practical difficulties associated with moving illicit funds to the network.

Pre-activity or enabling conditions

The money-laundering companies involved in Case X-Ray were established almost exclusively for **criminal purposes**, with no indications of legitimate business activities. By contrast, the companies using their services (i.e., client companies) could have genuine and, in some cases, legitimate business operations. Thus, they appeared to carry out actual construction work, but paid illicit wages. One interviewee perceived some of these companies as legitimate actors in the construction sector that used workers paid illicitly to meet project deadlines. This, in turn, led them to contact actors able to provide invoices through the cash compensation scheme. Many client companies used these services only a handful of times. There were no signs of coercion: representatives of all companies voluntarily contacted an actor within the scheme and paid for the services. If the requested service could not be provided, they were free to seek it elsewhere.

As more than twenty companies were involved in Case X-Ray, the process varied between them. Nevertheless, three key steps appear to have enabled their criminal use:

- **Step 1: Establishing or acquiring limited companies suitable for issuing invoices and facilitating transactions**

- **Step 2: Identifying suitable individuals to act as strawmen**
  The network appeared to rely on individuals in relatively vulnerable socioeconomic positions as strawmen. Many had insecure employment, temporary jobs, health problems, or substance-use issues. One interviewee described some of them as naïve and easily manipulated, with some believing that they were merely receiving a small amount of money in return for doing someone a favour. For some, the additional income appeared to be particularly important, as indicated by their statements during interrogations and in chat messages. These circumstances may have made them more susceptible to recruitment and exploitation by the network.

  Several individuals described during interrogations how they travelled from another EU Member State to Sweden on multiple occasions. Although they were recruited in different ways, they were always approached by someone they knew and were paid between EUR 100 and EUR 250 in cash per visit to Sweden. Some were subsequently asked whether they knew anyone else who might be interested in earning money in the same way, meaning that strawmen sometimes recruited additional individuals. In one case, an individual recruited others or misused their identities, reportedly receiving SEK 5,000 per digital bank ID.

  During the first trip to Sweden, they were taken to the National Tax Agency, where they registered as residents of Sweden and applied for an identity card. They understood little of what was taking place, as the person accompanying them interpreted the conversations and omitted relevant information. Generally, during a subsequent trip, they collected their identity cards and visited a bank to open accounts and apply for or install a digital bank ID on a smartphone provided to them.[111] The National Tax Agency occasionally questioned the registered residential addresses, while one bank 'offboarded' individuals, prompting further trips to Sweden to resolve these issues.

[111] When the strawmen were Swedish residents, they were typically instructed to remain available while the suspects remotely accessed their online banking.

- **Step 3: Creating a Bankgiro account number for invoicing**
  Many of the companies had a Bankgiro account number for invoicing, which made them appear more legitimate. Bankgiro is a proprietary clearing system used for transactions such as bill payments and is owned by several major banks in Sweden. Bankgiro conducts its own controls, and the case files indicate that a few companies lost their Bankgiro account before their bank accounts were closed or had their use restricted.

Activity

The client companies effectively purchased **'crime-as-a-service'** through the money-laundering companies. They contacted a telephone number, often operated by C3_X, or used chat platforms to order invoices, providing details of the work, specifications, and the amount to be paid. While some invoices contained information that was too superficial to withstand scrutiny by an experienced individual, others were sufficiently detailed and credible that their fraudulent nature would not be apparent from the invoice alone. At one point, the actors discussed the loss of a machine used to manufacture fake receipts, suggesting that they ordinarily provided this service as well. Some clients would only accept invoices issued by credible companies with an established history of activity.

Post-activity or post conditions

The main indicators of infiltration or criminal use were the scale of the payments, the numerous transactions between companies within the same network, the absence of genuine business costs, and the limited evidence of employees. The latter two would be expected if the client companies had actually paid for the services specified on the invoices. The companies therefore existed on paper, rather than as genuine businesses.

The **preliminary investigation** covers offences committed from Month 1 until the suspects' arrests in Month 21 (2024). However, there are indications that the scheme had been operating for several years before the start of the investigation. For example, C1_X had taken over from another individual, while several strawmen had visited Sweden as early as three years before Month 1. According to interviewees, the case is also connected to other cases involving companies used for similar purposes. Nevertheless, the overall scale of the operation remains unknown. The court established that the money-laundering companies had a combined turnover of almost SEK 400 million, while the preliminary investigation refers to SEK 500 million or more. More than twenty money-laundering companies were proven to have been used, while almost forty appear somewhere in the preliminary investigation, each for periods ranging from just under one month to seven months.

The Economic Crime Authority sought to arrest **seven suspects** simultaneously at several locations, with assistance from the police's national task force. Houses, cars, and offices were searched at the same time. According to one interviewee, this police unit is deployed when suspects are considered dangerous and/or when digital evidence needs to be secured quickly. One suspect was apprehended while attempting to delete chats from his phone. Under a European Investigation Order, the police in another EU Member State also assisted, conducting a search with Swedish personnel (of the Economic Crime Authority and Swedish Tax Agency) present. Subsequently, two foreign tax authorities interviewed several suspected strawmen, while neighbouring countries assisted in searches relating to the strawmen and the misuse of their identities. Ultimately, five individuals (C1_X, C2_X, C3_X, C4_X, and C5_X) were convicted with regard to the crime scheme. Substantial amounts were transferred

abroad, either to private individuals or, more commonly, to business bank accounts. Cryptocurrencies were also used, although these transactions were not traced or analysed beyond their transfer from the money-laundering companies' accounts.

4. Financial profile of the criminal network involved in Case X-Ray

Financing sources and start-up capital

The source of the funds used to establish the scheme remains unknown. However, they likely originated from illicit labour in the construction sector and commercial money laundering in previous operations. C1_X was, at one point, suspected of similar offences over a two-year period involving a comparable level of turnover. Another potential source of income was the underground banking system, including exchange and value-transfer services provided to immigrants and drug traffickers.

Payment methods and arrangements within the network

The scheme was largely built around transactions between company accounts held with both large and smaller banks. Some transactions were routed through private accounts, depending on the amounts and timing. Cryptocurrencies and cash transfers were also used, although their extent and purpose are difficult to determine. Currency exchange appears to have taken place mainly through the underground banking side of the business. The fictitious salaries paid to C1_X and C4_X may also have formed part of the payment arrangements, incentivising transfers from different company accounts to their personal accounts. Similarly, payments by multiple companies towards loans and expenses, particularly those of C5_X, may have functioned as another form of payment. Strawmen were generally paid in cash and were sometimes reimbursed for travel expenses through transfers from business accounts.

The network appeared to control **bank accounts** at most major Swedish banks, as well as several large European neobanks and banks in a number of Eastern European countries. However, accounts were sometimes frozen or closed by the banks, forcing the network to seek new accounts and strawmen with accounts at suitable banks. The actors also tried to keep track of which company accounts could be used, depending on their existing transaction flows. Some banks additionally restricted access when the same IP address was used to log into different individuals' accounts. These security measures made the scheme more difficult, costly, and stressful to operate. Furthermore, the use of **cryptocurrency** may have facilitated the transfer of criminal proceeds abroad, potentially below the radar of LEAs.

Costs of business operations

In general, the scheme was designed to reduce costs for the network by facilitating illicit labour and avoiding taxes and fees. By operating its own invoice factory, the network could control the costs associated with that part of the business. The operating costs were low and were largely covered by client companies and other customers. The operation was run from a residential building, with limited expenses for smartphones, digital bank IDs and strawmen. Strawmen were generally paid only a few hundred euros initially and could then be used for some time. A few had to return to Sweden when authorities or banks required them to appear in person, generating additional travel costs. Staff were paid, but the investigation suggests relatively low salaries.

Revenues and proceeds

The revenues and assets of the wider network across its criminal activities remain unknown. In Case X-Ray, however, the verdict estimates that C1_X received at least one-third of the 15-16% fee paid by clients. Some information in the case files suggests that he may have retained as much as 9-10% of the transaction value, using the remainder to pay intermediaries (C4_X and C5_X) and cover expenses. Thus, C1_X's revenues alone appear to have exceeded the operating costs. C1_X is estimated to have earned well over SEK 15 million in this case. C4_X and C5_X ultimately had amounts forfeited that were broadly comparable to those of C2_X and C3_X, although the prosecution had sought approximately ten times as much. Some assets, particularly cash, were seized during searches of the suspects' properties. The Economic Crime Authority also seized funds from bank accounts belonging to C4_X and C5_X. The estimated criminal proceeds described above were subject to extended confiscation. Funds were also seized from several company accounts.

5. Harms caused by Case X-Ray

Harms to individuals

The use of illicit workers and strawmen, who received only a few hundred euros in exchange for voluntarily providing digital banking credentials used in large-scale criminal activities, may cause harm to individuals. Strawmen were subsequently questioned by Swedish authorities and elsewhere in Europe. This caused stress and, in some cases, feelings of betrayal, particularly where recruiters had assured them that no one would be harmed or that their involvement would be limited to less harmful activities. The use of strawmen may also complicate accountability where workers, often foreign nationals, are injured. Although there is no indication that this occurred in Case X-Ray, Sweden's construction sector has reportedly been characterised by several fatal workplace incidents.

Harms to other businesses

The scale of the operation distorted competition in the construction sector. One interviewee assessed that prices were affected by the widespread use of undeclared labour, cash compensation schemes, and worker exploitation or, at minimum, poor working conditions.

Harms to public institutions

More than SEK 400 million was reportedly recorded as expenses by companies, supported by invoices containing false information. This reduced the tax liabilities of client companies, resulting in lost tax and social security revenue for the State. There are also indications that the reduced liabilities were not always paid. Such practices may further undermine confidence in control systems. Although not explicitly mentioned in the case file, fabricated income information could also result in wrongful welfare payments. Moreover, it may be used to avoid or complicate proceedings for so-called extended forfeiture.

Harms to the social environment

Strawmen were used on a large scale, with their identities exploited with relative ease. Several banks allowed suspicious, large-scale transactions associated with apparent money-laundering schemes in the construction sector to proceed. It took considerable time and financial resources before banks began rejecting transactions and closing accounts, potentially undermining public trust in the banking sector. Client companies were also suspected using of undeclared labour, while trade unions raised concerns about poor working conditions among their workers.

Annex 8.Y – Case Yankee: Money, Meat, and MTIC

1. Legitimate businesses involved in Case Yankee

Case Yankee appears to represent a relatively simple form of the MTIC fraud's scheme. It involves two companies in Sweden: **LTD2_Y**, the missing trader, which imports meat and sells it to **LTD1_Y**, which in turn supplies grocers and restaurants (see Table 19). At its simplest, the scheme began with the acquisition of LTD0_Y, a company of dubious character, by two men (C1_Y and C6_Y). C6_Y had a background in the meat industry and a history of using MTIC schemes, suggesting that the company was likely acquired with this purpose in mind.

Table 19
Overview of the businesses involved in Case Yankee (Stockholm)

Company	Economic sector	Status in 2025	Location
LTD0_Y	Selling meat	Became LTD1_Y	Stockholm Region, Sweden
LTD1_Y	After takeover by C1_Y and C6_Y: importing and selling meat	Bankruptcy (Year 3)	Stockholm Region, Sweden
LTD2_Y	Importing meat (*missing trader*)	Bankruptcy (Year 4)	Stockholm Region, Sweden

In many respects, LTD2_Y closely matches the definition of a **shell company** or missing trader set out in the EU Commission Regulation No 1925/2004. LTD2_Y displays many of these characteristics, although it was used for longer than would normally be expected. This may partly be explained by C1_Y and C6_Y apparently losing control of the scheme at an early stage (cf. *infra*). The purpose of the MTIC structure is to shield one company – in this case, LTD1_Y – from the illicit activity by using a missing trader as a buffer. However, LTD2_Y was managed so poorly that LTD1_Y was repeatedly forced to import meat directly. Data from the Tax Authority show that LTD1_Y imported meat worth between SEK 10 million and SEK 30 million annually.

2. Criminal network involved in Case Yankee

The actors surrounding LTD1_Y and LTD2_Y constituted a network in the definitional sense: a group of individuals engaging in criminal activities together (see Table 20). However, the boundaries of this network were unclear, with owners and associates coming and going and conflicts arising between them. It could therefore be more accurately understood as a broader **criminal environment**. The two key actors, C1_Y and C6_Y, appeared from the case file to have had loose ties – through friendship or family – to criminal groups, but there was no indication that they themselves were members of such groups. The most direct **link to organised crime** was through C5_Y, who was closely related to key figures in a major criminal group whose members originated in the Middle East and had a substantial diaspora in Sweden. The group was involved in narcotics trafficking, drug sales, and acts of violence, although its activities extended across various sectors and businesses, including restaurants. The original owner of LTD0_Y may also have been linked to the group.

Table 20
Overview of the core members of the criminal network involved in Case Yankee (Stockholm)

Member	Role	Gender
C1_Y	Sole board member of LTD1_Y and LTD2_Y (for a certain period of time); Withdrawing and introducing strawmen	Male
C2_Y	Investor and board member of LTD1_Y; Possibly unwitting strawman in LTD2_Y	Male
C3_Y	Board member of LTD2_Y; Strawman	Male
C4_Y	Accountant; Relative of C5_Y	Female
C5_Y	Investor and temporary CEO of LTD1_Y; Strongly connected to criminal organisations	Male
C6_Y	'Mastermind' of MTIC set-up; Operator behind LTD1_Y and LTD2_Y	Male
C7_Y	Early investor in LTD1_Y	Male
C8_Y	Strawman	Male
C9_Y	Owner of LTD0_Y acquired by C1_Y; Likely linked to criminal organisations	Male

- **C1_Y** and **C6_Y** were the main actors behind LTD1_Y and LTD2_Y and are considered the *de facto* owners by the Swedish authorities. They had previously worked together. C1_Y had been involved in numerous businesses and his family was active in several sectors, including the restaurant industry. C6_Y had likewise been involved in several previous businesses, some suspected of MTIC fraud, linked to food imports. He also had debts exceeding SEK 10 million with the Swedish Enforcement Agency.

  According to some reports, C6_Y was the architect of the split between LTD1_Y and LTD2_Y. Although he formally was an employee – and reportedly subject to a ban on running a business – he appears to have played a **key role** in the overall set-up, with his contacts among meat sellers across Europe enabling the scheme. Witnesses from LTD1_Y described C1_Y as responsible for drafting employment contracts, handling personnel matters, and managing administrative tasks, while C6_Y primarily handled sales, customers, and banking matters. C6_Y was involved from the outset and was a deputy board member. He was formally employed and paid by LTD2_Y from its inception until the third year, while also conducting sale activities for LTD1_Y.

- **C2_Y** was active in food retail in another part of Sweden and was brought in by C6_Y as the formal owner of LTD1_Y and LTD2_Y while the MTIC fraud was ongoing. He may have acted in good faith and may have been used by C1_Y and C6_Y to invest in the companies. Alternatively, the situation may have involved a dispute over money. During interrogation, he stated that he had assumed a board position to recover the money he had invested and that he wanted to withdraw from the businesses but had been threatened by C5_Y, who claimed that C2_Y owed him money.

- A change in the board of LTD2_Y was registered approximately one year after the company was founded, with **C3_Y** appointed as board member and **C8_Y** as deputy board member. Both had been registered on the boards of other companies operating in various sectors, including construction, removals, consultancy, cleaning, and welfare services. Most of these companies had substantial outstanding debts with the Swedish Enforcement Authority and had gone bankrupt. C3_Y had also been convicted of narcotics offences, had a history of drug abuse, and had no apparent connection to the business beyond his formal role.

There was a strong suspicion that C3_Y and C8_Y had acted as **strawmen**, which was supported by an employee who stated that they had never seen or heard of either of them. In its investigation, the National Tax Agency considered C1_Y to have been the actual operator behind LTD2_Y during the period in which C3_Y and C8_Y acted as strawmen. This assessment was based, among other things, on C1_Y having access to LTD2_Y's banking and accounting systems after C3_Y had been registered as a board member. Moreover, C1_Y continued to respond to the accountant's questions regarding LTD2_Y's salary accounting, financial results, and financial statements.

- **C4_Y** was an accountant and Authorised Tax Agent for LTD1_Y and LTD2_Y and had been brought in by C5_Y. She was a close relative of C5_Y and had been accused by others of acting on his behalf. Although she may have acted in good faith, the available information indicated that she had clearly aided and abetted these activities.

- The case material indicates that **C5_Y** viewed LTD1_Y as an opportunity to participate in a legitimate business. He appeared to possess substantial intimidation capital and had experience using violence, although this did not always enable him to get his way in the context of LTD1_Y and LTD2_Y. According to C6_Y, C5_Y was not himself a criminal but 'knew' people. Nevertheless, C5_Y was clearly able to draw on his family connections to recruit bookkeeper C4_Y, who assisted him, at times in conflict with other business partners. He also threatened and may have assaulted some of the other key actors.

3. Crime script based on Case Yankee

Motivation – Purpose

The primary motivation of the network involved in Case Yankee was clearly **financial gain**. However, interviews with the suspects also revealed, at times, an aspiration to run a business of their own. Although the business relied on illegal means to evade taxes, it may have represented, for some actors involved in traditional criminal markets, a step towards establishing a legitimate business. This may have been particularly relevant for C5_Y, who had extensive criminal connections, for whom cultivating a reputation as a 'legitimate entrepreneur' may have been an additional motivation. This could partly explain the conflict between C5_Y, on the one hand, and C1_Y and C6_Y, on the other: whereas the latter primarily viewed the business as a means of generating money, C5_Y appeared to regard it more as a long-term, legitimate business.

Preparation

Based on the interviews conducted, it appeared that criminal networks are heavily involved in the 'food industry', encompassing food production, import and export, wholesale, and retail.[112] In Sweden, oversight of imported food is divided among several agencies, including local municipalities, county

[112] Many of the businesses previously encountered by the municipality were located in a **warehouse district in Stockholm**, characterised by extensive imports of foreign food (including meat, fruit, and vegetables) for restaurants and 'immigrant food stores'. The area was widely regarded as a hub for organised crime and the criminal economy, including various forms of smuggling, with many of the most notorious networks – including the network involved in Case Yankee – being linked to it. The area was reportedly run-down, with containers arriving at night and leaving again by morning. Inspections by the police and other authorities had also revealed undocumented workers in the warehouses, some of whom were reportedly living on the premises.

administrative boards, and the Swedish Food Agency. Routine inspections rarely detect **food fraud**. Instead, such fraud is primarily uncovered through targeted operations. As noted in a recent report from the Swedish Food Agency, food fraud is often difficult to detect because it can be concealed within legitimate wholesale or retail operations (Livsmedelsverket, 2025). When violations are identified, authorities typically rely on administrative measures, such as formal warnings or bans on the sale of products. Moreover, it is highly profitable. The combination of a low risk of detection, high financial returns, and the ability to operate within legitimate businesses makes the food sector an attractive target for organised crime. In a broader sense, the EU system of deferred VAT on goods traded between EU Member States can be considered an enabling condition, alongside institutional shortcomings in the capacity of government agencies to identify and combat VAT fraud swiftly and effectively.

Today, Sweden is more dependent on imported food than at any other previous point (Livsmedelsverket, 2025). This longer, international, and increasingly interconnected supply chain also creates greater opportunities for food fraud, as each additional stage introduces a potential point of exploitation. According to representatives of tax authorities, **MTIC fraud involving meat** has long been among the most lucrative forms of fraud. The knowledge required to operate an MTIC fraud in the meat sector is reportedly widespread within certain criminal circles, most likely those connected to the previously mentioned warehouse district (see Footnote 112). C6_Y, in particular, appeared to have been familiar with this criminal environment and the MTIC fraud scheme. His previous businesses had also provided him with knowledge of EU-based companies from which meat could be sourced. He subsequently brought in individuals with sales experience to sell the meat to large Swedish companies.

Pre-activity or enabling conditions

The initial *modus operandi* involved acquiring a legitimate but indebted meat-trading company (LTD0_Y/LTD1_Y) with the explicit purpose of establishing an MTIC fraud scheme. To facilitate this, the company was divided into two entities, LTD1_Y and LTD2_Y, which operated from the same address for a period. A key element of the scheme was to distance the primary beneficiary (C1_Y) from the 'missing trader' company (LTD2_Y) by appointing strawmen board members with histories of bankruptcy and debt. The company was acquired for SEK 0. Although new financiers were initially attracted by what appeared to be a viable business model, operational control remained with the core individuals (C1_Y and C6_Y). Basic checks of customers and invoices were not carried out, contributing to the rapid failure of the business and subsequent non-payment.

During the COVID-19 pandemic, C1_Y invested in LTD0_Y, which was experiencing financial difficulties, and subsequently acquired the company with financing from a major Swedish bank through factoring. C1_Y was initially a co-owner with C7_Y before becoming the sole owner. Through the bank's factoring system, C1_Y, as the sole signatory for LTD1_Y, was able to register other individuals as authorised users in the bank's power of attorney register. He initially authorised himself and subsequently C6_Y, who made extensive use of this access. C6_Y became LTD1_Y's main contact with the bank and had also served as a deputy board member since the end of the third year. According to the bank, C1_Y and C6_Y used their access to create a system of false invoices, resulting in losses of up to several million SEK for the bank.

A few months after the acquisition, C7_Y also invested in the business. According to his interrogation, his other businesses had been severely affected by COVID-19, prompting him to diversify. He also began using his existing transport business to transport meat for the company. C6_Y reportedly told him that the company needed money to settle tax debts and was seeking financiers. C7_Y conducted due diligence and agreed to invest a substantial amount of money on the condition that he would take over LTD1_Y's customers. The investment was made in the company that subsequently became LTD2_Y. According to C7_Y, the business model appeared sound and legitimate. However, payment problems arose almost immediately, and he decided to withdraw at the end of the second month.

On paper, LTD0_Y appeared to have been a relatively well-functioning company prior to its acquisition by C1_Y, although it had substantial outstanding debt. Its activities included the purchase and sale of, among other goods, meat sourced from within the EU. The available files do not establish whether an MTIC fraud was already taking place within LTD0_Y at the time of its acquisition. One possibility is that LTD0_Y had been importing meat from another missing trader, and that C6_Y had identified an opportunity to control the entire chain by splitting the company into two entities. The two businesses, however, encountered difficulties very quickly, potentially as a result of their links to criminal networks.

Activity

The scheme relied systematically on **tax fraud** facilitated through LTD2_Y, which consistently and substantially underreported its output VAT liabilities across different management periods, with unreported amounts totalling millions of Swedish kronor (SEK) annually. The structure was facilitated by C1_Y's authority across both companies. C1_Y also shared this authority with C6_Y, and together they authorised hundreds of payments worth tens of millions for the two companies. Both actors were also involved in **credit fraud**. Using the authorisations registered in the bank's system, C1_Y and C6_Y repeatedly created false invoices and submitted them through the bank's factoring system, resulting in payments to LTD1_Y. The deliberate submission of both genuine and false invoices made it difficult for the bank to identify the fraudulent ones. In total, false invoices worth more than SEK 10 million were submitted, causing the bank losses of just over half of the amount.

The use of two parallel companies, one ostensibly legitimate and the other serving the fraudulent scheme, also created **operational confusion**. On paper, LTD2_Y imported meat and other goods, primarily from other EU countries, and sold them to LTD1_Y, which in turn supplied grocers and restaurants. In practice, however, several employees were reportedly unaware of LTD2_Y's existence, and much of the imported meat was delivered directly to LTD1_Y upon arrival in Sweden. Internal conflicts, threats, and the involvement of organised crime figures further complicated the operation, at times resulting in direct imports through LTD1_Y when LTD2_Y failed to function.

There are indications that C1_Y and C6_Y encountered difficulties with the set-up at an early stage, whether for financial, logistical, administrative, or other reasons. They brought in two additional investors and associates, C2_Y and C5_Y, although the reasons for their involvement were unclear. According to one witness, C1_Y and C6_Y stated that they urgently needed funds to pay outstanding taxes and therefore sought additional investment. By contrast, C2_Y and C5_Y stated that their involvement was intended to support the expansion of the businesses into other parts of Sweden. Although C2_Y joined the business as a part-owner and investor, he soon became involved in **conflicts**

over management, finances, and his role in LTD2_Y. He later sought to recover his investment and distanced himself from the businesses. C5_Y, who had also become increasingly involved, came into conflict with C1_Y and C6_Y over the management and financial difficulties of the businesses. Recovered communications indicated ongoing disputes over debts, payments, and responsibilities, including delayed payments to meat suppliers. C6_Y appeared at times to mediate between C1_Y and C5_Y, although his position was unclear.

Post-activity or post conditions

It is unclear exactly when or why the authorities began investigating LTD1_Y and LTD2_Y. However, during a tax audit, LTD2_Y was identified as a missing trader in relation to LTD1_Y, although the scheme appeared poorly administered. LTD2_Y repeatedly failed to report or pay VAT and did not declare several million SEK in output VAT on sales to LTD1_Y during the early accounting periods of the second year. The National Tax Agency also identified major EU acquisitions, frequent changes in the board, the use of strawmen, and numerous unusual invoices from LTD2_Y to LTD1_Y. Although the investigators remained uncertain about the precise nature of the financial dispute between C1_Y and C2_Y, they considered both responsible for the fraud committed. LTD2_Y's company tax approval was revoked at the end of the second year, and bankruptcy proceedings were initiated in the middle of the third year. By the beginning of the fourth year, its outstanding tax debt exceeded SEK 15 million. C6_Y attributed LTD1_Y's bankruptcy to a private conflict with C5_Y.

4. Financial profile of the criminal network involved in Case Yankee

Financing sources and start-up capital

The investigation did not examine the origin of the funds invested in the businesses. Substantial amounts of private funds and funds from other companies of the actors involved were invested by C1_Y, C2_Y, C5_Y, C6_Y, and C7_Y. The available evidence did not establish whether these funds derived from legitimate or illicit sources. It was therefore possible that the capital originated from a combination of both. LTD1_Y also obtained factoring finance from a major Swedish bank, initially with a maximum invoice facility of several million SEK, based on the available information on the company's accounts and operations.

Payment methods and arrangements within the network

Case Yankee reveals a mix of formal and informal financial arrangements. Some were documented through formal contracts, while others took the form of informal but established agreements within criminal networks. For example, according to C6_Y, the debt incurred by C1_Y towards criminal groups following the acquisition of LTD1_Y was informal. By contrast, the involvement of C2_Y and C5_Y was governed by formal agreements and legal documentation. More broadly, the boundaries between private and company funds appeared blurred, with significant problems surrounding payments, particularly from LTD2_Y to meat suppliers. During the period covered by the investigation, LTD1_Y made more than 1,000 payments totalling approximately SEK 150 million. Seven individuals were involved in executing these transactions, including C1_Y, C2_Y, C4_Y, C5_Y, C6_Y, and C7_Y.

Costs of business operations

Setting up the VAT fraud through two companies entailed greater costs, risks, and administrative, logistical, and legal complexity. The network surrounding LTD1_Y and LTD2_Y appeared unable to manage this complexity effectively. Both the legitimate and fraudulent aspects of the operation involved substantial costs, including premises, staff, transport, equipment, accounting services, payments to strawmen, and credit costs.

Revenues and proceeds

The revenues obtained by the individuals involved and their wider networks were not established. The available evidence nevertheless suggests that some investors and key actors may have lost money in the disorganised operation. The scheme also resulted in the bank paying out several million SEK against false invoices, none of which were repaid. It was not established whether these funds were reinvested in LTD1_Y and LTD2_Y, redistributed among the organisers, or used for other purposes.

5. Harms caused by Case Yankee

Harms to individuals

Throughout the various conflicts that have plagued the businesses, there have also been threats and even physical assaults directed at some of the owners and employees. These incidents have sometimes involved other criminally connected owners, while on other occasions they have involved outsiders. In this sense, the highly involved individuals can be regarded as both perpetrators and victims. One employee who worked in sales was dismissed after just over two years, reportedly because he was considered to be 'troublesome' after requesting his holiday pay. The strawmen who have been recruited and paid have most likely used the money to finance their drug use.

Harms to other businesses

Clearly, by avoiding the payment of VAT on its imports, LTD1_Y had gained a substantial market advantage over its legitimate competitors. This enabled it to offer lower prices and capture market share. If such practices are scaled up, they may ultimately eliminate competition within the industry. If they become sufficiently widespread and are combined with other forms of fraudulent behaviour, they could potentially undermine an entire industry. The extent to which this type of VAT fraud occurs across the meat sector more generally, and in relation to the specific types of imported meat concerned in Case Yankee, remains an open question. There is also a risk that the use of criminal methods, such as intimidation and violence, in business activities may undermine trust within the sector. This, in turn, could reduce the willingness of businesses to engage with new business partners or to purchase companies operating within this sector.

Harms to public institutions

Case Yankee involves substantial tax losses and required considerable time and financial resources to investigate. There may are also be potential harm in terms of diminished public trust in public institutions when such a scheme can be implemented and operated for such an extended period without detection, particularly when it is not conducted in a particularly sophisticated manner.

Harms to the physical environment

While the investigation does not identify any direct harm to the physical environment, it can be argued that Case Yankee has further reinforced the perception of the storehouse area as a shady place (see Footnote 112). The area already had a reputation as a hub of illicit activity and organised crime.

ANNEX 9

UTRECHT

DETAILED CASE STUDIES

Annex 9.Z – Case Zulu: The Gold Trading Landscape

1. Criminal network involved in Case Zulu

Available information suggests that the involvement of criminal networks in the jewellery and gold trading sector primarily concerns the use of legitimate businesses as **facilitating structures**. Rather than being fully embedded within a single criminal organisation, jewellers and gold traders may act as service providers that enable specific financial transactions for criminal actors, as indicated by respondents. The structure of the sector may contribute to this dynamic (cf. *infra*). The prevalence of small-scale enterprises and sole proprietorships, often combining retail, second-hand trading, and gold purchasing activities, creates an environment in which individual businesses operate with considerable autonomy and where high-value transactions are part of normal business practice.

2. Legitimate businesses involved in Case Zulu

Gold trading does not fall within a single, clearly defined economic category in the Dutch classification system. The legitimate structure of the jewellery and gold trading sector is primarily rooted in retail, with many businesses operating as small-scale enterprises that combine multiple commercial activities within a single establishment. These businesses typically sell watches and jewellery. A total of 3,970 businesses were registered in 2025 with **jewellery retail** as their primary activity (CBS, 2026b). Of these, at least 75% appear to operate as sole proprietorships and small enterprises with limited staff, highlighting the sector's highly fragmented structure. Pawnbroking and other forms of short-term lending also appear to be intertwined with these activities. As businesses often operate across multiple 'stages' of the gold value chain, this complicates oversight and may increase the sector's vulnerability to criminal use.

Alongside these traditional jewellery retail activities, businesses in this sector may also trade in second-hand goods, including the purchase of scrap gold from private individuals, which constitutes an important source of gold entering the secondary market. Consequently, the boundary between jewellery retail and **gold trading** is often blurred in practice. However, businesses specialising in the wholesale of metals and metal ores remain relatively scarce. Nationally, only 45 companies are registered with this activity as their primary activity, suggesting that large-scale or specialised gold trading is concentrated among a limited number of actors. A similar pattern is observed in Utrecht, where approximately 120 businesses are registered primarily as jewellery retailers, compared with only five registered as wholesalers of metals, including gold.

The gold value chain comprises multiple interconnected stages, including extraction, refining, trade, manufacturing, retail, and recycling. Its circular nature, whereby gold can be repeatedly melted down and reintroduced into the market, creates multiple entry and exit points through which illicit assets can be integrated and legitimised. This structural characteristic complicates oversight and facilitates the commingling of licit and illicit flows (NSOC, 2023). Within this system, several recurring forms of criminal use can be identified. One involves relatively straightforward **money laundering** through the conversion of criminal proceeds into gold products, such as jewellery or watches, which can subsequently be resold. Gold is also used in **underground banking** systems, where value is transferred across borders through the physical movement of gold, often facilitated by intermediaries such as jewellers or gold traders.

More complex forms of criminal use include **fraudulent trade schemes** in which gold and jewellery are repeatedly imported and exported to facilitate value transfer, invoice manipulation, and the commingling of licit and illicit goods. Criminal actors may also operate at earlier stages of the value chain, for example by investing in mining activities or exploiting export processes to introduce illicit funds under the guise of legitimate production or logistics. Finally, the gold trade is used in investment fraud, including fictitious transactions and schemes involving non-existent gold assets (NSOC, 2023).

3. Crime script based on Case Zulu

Motivation – Purpose

The primary motivation for the criminal use of businesses in the jewellery and gold trading sector is their potential to facilitate money laundering. The sector provides opportunities to introduce, transform, and integrate illicit proceeds into the legitimate economy, making it particularly attractive during the financial phase of organised crime activities (NSOC, 2023). The illustrative case discussed above potentially exemplifies this role, as the jeweller is suspected of facilitating money laundering (Politie, 2025).

Preparation

Several characteristics of jewellery shops and the gold trading sector constitute structural vulnerabilities. At the sectoral level, the gold trade offers additional advantages for criminal actors. Gold and watches function as compact stores of value, allowing substantial wealth to be transported discreetly across the borders or within domestic markets. Once melted, gold becomes extremely difficult to trace, effectively obscuring links to its original (criminal) source. Moreover, the continued prevalence of cash payments within the sector further reduces **traceability** and increases its attractiveness for laundering illicit proceeds.

Regulatory mechanisms intended to enhance transparency can also be subject to **manipulation**. The Digital Trader's Register (DOR), a registry designed to record transactions involving second-hand goods, relies heavily on accurate and consistent registration by traders (CCV, 2026). In practice, incomplete, delayed, or deliberately omitted entries undermine its effectiveness as a control instrument. Repeated non-compliance may persist over time, as administrative enforcement often targets physical premises rather than the underlying business structure. Consequently, even when authorities close a shop at a specific location, the business may relocate and continue operating, allowing criminal use to persist with limited disruption.

In addition, at the level of individual businesses, the buying and selling of jewellery, watches, and gold provide a **credible commercial front** with high turnover, allowing illicit proceeds to be integrated into seemingly legitimate revenue streams. The presence of high-value goods enables substantial amounts of money to be channelled through a limited number of transactions, reducing vulnerability.

Pre-activity or enabling conditions

Regarding the degree of criminal use of businesses within the jewellery and gold trading sector, available information does not allow for firm generalisations. Respondents indicate that, while some actors may structurally facilitate illicit activities, it often remains unclear whether this results from deliberate involvement or gradual entanglement over time. Nevertheless, failure to register goods in the DOR can remove a crucial audit trail for gold purchases and sales, enabling unreported transactions and the disposal of illicit gold or valuables outside regulatory oversight.

Activity

As noted above, the criminal use of businesses within the jewellery and gold trading sector is primarily characterised by their role as facilitating structures in the financial processes of organised crime. Rather than operating as independent criminal enterprises, such businesses may be used to move and launder illicit value through seemingly legitimate commercial activities (NSOC, 2023). Various recurring *modus operandi* enable the conversion, transfer, and legitimisation of illicit proceeds. One commonly identified method involves relatively straightforward forms of **money laundering** using gold and jewellery (NSOC, 2023). In this model, criminal proceeds originating from activities such as drug trafficking, fraud, or cybercrime are used to purchase gold, jewellery, or luxury watches through jewellers or related actors. These transactions may occur in physical shops or via online platforms. The acquired goods can subsequently be resold, allowing the proceeds to re-enter the financial system under an apparently legitimate origin. Through this process, illicit funds are transformed into physical assets and subsequently converted back into monetary value, obscuring their criminal source.

In addition to direct purchase and resale, interviewees indicated that transactions may be structured through administrative mechanisms. One potential *modus operandi* involves the creation of **fictitious invoices**, creating the appearance of legitimate trade in gold or jewellery. In such cases, a business owner may record transactions suggesting the purchase or sale of goods, while in reality these transactions serve to legitimise previously acquired illicit funds. This constitutes a form of trade-based money laundering (TBML), whereby criminal proceeds are distinguished and value is transferred through trade transactions to create the appearance of legitimacy (FATF, 2006).

Another observed practice concerns the conversion between different forms of value, as some businesses may facilitate exchanges between **cash** and digital assets (Politie, 2025). For example, cryptocurrency ATMs can be used to convert cash into cryptocurrency or *vice versa*. Although such services are not unique to the jewellery sector and also occur in other contexts, their presence within businesses dealing in high-value goods may provide an environment in which substantial transactions can take place. Furthermore, as noted above, the **recyclability of gold** itself contributes to the sector's vulnerability (NSOC, 2023). Gold can be melted down and reintroduced into the value chain, removing identifiable characteristics of the original product. This process can obscure the origin of the gold derived from illicit sources, such as theft or other criminal activity. Once reintroduced, the gold may be traded within the legitimate market, facilitating the commingling of licit and illicit flows.

Post-activity or post conditions

The post-activity phase of criminal use within the jewellery and gold trading sector is characterised by limited visibility and **challenges** in determining the duration and extent of such criminal use. Due to the embedded nature of these activities within legitimate business operations, it is often challenging to establish how long a business has been used for criminal purposes or whether the business was established with criminal intent from the outset.

Signals of criminal use may include **inconsistencies** in administrative records, irregular transaction patterns, or repeated non-compliance with regulatory obligations, such as registration requirements (i.e., DOR in the Netherlands). Indicators may also relate to transactions that are disproportionate to the size and profile of the business, or to the presence of services that facilitate value conversion more broadly. However, detecting such signals depends heavily on proactive controls, inspections, and effective information-sharing between authorities.

Administrative interventions ca be applied at the level of individual businesses. One such measure is the temporary closure of business premises by local authorities where sufficient indications exist that a business facilitates criminal activity or poses a risk to public order. Such interventions may disrupt ongoing operations and were applied in an illustrative case in which a jeweller's premises were closed for twelve months (Schouten, 2025).

4. Financial profile of the criminal network involved in Case Zulu

The financial profile of criminal activity within the jewellery and gold trading sector is difficult to assess in general terms, due to the concealed nature of financial flows and the strong reliance on case-specific information. Available evidence suggests that the sector primarily functions as a facilitating environment for the movement and transformation of illicit value, rather than as a direct generator of criminal profits. Financial gains associated with the criminal use of such businesses are therefore more likely to take the form of service-based income, such as commissions, transaction margins, or fees related to the conversion, transfer, or integration of illicit value. However, the extent of this financial profile, including the scale of potential revenues, cannot be determined at sector level.

5. Harms caused by Case Zulu

Harms to individuals

Within the jewellery and gold trading sector, risks to individuals may arise in relation to employment practices. Given the prevalence of small-scale enterprises and sole proprietorships, there is a potential for informal or undeclared labour arrangements. Such arrangements may leave workers without legal protections, including social security coverage, employment rights, and access to formal dispute resolution mechanisms. This, in turn, may increase their vulnerability to exploitation and precarious working conditions, even in contexts that may outwardly appear legitimate (European Commission, 2023b).

Harms to other businesses

The criminal use of the sector for financial crime can distort fair competition within the market. Businesses that benefit from illicit financial flows may gain advantages that are not accessible to compliant actors, such as access to additional capital, the ability to absorb financial losses, or the capacity to operate in more commercially attractive locations. In particular, access to financial resources outside the formal financial system, such as underground banking, may enable businesses to operate in ways that would not be economically viable under normal market conditions. This can place legitimate businesses at a structural disadvantage, thereby contributing to unfair competition and potentially resulting in market displacement.

Harms to public institutions

The use of businesses for money laundering or other forms of financial crime can undermine public institutions, particularly in the area of taxation. When transactions are not properly recorded or declared, this may facilitate tax evasion and reduce the public revenues available for government expenditure. Beyond the resulting financial losses, such practices can also undermine trust in regulatory systems and compliance frameworks. If businesses are perceived to operate outside established rules without consequence, this may erode the credibility of oversight mechanisms and, in turn, reduce overall compliance within the sector.

Harms to the social environment

The criminal use of legitimate businesses can affect the social environment, particularly with regard to trust and perceived safety. When criminal activities become embedded within everyday commercial settings, this can blur the distinction between legitimate and illegitimate enterprises. Even in the absence of direct victimisation, the presence of criminal activity within local businesses may contribute to a perceived decline in public order and safety. Moreover, signals such as irregular activity, increased attention from authorities, or administrative interventions, including the closure of business premises, may shape how residents and other local stakeholders perceive the safety and integrity of their surroundings.

Annex 9.AA – Case Alfa-Alfa: Fraudulent Healthcare[113]

1. Criminal network involved in Case Alfa-Alfa (AA)

Assessing the size of the network involved in Case Alfa-Alfa (AA) is challenging, as it depends on how a 'criminal network' is defined. Respondents indicated that organised healthcare fraud is relatively easy to perpetrate. Once an effective *modus operandi* has been identified, it tends to spread rapidly within criminal milieus. However, this diffusion does not necessarily imply direct collaboration, despite the use of shared and **interconnected methods**. Furthermore, these fraudulent businesses often rely on the same service agencies, enabling offenders to identify suitable facilitators for their schemes. Respondents stated that criminal networks involved in healthcare fraud, including the one examined here, generally operate independently while sharing *modus operandi* within social circles, sometimes linked by ethnicity or geographic location.

[113] The analysis of Casa Alfa-Alfa (AA) is based on two interviews and the analysis of the judicial record.

The network involved in Case Alfa-Alfa (AA) primarily consisted of **family members** and individuals from their social circle, who shared in the profits, while others were victims of inadequate healthcare. The operation was led by three brothers, with clearly defined roles.

- **C1_AA** managed the company's formal structure and served as its legitimate public face. In this role, he handled administrative obligations, maintained contact with authorities when required, and ensured organisational continuity when the company came under limited scrutiny.
- **C2_AA** was primarily responsible for recruiting clients, relying on the family's social network and community ties, particularly within migrant communities from Turkey. Many recruited clients had limited proficiency in Dutch, low administrative capacity, or were dependent on local social networks, making them more susceptible to involvement in the fraudulent scheme.
- **C3_AA** oversaw invoicing, claims, time-registration systems, and the creation of fictitious care records, enabling the systematic manipulation of care hours and payment flows.

Funding intended for individual healthcare was channelled through at least 47 budget holders or representatives who received **personal care budgets** (PGB) on behalf of other care recipients. A personal care budget (in Dutch: *Persoonsgebonden Budget*) is an alternative to municipally organised care provision, enabling budget holders, or their representatives, to arrange care independently and select their own care providers. It is intended for individuals with an illness or disability requiring long-term care or support and is based on the principle of empowering budget holders to organise care according to their own needs and preferences.

To receive a PGB, the person requiring care, or their representative, must be capable of managing the budget and the responsibilities associated with arranging and coordinating care providers (Rijksoverheid, n.d.). Within the network involved in Case Alfa-Alfa (AA), **budget holders** were predominantly representatives of individuals with genuine care needs. In this case, many shared in the company's profits through the distribution of publicly funded care budgets between the three brothers and the budget holders. According to respondents and the judicial case file, most budget holders belonged to the same ethnic community and were part of the family and social network of C1_AA, C2_AA, and C3_AA. In cases of healthcare fraud, budget holders are often indirectly involved in the care provider's criminal activities. However, recent prosecutions of multiple budget holders associated with this company indicate that the Public Prosecutor considers them to have a **direct role**. By sharing in the profits and knowingly accepting that the people they represented – mostly family members – did not receive genuine, adequate care, they actively contributed to the organised healthcare fraud scheme. This interpretation was upheld by the court, which convicted multiple budget holders of joint fraud, resulting in fines and community service orders.

Although respondents estimated that the organisation employed approximately ten to fifteen staff members to provide home-based and day care, the judicial case file suggests that their actual role and function was far more limited and ambiguous. While the case file contains no dedicated employee records, its financial and operational analyses provide valuable insight into the **role of personnel** within the fraudulent scheme.

- First, personnel costs were exceptionally low compared to sector norms, suggesting that the number of genuinely active care workers was substantially lower than the reported workforce. This discrepancy further indicates that some individuals listed as employees may have had only a nominal role **without providing genuine care**. Although some employees stated during the investigation that they believed they were delivering legitimate care, the Inspectorate's reconstruction showed that the organisation could have provided only a fraction of the care claimed. This indicates that even those who performed care-related tasks were structurally unable to deliver the volume of services reported.
- Furthermore, the organisation strategically incorporated **pseudo-employees**, including relatives or acquaintances of clients, who were registered as care workers but performed no actual duties. Collectively, personnel fulfilled a dual function within the criminal enterprise. First, a small core of ostensibly genuine care workers helped maintain the appearance of legitimacy, although it remains unclear to what extent they were aware of the fraud. Second, a broader group of nominal or complicit staff, largely comprising relatives of budget holders or the budget holders themselves, helped conceal the scale of the fraud.

2. Legitimate businesses involved in Case Alfa-Alfa (AA)

The healthcare company in this case (**LTD1_AA**) was established in 2014 as a private limited company providing home and day care services. It was managed by three brothers (C1_AA, C2_AA, C3_AA), who jointly acted as the company's representatives. Respondents estimated that the organisation employed approximately ten to fifteen care workers responsible for visiting clients' homes to provide care, as the judicial case file contains no employee records or staffing overview. In addition to home care, the company also operated a day-care centre under the same legal entity.

In addition, the judicial case file refers to another business venture based on multiple transactions made by C3_AA to a construction project management company (**LTD2_AA**) for the development of an apartment complex in Turkey. However, little is known about the scope of the project or the business behind it.

3. Crime script based on Case Alfa-Alfa (AA)

Motivation – Purpose

The healthcare business (LTD1_AA) was primarily used for criminal purposes because it offered a relatively low threshold opportunity to **generate substantial revenues** from publicly funded care schemes while converting these funds into seemingly legitimate cash and assets. In this case, the business model facilitated systematic fraud by claiming reimbursement for care that was either not provided or delivered at a substantially lower level than declared. Beyond direct financial gain, respondents and the judicial case file indicated that healthcare companies may also be used to facilitate financial positioning within the legitimate economy, for example by creating administrative records to support credit or mortgage applications through fictitious employment arrangements.

Beyond this case, respondents described a broader pattern in which some actors involved in organised crime use healthcare businesses to integrate or redirect illicit funds into enterprises receiving legitimate income from municipalities or health insurers. In the Utrecht context, this pattern involves individuals who are simultaneously active in healthcare and other criminal markets.

Preparation

The healthcare sector in Utrecht faces significant social and structural **challenges**.[114] A key issue is the persistent shortage of personnel, despite overall economic growth. At the same time, an ageing population is increasing the demand for care, while a substantial share of the current workforce is approaching retirement (Koning, 2024). Utrecht has prioritised the healthcare sector for several years, supported by a relatively strong information base on the criminal use of the legal economy. In 2023, for example, 338 signals concerning 293 healthcare providers were registered nationally (IKZ, 2024). Common forms of fraud include 'ghost care': declaring care that was never provided, invoicing more hours than delivered, or deploying unqualified personnel (cf. *infra*).

Furthermore, van der Torre and Jongepier (2021) identified concerning indications of links between healthcare and organised crime in Utrecht. These included the use of the sector for money laundering, tax fraud, and healthcare fraud, as well as the potential role of healthcare training institutes as recruitment grounds and the exploitation of vulnerable individuals in care institutions. The study concluded that the sector's complexity and legal constraints create structural vulnerabilities: providers seeking to commit fraud can exploit gaps in legislation and policy, while existing oversight mechanisms and the municipality's information position leave considerable scope for improvement.

As noted above, criminal exploitation of the healthcare sector is facilitated by structural and institutional conditions that hinder effective intervention by authorities. A key enabling factor is the operational **complexity** of **addressing fraudulent care providers**: once under scrutiny, providers may dissolve their legal entity, relocate operations, or transfer their client base to another company. As inspections and investigations require a clear and stable overview of a provider's activities and administration, such organisational mobility can disrupt oversight processes and require authorities to reassess the situation from the outset. Moreover, relocation to another municipality can further fragment oversight.

A second enabling condition concerns the sector's **financing and oversight architecture**, particularly in the context of non-contracted care and personal budgets. Health insurers are described as having limited direct oversight of non-contracted care, and new providers can enter the market with limited prior, issue invoices, and receive payments that are often processed on a trust-based basis. This creates opportunities for fraudulent providers to establish profitable arrangements with clients or budget holders, particularly when administrative capacity to verify care delivery is limited. Moreover, long-term care involves substantial budgets and requires an eligibility assessment. However, once granted, this indication is often permanent.

[114] The healthcare sector comprises approximately 3,951 healthcare institutions and, by 2025, around 94,500 workers in the broader Healthcare and Wellbeing domain (Patiëntenfederatie Nederland, n.d.; UtrechtZorg, n.d.). A notable development is the growth of self-employed care workers, with the number of independent professionals increasing by approximately 81% over the past decade. This trend is primarily attributed to a desire for greater control over working hours, improved work-life balance, and the provision of higher-quality care (CBS, 2026a).

Furthermore, social and cultural opportunity structures may facilitate **target selection** and recruitment strategies. Criminal networks may exploit populations they are part of, particularly where access to care is hindered by language or cultural barriers, age, illness, or limited administrative capacity. In these contexts, individuals may become dependent on their social networks to arrange care, increasing their vulnerability to fraudulent arrangements or participation in profit-sharing models. Administrative enforcement at municipal level is further complicated by the **'double intent' requirement** described by respondents: action against both the provider and the personal budget holder requires intent to be demonstrated for each party. In practice, this creates a significant barrier, particularly when providers and budget holders protect one another through aligned narratives and mutual interests.

Pre-activity or enabling conditions

The business (LTD1_AA) had a client base of approximately one hundred people requiring a specific type of care. It remains uncertain whether the business was established with legitimate intentions or primarily to facilitate organised fraud. However, given the fact that the offences continued for three to four years and that the business was established around 2015, it is likely that it was set up as a premeditated fraudulent enterprise. Furthermore, it is known that the organisation actively recruited individuals in need of care services through their social network. It is possible that the initial client base was part of the scheme from the outset and received little, if any, actual care, as they may have received a share of the care funds in exchange for their silence.

A key enabling factor was the division of labour among the three brothers (C1_AA, C2_AA, C3_AA), which allowed the fraud to operate efficiently and with limited external scrutiny (cf. *supra*). Moreover, the network specifically targeted individuals eligible for a personal care budget (PGB) who experienced difficulties navigating administrative procedures or arranging appropriate care. These vulnerabilities were exploited through personal approaches and promises of mutual financial benefit. Once recruited, **agreements with PGB holders** were established at an early stage. These arrangements, including the specific share of care funds to be returned to the business, were documented in a 'distribution list' detailing the percentages paid back to the network. Some clients reportedly received little or no actual care, accepting the arrangement in exchange for direct cash payments.

Activity

During the operation of the legitimate business, the network provided **little to no actual care services**. C3_AA, responsible for administration, manipulated the care registration system to record fictitious care hours. These declarations included hours that were never delivered, inflated hours exceeding the actual care provided, and uniform patterns of claimed care across multiple clients, indicating structural manipulation. The falsified hours were subsequently invoiced to insurers or municipalities under the relevant healthcare frameworks. One respondent stated: "Where thirty hours of care should have been delivered, clients would only receive ten hours." A behavioural signal that attracted investigative attention was the pattern of clients visiting the premises on the same date each month. These visits were unrelated to care, meetings, or legitimate services. Instead, they coincided with monthly payment moments during which clients collected their share of the fraudulently obtained funds. Moreover, the care provided was often superficial, consisting of simple tasks such as making coffee and assisting with household tasks rather than appropriate care and nursing.

Post-activity or post conditions

The investigation into the legitimate healthcare businesses began in late 2017 and culminated in a criminal trial concluded in 2019. The **investigation** combined financial analysis, administrative records, witness statements, intercepted communications, and digital evidence. Investigators examined company accounts, client files, payment records, WhatsApp conversations, and recorded communications between key individuals involved in the organisation. According to the judgment, evidence from these sources, together with statements from budget holders and their relatives, ultimately demonstrated that substantial amounts of care had been billed but not delivered and that part of the PGB funds had been shared with clients.

A key finding was the discovery of a distribution list documenting approximately one hundred arrangements between the healthcare provider and individual clients. These arrangements specified the percentage of healthcare funds to be shared per client. Furthermore, it was established that approximately EUR 1 million derived from healthcare funds was invested in the construction of an apartment complex in Turkey. Ultimately, the court convicted multiple budget holders of joint fraud, resulting in fines and community service orders.

4. Financial profile of the criminal network involved in Case Alfa-Alfa (AA)

Payment methods and arrangements within the network

In Case Alfa-Alfa (AA), the clients of the legitimate business were involved in the fraudulent scheme. This involved arrangements whereby healthcare funds were divided between the provider and the client. For example, when a client received EUR 4,000 in healthcare funds and the agreement specified a 50% split, EUR 2,000 was retained by the client and EUR 2,000 by the healthcare provider. Furthermore, one of the brothers was on the payroll despite not carrying out any actual work for the company.

Additionally, **cash** withdrawn from company funds played a central role in compensating clients and paying certain staff. Clients received their agreed-upon share in cash, limiting traceability. These payments were often made from the healthcare budget received by the company. Some staff members were also paid in cash, raising concerns about the origin of these funds. Furthermore, cash also facilitated laundering mechanisms within the network, as illustrated by the investment of approximately EUR 1 million in apartment construction in Turkey.

Costs of business operations

According to the criminal court judgement, personnel costs constitute the largest expense in operating a healthcare company. Therefore, significantly lower personnel costs compared with other companies in the sector may indicate that little or no care was provided. Across relevant publications, average personnel costs account for approximately 71% of healthcare sector revenues, whereas the network's costs represented only 8.2%, 9.6%, and 11.3% of revenue in 2014, 2015, and 2016, respectively.

Revenues and proceeds

Of the EUR 4.67 million in PGB-funded care that formed the basis of the fraud, the court concluded that a substantial proportion did not correspond to care that had actually been delivered. The court found that the healthcare provider could have delivered, at most, 28.1% of the care that had been invoiced. Consequently, a substantial share of the PGB-funds received was not associated with the provision of actual care. A portion of these funds was distributed to budget holders, while other amounts were withdrawn, transferred to private individuals, or invested in Turkey.

5. Harms caused by Case Alfa-Alfa (AA)

Harms to individuals

Individuals requiring care, often on a 24-hour basis, are particularly vulnerable due to their high degree of dependency on others to manage their daily affairs. This dependency was systematically exploited. In terms of the care actually provided, services were frequently inadequate or of poor quality. In some instances, care was delivered by self-employed staff who were found to hold falsified qualifications. Such practices posed an immediate and serious risk to the health and safety of clients. Court proceedings against the budget holders were described as 'hard to sit through', as many of the individuals, whether represented by legal guardians or acting on their own behalf, clearly required genuine care that had not been adequately provided.

Harms to other businesses

Bona fide healthcare businesses face increased administrative burdens as a result of governmental efforts to combat fraud. Moreover, the use of self-employed caregivers who are paid under the table creates unfair competition for legitimate healthcare providers. Fraudulent businesses can also cause reputational damage to the healthcare sector as a whole. In addition, genuine caregivers have been observed leaving organisations due to the involvement of problematic figures.

Harms to public institutions

Most healthcare is financed through the money of taxpayers. When information emerges about the ease with which fraud can be committed and substantial amounts of public money can be obtained fraudulently, this can undermine trust in public institutions and raise questions about what taxpayers are ultimately paying for. Rough estimates provided by respondents reveal that almost ten percent of the entire healthcare budget in the Netherlands may be defrauded in some form. This represents a substantial drain on the tax system.

Harms to the social environment

Fraudulent healthcare providers are believed to be one of the factors contributing to rising insurance premiums, based on the assumption that healthcare costs increase due to funds being lost to fraud.

Annex 9.BB – Case Bravo-Bravo: From Showroom to Shadow[115]

1. Criminal network involved in Case Bravo-Bravo (BB)

The criminal network centred around **C1_BB**, who operated a car-related business and was identified by the court as the leader of an organisation involved in the preparation of large-scale cocaine trafficking. It comprised multiple individuals performing roles related to the logistics and facilitation of **drug trafficking**. However, the available judicial record provides limited insight into the network's structure beyond C1_BB's central role. Although the court established that the suspect led and participated in a criminal organisation involving multiple individuals, the judgement did not specify their identities or operational roles.[116] Nevertheless, the court concluded that several individuals engaged in a structural collaboration to facilitate the trafficking and distribution of cocaine.

Within this network, C1_BB played a coordinating and leading role. Using **encrypted communication** platforms such as SkyECC, he maintained contact with various actors involved in preparing drug trafficking operations. These communications concerned logistical arrangements, including pricing, quantities, transportation, storage, and payment for narcotics. The network's activities included maintaining contact with transporters and intermediaries, coordinating meetings and agreements concerning drug shipments, providing instructions, information, and financial resources to other participants, and facilitating logistics, including storage and transport arrangements. These activities indicate a relatively structured collaboration in which participants performed distinct roles. It is therefore likely that additional companies in the transport and logistics sector were involved but were either not included in the verdict or omitted from the judgement due to the procedural agreements. In addition to the drug-related activities, C1_BB managed at least part of the criminal proceeds through the associated business.

2. Legitimate businesses involved in Case Bravo-Bravo (BB)

According to the judicial case file, C1_BB operated a car-related business (**LTD1_BB**) alongside his criminal activities. The judgement did not specify the company's legal form, size, number of employees, or the precise nature of its automotive services. However, it indicated that the business was involved in the acquisition and handling of vehicles, suggesting activities in the automotive trade or related services.

LTD1_BB appears to have played a key role in the financial narrative constructed by C1_BB during the investigation. When confronted with money laundering allegations, he sought to justify the ownership of several vehicles by presenting invoices and consignment agreements, suggesting that the vehicles had been legitimately sold or held on consignment. In this way, the business was used to manage **high-value assets** and financial transactions that concealed their criminal origin. Beyond this, the judgement provides little information about LTD1_BB's operational activities. It therefore remains unclear whether the company functioned as a genuine commercial enterprise or primarily as a façade to legitimise the acquisition and possession of vehicles.

[115] The analysis of Case Bravo-Bravo (BB) is based on the available judicial record from 2025.

[116] This lack of detail reflects the abbreviated nature of the judgement, which omits the evidentiary record following procedural agreements between the prosecution and the defence.

3. Crime script based on Case Bravo-Bravo (BB)

Motivation – Purpose

In Case Bravo-Bravo (BB), the legitimate automotive business (LTD1_BB) appears to have primarily served as a means of legitimising assets derived from criminal activities, rather than as the setting in which the offences were committed. The criminal network led by C1_BB was primarily involved in preparing large-scale **cocaine trafficking**, while the business provided a context for concealing and justifying high-value assets, including vehicles. The business enabled C1_BB to present an apparently legitimate explanation for the possession and transfer of vehicles that the court identified as proceeds of crime. The judicial case file therefore indicates that the business functioned as a supporting structure for **money laundering**, facilitating the integration of criminal proceeds into an outwardly legitimate vehicle trading environment.

Preparation

The automotive sector can **attract criminal actors** in several ways.[117] On the one hand, it provides opportunities for storing and transporting illicit goods, such as drugs, and for acquiring vehicles used in bombings ad targeted killings. On the other hand, large-scale investigations indicate that companies in the sector may be exploited for extensive VAT fraud. A 2023 investigation found that companies may convert VAT-liable vehicles into margin scheme vehicles, resulting in reduced VAT payments. This process is suspected to involve the use of falsified purchase invoices (FIOD, 2023).

Furthermore, criminals exploit structural and operational characteristics of the sector that make it vulnerable to **money laundering**. Research shows that offenders frequently use large amounts of cash to purchase vehicles in bulk and subsequently export them, a method known as ‘cash integration’ (ten Dam, 2021). Vehicles are particularly suited to this purpose due to their high value, rapid tradability, and relatively limited oversight in international trade. This enables criminals to integrate illicit proceeds into the legitimate economy, as international vehicle trading provides a low-threshold means of legitimising criminally obtained cash.

These opportunities are reinforced by the structural characteristics of the automotive sector. The market consists of a large number of small and medium-sized enterprises, ranging from individual traders to mid-sized dealerships, with varying levels of administrative organisation and regulatory compliance. This fragmented structure contributes to inconsistent oversight and uneven implementation of due-diligence measures. Recent national and international cases of fraud and money laundering demonstrate how these vulnerabilities enable criminals to exploit automotive businesses as transactional channels and fronts for concealing illicit financial flows (NVB, 2024; van der Veen & Heuts, 2024).

[117] In the Province of Utrecht, 2,925 companies were registered with the Chamber of Commerce under the classification “sale and repair of motor vehicles”. This figure excludes car rental companies (CSB, 2026b).

Pre-activity or enabling conditions

The case provides limited information on the establishment of the automotive business (LTD1_BB) or whether it was originally created with criminal intent. The judicial record only confirms that C1_BB operated a car-related business during the period in which the criminal activities occurred. It therefore remains unclear whether the business initially functioned as a legitimate enterprise before being used for criminal purposes. Nevertheless, the existence of a legitimate business environment provided C1_BB with a credible commercial setting in which the acquisition and possession of vehicles could appear legitimate.

Activity

The criminal use of the business primarily emerged during the financial investigation, when C1_BB attempted to legitimise assets linked to criminal activity. This involved presenting documents suggesting that the vehicles formed part of legitimate business transactions, including invoices and consignments agreements indicating that certain vehicles had been sold or temporarily held on behalf of other parties. Such **documentation** was submitted to the police to legitimise the legitimise the possession of these assets and create the appearance of normal commercial activity within the automotive sector. However, the court determined that these documents had been deliberately falsified and that the described vehicle transactions had not taken place. Instead, the documentation served to provide a plausible explanation for the possession of vehicles and other valuable goods considered as proceeds of crime. Through this mechanism, the automotive business environment was used to conceal the criminal origin of assets and integrate them into an appearance of legitimate trade.

Post-activity or post conditions

The drug-related offences were committed between December 2019 and March 2021, while the laundering of assets and falsification of business records occurred between 2021 and 2023. In November 2022, authorities seized approximately EUR 286,000 in cash, six luxury watches, several cars, and a motorcycle identified as criminal proceeds. These assets were determined by the court to originate from criminal activity. In October 2025, the court convicted C1_BB for several offences, including participation as a leader in a criminal organisation involved in the preparation of international cocaine trafficking, money laundering of large sums of cash and luxury goods, and falsification of documents relating to vehicles. According to the court, the suspect played a leading role in a criminal network that prepared the import, processing, and distribution of significant quantities of cocaine. The court imposed a 36-month prison sentence, partly reflecting procedural agreements between the prosecution and the defence.

4. Financial profile of the criminal network involved in Case Bravo-Bravo (BB)

Financing sources and start-up capital

The judicial record does not provide explicit information on the origin or size of the start-up capital used by the network, making it impossible to determine how the initial activities were financed. However, the court established that C1_BB was involved in preparing large-scale cocaine trafficking, an activity generally associated with substantial financial flows. Although the record does not specify whether such funds were available at the start of the observed period (2019-2021), it confirms that significant criminal proceeds were generated during the network's operation.

Payment methods and arrangements within the network

The judicial case file provides limited direct information on payment methods within the network. However, several elements offer partial insight. First, the substantial amount of cash (EUR 286,000) found in C1_BB's possession indicates that **cash** played an important role in storing or handling criminal proceeds. Second, the nature of the offences, particularly drug trafficking, suggests the use of informal and non-transparent payment methods, although the record does not specify transaction mechanisms such as cash exchanges, bank transfers, or alternative systems (e.g., underground banking). Third, the case demonstrates the use of assets as a store of value, serving to retain and potentially conceal criminal proceeds rather than functioning as direct payment instruments within the network.

Revenues and proceeds

The primary source of revenue in Case Bravo-Bravo (BB) was derived from drug-related criminal activities, specifically the preparation and facilitation of large-scale cocaine trafficking. The court indicated that these activities involved at least one hundred kilograms of cocaine, although no financial valuation was provided. In addition, the case establishes the presence of substantial criminal proceeds, including a Harley Davidson motorcycle, several cars, six luxury watches, including brands such as Rolex, Breitling, and Cartier, and cash. These assets were classified by the court as originating from criminal activity and therefore represented part of the network's criminal proceeds or accumulated profits.

5. Harms caused by Case Bravo-Bravo (BB)[118]

Harms to individuals

Criminal interference in automotive businesses may contribute to unsafe working environments for employees, including exposure to threats, intimidation, or violence. Moreover, customers may experience feelings of insecurity when visiting businesses associated with criminal activity. In more severe cases, the use of business premises for illicit activities, such as drug production, may create serious safety risks, including explosions or fires, thereby endangering both staff and visitors (Gemeente Utrecht, 2022).

Harms to other businesses

Automotive businesses appear to be disproportionately represented in incidents of and involvement in criminal activity on industrial estates (Gemeente Utrecht, 2022). The criminal use of automotive businesses for money laundering or fraud may result in unfair competition, as criminal actors can operate with illicit capital and thereby distort market prices.

Harms to the social environment

The presence of violence, including shootings or explosive incidents, may contribute to a climate of insecurity in industrial areas. Furthermore, the use of business premises for criminal purposes, including drug-related activities, can result in physical damage to properties, such as neglected or deteriorating buildings, as well as create risks of fire or explosion that may extend to surrounding premises (Gemeente Utrecht, 2022; Veiligheidsalliantie Rotterdam, n.d.).

[118] The harms identified in this section are not derived from interviews, as no interviews were conducted for Case Bravo-Bravo (BB). Moreover, the judicial file does not explicitly address harms resulting from the criminal activities or the criminal use of the automotive business. Consequently, the harms described in this section reflect generalised harms associated with the criminal use of businesses in the broader automotive sector.

ANNEX 10

METHODOLOGICAL ANNEXES

Annex 10.1 – Guide for the identification of five economic sub-sectors

As local key actors are required to identify and select five economic sub-sectors, the following prioritisation guidelines have been developed based on the 'Taxonomy of Bearers and Types of Harm' (Greenfield & Paoli, 2022).

The criminal use of the legitimate economy by criminal networks should be understood as a process rather than as a single offence. This process may involve a range of criminal activities, including violence associated with trafficking in human beings for labour or sexual exploitation, drug production and trafficking, fraud (e.g., social, tax, or domicile fraud), corruption, and money laundering.

These activities may cause **harm to different groups of victims** and to the wider environment. The questions below are intended to support local key actors in identifying economic sub-sectors in which such harms may occur to a greater extent than in other sub-sectors in their city. The questions are indicative rather than exhaustive and should be considered in light of the local context.

- **Individuals**
  - In which economic sub-sectors do workers experience poor or unsafe working or living conditions as a result of to criminal networks operating in or using these sub-sectors?
  - Are there deaths, non-fatal injuries, illnesses, or traumas associated with the use of specific economic sub-sectors by criminal networks? For example, physical or psychological harms caused by criminal cover-ups involving the production or sale of substandard or contaminated counterfeit products.
  - In which economic sub-sectors do workers experience material losses, such as loss of income or property, as a result of criminal networks using these sub-sectors?
  - In which economic sub-sectors have individuals experienced material loss or physical or psychological harm as a result of money laundering?
  - Are there economic sub-sectors in which minors are recruited as part of the criminal infiltration process more frequently than in other sub-sectors?
- **Businesses**
  - In which economic sub-sectors have businesses, knowingly or unknowingly, been exposed to or become victims of criminal use, for example through corruption, fraud, or money laundering?
  - Are there economic sub-sectors in which shell companies or criminal cover-ups are more prevalent?
  - In which economic sub-sectors have businesses experienced material losses or functional impairment, such as loss of sales, damage requiring repairs, or bankruptcy?
  - In which economic sub-sectors does the criminal use of legitimate businesses create unfair competition or otherwise disadvantage legitimate businesses?
- **Public institutions**
  - The criminal use of which economic sub-sector has the potential to undermine public trust in, or damage the reputation of, public institutions?

- **Physical environment** (including, among other things, wildlife, air quality, soil, and waterways)
  - Which economic sub-sectors used by criminal networks cause harm to elements of the physical environment? For example, water pollution caused by drug production in the real estate sector.
- **Social environment** (including, among other things, public nuisance, social fragmentation, perceptions of insecurity, and loss of trust in private and public institutions)
  - Which economic sub-sectors used by criminal networks contribute to harm to the social environment? For example, hairdressing salons used as criminal covers for drug dealing or other criminal activities, thereby contributing to violence or perceptions of insecurity.

Annex 10.2 – Overview of Belgian respondents

Table 21
Respondents interviewed as part of the Belgian (BE) data collection process

Respondent	Organisation / Department
R1_BE	Federal Judicial Police Antwerp – Financial and Economic Crime Section
R2_BE	Federal Judicial Police Ghent – Financial and Economic Crime Section
R3_BE	Belgian Financial Intelligence Unit (CTIF-CFI)
R4_BE	City of Antwerp
R5_BE	Federal Judicial Police Brussels – Financial and Economic Crime Section
R6_BE	Federal Judicial Police Antwerp – Financial and Economic Crime Section
R7_BE	Federal Judicial Police Antwerp – Financial and Economic Crime Section
R8_BE	Federal Judicial Police Brussels – Financial and Economic Crime Section

Annex 10.3 – Overview of Italian respondents

Table 22
Respondents interviewed as part of the Italian (IT) data collection process

Respondent	Organisation / Department	Information provided on case(s)
R1_IT	Public Prosecutor assigned to the cases under investigation	Case Golf and Case Hotel
R2_IT	Public Prosecutor assigned to the cases under investigation	Case India and Case Juliett
R3_IT	Investigative journalist; Expert of the criminal use of the legitimate economy	Case Golf, Case Hotel, and Case India


PREVENT