

Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures

December 2024





LEVERAGING LEGITIMACY: HOW THE EU'S MOST THREATENING CRIMINAL NETWORKS ABUSE LEGAL BUSINESS STRUCTURES

PDF | ISBN 978-92-95236-92-9 | DOI: 10.2813/7731594 | QL-01-24-014-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2024

© European Union Agency for Law Enforcement Cooperation, 2024

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

Cite this publication: Europol (2024), Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structure, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

CONTENTS

FOREWORD	3
KEY FINDINGS	4
INTRODUCTION	5
CRIMINAL INFILTRATION OF THE LEGAL ECONOMY	7
Defining legal business structures	7
Varying degrees of criminal exploitation and infiltration of LBS	8
All business sectors at risk	9
LEGAL BUSINESS STRUCTURES ENABLING THE CRIMINAL PROCESS	11
LBS as multifunctional tools for serious and organised crime	11
Crime-specific exploitation at every step of the criminal process	11
A BORDERLESS PHENOMENON	28
Global links between organised crime and legal businesses	28
CONCLUSION	31
ANNEX	32
LIST OF ABBREVIATIONS	33

FOREWORD

The infiltration of legal business structures by criminal networks poses profound risks to financial integrity, public safety and economic fairness. By blurring the lines between lawful and unlawful enterprises, these networks complicate efforts by authorities to detect and dismantle their operations, eroding public trust in the economy and the legal system. Leveraging legitimate business structures allows organised crime to grow in power and influence, creating a self-sustaining cycle that threatens the foundation of society.

Through legal businesses, criminal networks can channel illicit funds, or dirty money, into legitimate operations, disguising the origins of their assets and even gaining access to legitimate financing. Whether through money laundering or by securing legitimate funds, their criminal enterprises expand and flourish. The use of shell companies to evade taxes or distort economic competition undermines the integrity of economies and creates unfair advantages that weaken honest businesses.

Among these threats, however, the combination of the abuse of legal business structures and corruption stands out as one of the most severe. By exerting control over legitimate sectors, local communities and even political figures, criminal networks gain influence that extends well beyond the business world. In some cases, communities become economically dependent on these criminal-run businesses, leading to a lack of cooperation with law enforcement and further shielding of illicit operations.

As these enterprises expand, so does the power of the criminals who infiltrate or control them. With each new acquisition and each community dependency, these criminal networks tighten their grip. They weave into the fabric of legitimate business, making it harder for law enforcement to detect illegal activities.

This use of legal business structures creates a dual economy—one that appears lawful but serves as a cover for corruption, exploitation and criminal control. This web of businesses does not just evade detection; it undermines trust in the economy and erodes the integrity of legitimate commerce, creating a world where the line between legal and illegal becomes blurred.

The entrenchment of criminal networks within legal structures requires a coordinated but multi-disciplinary response from law enforcement, the private sector, public authorities and communities to protect the integrity of our economy and societies.

KEY FINDINGS

- ▶ **The infiltration of legal businesses by criminal networks is a key threat vector.**
 - **86 % of the EU's most threatening criminal networks** abuse legal business structures (LBS).
 - Criminals use legal business structures to **support, disguise and facilitate** a wide range of illicit activities and to **launder** their proceeds. By exploiting the legitimate frameworks of companies, trusts, partnerships and other entities, criminals try to evade detection, launder money and expand their operations with reduced risk.
 - LBS are susceptible to exploitation, offering opportunities for criminal networks **across numerous sectors and for a wide range of illicit purposes**. This allows criminals to conduct and conceal illegal activities at virtually every stage of their operations.
 - **Legal business structures are exploited by all types of serious and organised criminal networks**, knowingly or not. A range of criminal activities inherently rely on the abuse of LBS, while for other crime areas, they are an optional enabler.

- ▶ **The highest threat concerns high-level infiltration or criminal ownership of LBS**, as they are tailored to the requirements of the criminal activities and criminal actors exercise a high level of control over them.
 - Criminally owned LBS may mix licit and illicit activities, or they may be set up ad hoc purely as a front to facilitate crime.
 - The take-over of long-established LBS functions as a countermeasure and mirrors the resilience over time of some of the most threatening criminal networks in the EU.
 - Insider threats involve individuals who exploit their legitimate positions, often within businesses or public institutions, to assist criminal networks. These individuals—often employees, managers or even executives—use their access, knowledge and influence to facilitate criminal activities.

- ▶ The criminal exploitation of LBS is **a critical factor in the financial goals of organised crime**, which has a large stake in the cash-intensive sector – a sector which can provide opportunities and shielding for money laundering activities.

- ▶ **The abuse of LBS is a borderless phenomenon.** However, in most cases, LBS need to be close to operations in order to be effective. Therefore, most exploited and infiltrated LBS used/abused by the EU criminal networks are located either in the EU itself (all EU Member States are affected) or in the countries neighbouring the EU.

- ▶ Criminally operated LBS may serve the needs of **multiple criminal networks** and facilitate multiple criminal purposes in parallel.

INTRODUCTION

Background

In April 2024, Europol issued a Europe-wide analysis on the inner workings of the criminal networks that pose the highest threat to the EU's security¹. The report was initiated as one of the goals within EMPACT to further strengthen the intelligence picture of the most threatening criminal networks, in line with the EU roadmap to fight drug trafficking and organised crime², and as a complement to the EU Serious and Organised Crime Threat Assessment (EU SOCTA).

The report described in detail how the most threatening criminal networks are organised, which criminal activities they engage in, and how and where they operate. The report also assessed the specific characteristics of criminal networks which increase the threat to the EU's internal security.

One of the findings of this milestone report was that the most threatening criminal networks exhibit remarkable agility. A key contributing factor to this agility is their ability to inventively make use of opportunities in the legal economy, where the abuse of legal businesses is a key characteristic. The report found that nearly all of the most threatening criminal networks affecting the EU make use of legal businesses to further their criminal objectives.

Such an encompassing finding requires further exploration in order to better understand how, why and where this abuse of legal businesses takes place, and to gain better insight into how it enables various areas of crime and what stages of the criminal process are impacted. These are the questions that this analysis aims to clarify.

This need was expressed by the Council of the European Union in its Conclusions of 13 June 2024 on mapping the most threatening criminal networks. The EU JHA Council tasked Europol with preparing a dedicated assessment on the use of legal business structures by the most threatening criminal networks.³

In parallel, Europol, as the Coordinator for the EMPACT Common Horizontal Goal 1 on enhancing the tactical and strategic intelligence picture, is leading an Operational Action implemented under each EU Priority and its 15 Operational Action Plans 2024-2025. The aim of this initiative is to find a true horizontal approach towards better understanding organised crime via this key enabling factor, including a better tailoring of such an approach via preventative or administrative pathways.⁴ The horizontal Operational Action resulted in the extensive engagement of Member States and third partners, providing dedicated input detailing the abuse of legal businesses under all EU crime priorities.

The analytical findings of this report will inform future Operational Actions, will feed into the EU SOCTA 2025 and may inform initiatives with regard to prevention or the administrative approach.

¹ Europol, 2024, Decoding the EU's most threatening criminal networks, available at <https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks>.

² European Commission, Communication from the Commission to the European Parliament and the Council on the EU roadmap to fight drug trafficking and organised crime (18 October 2023), 641/23.

³ Council of the European Union, Council conclusions on mapping the most threatening criminal networks (13 June 2024), 11153/24.

⁴ Council of the European Union, EMPACT Terms of Reference (17 May 2023), 8975/23.

Scope

This report deepens the analysis based on the dataset of the 821 most threatening criminal networks identified in the context of the report 'Decoding the EU's most threatening criminal networks'. It focuses on:

- Which types of legal businesses are prone to criminal abuse or infiltration?
- Which organised crime activities are enabled by legal businesses?
- How does the legal business enable the criminal activity?
- Where are legal businesses mainly abused?

Sources

The main starting point of this analysis is the dataset on the 821 most threatening criminal networks. In order to supplement the data available on the abuse of legal business structures, this report also utilises a broader dataset stemming from operational information from investigations shared with Europol, recent analytical reports, in particular from participants in the EMPACT Operational Action on this topic who provided a rich overview of case studies tailored to flow into this analysis.

CRIMINAL INFILTRATION OF THE LEGAL ECONOMY

Defining legal business structures

The threat posed by serious and organised crime is influenced by characteristics of the criminal market or the criminal actors. However, it is also revealing in this context to consider available crime infrastructure – or enablers of crime. These enablers can either be criminal acts in themselves (e.g. corruption or document fraud), or can be part of the legal system but exploited for criminal motives (e.g. abuse of legal business structures or abuse of digital and technological infrastructure).⁵

Legal business structures used in the context of this analysis (and other Europol analyses), refer to a broad range of legitimate business forms that may be abused to function as an enabler for serious and organised crime. They are organisational frameworks determining how a business entity operates in a given jurisdiction. Such a framework is essential in determining the business owner's liability, as well as tax obligations.

Most types of legal structures exist in all EU Member States under different names, sometimes with slightly different regulations. Generally, they can be categorised⁶ to include limited liability companies⁷, unlimited liability companies⁸, sole traders⁹, partnerships¹⁰, trusts¹¹, associations¹², and state-owned enterprises.

Depending on the jurisdiction, legal entities can combine elements of different types of legal structures (e.g. entities with elements that are typically those of a sole trader, but with a limited degree of liability). Different risk indicators can be associated with the criminal abuse of the different legal structures.

⁵ Council of the European Union, 21 November 2023, European Union Serious and Organised Crime Threat Assessment (EU SOCTA 2025) – Revised methodology, 14642/2/23 Rev2.

⁶ Ibid.

⁷ Most common legal forms for small and medium-sized enterprises (SMEs), where the shareholders are not personally liable for the debts of the company, as they are separate from the legal entity itself. Limited liability companies can be either private limited companies or public limited companies. The latter are generally publicly traded on a stock exchange and are required to have a minimum share capital.

⁸ While being similar to a private limited company, the liability of the owners is not limited to the value of the shareholding, meaning that the owners are personally liable for the debts and obligations of the company.

⁹ A business owned and operated by a single individual who is personally liable for its debts and obligations.

¹⁰ An arrangement between two or more individuals to oversee business operations and share profits and liabilities. There are partnerships where at least one party has unlimited liability for the partnership's debt (limited partnerships), and others where all parties have unlimited liability (general partnerships).

¹¹ A legal entity where a party known as a trustor gives another party, the trustee, the right to hold title to and manage property or assets for the benefit of a third party, the beneficiary.

¹² A legal form typically used by non-profit organisations, charities and foundations.

Varying degrees of criminal exploitation and infiltration of LBS

Legal business structures can be exploited to facilitate criminal activity in various ways and to varying degrees.

An existing LBS can be used by a criminal network unknowingly, without the LBS being aware of it. In this case, the criminal network does not exert any control over the LBS, but merely uses its name, infrastructure or services. In a further step, a criminal network can infiltrate the LBS at a low level, or collude with or coerce its employees. Lastly, a criminal network can infiltrate the LBS at a high level, coercing key individuals within the structure, or even set up its own LBS that it fully controls.

Of the 86 % most threatening criminal networks that make use of LBS¹³, the largest part (63 %) does this in a way that represents the highest threat level: by setting up its own LBS, infiltrating an existing LBS at a high level or colluding with or coercing key individuals within a LBS to gain access to or control over it. 16 % of criminal networks infiltrate the LBS at a low level or are able to collude with employees. A further 7 % make use of legal business structures without their knowledge.

CASE EXAMPLE – A NETWORK OF LEGAL BUSINESS STRUCTURES SET UP TO FACILITATE INTERNATIONAL COCAINE TRAFFICKING

Over a period of 10 years, a criminal network has built a complex network of companies, mainly related to the international trade of fruits, in different European countries to traffic cocaine from South America to Europe. The network of companies continues to be expanded with new companies. Core members coordinate the activities of low-level members, who set up international trade companies in the EU. Other members are responsible for infiltrating the logistics companies and customs services providing the necessary information to organise the transit. A broker plays a critical role in the traffic as the connection between the European companies and South American export companies, and as organiser of the transports.

The abuse of legal business structures can be an inherent part of the crime area in which criminal networks are active, such as in the case of fraud against the national financial interests of EU Member States, the abuse of public funding, value added tax (VAT) fraud and missing trader intra-community (MTIC) fraud. For other crime areas, even though LBS are not an intrinsic part of the modus operandi, they may be important facilitators of criminal activities. For example, front or shell companies may be used to facilitate the movement of illicit or stolen goods or to enable money laundering activities. Companies are set up to provide official work for members of the criminal networks. Shell companies are set up to conceal and facilitate a wide range of criminal activities, from investment fraud and match-fixing to recruitment of victims for trafficking in human beings (THB), and beyond.

Infiltration and abuse of LBS can be systematic and long-term, or temporary. When the abuse is systematic, it becomes a functional part of the process, without which the criminal activity cannot be carried out. Examples of systematic abuse are those steps of the criminal process that occur within the legitimate economy (i.e. obtaining commodities/services/support from public resources, transport via postal services, online distribution via legitimate websites and on marketplaces, marketing via social media, and retailing in legitimate stores). Systematic abuse usually occurs in those LBS abused to launder criminal proceeds. The services sector (retail, hospitality) and the

¹³ Europol, 2024, Decoding the EU's most threatening criminal networks, available at <https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks>.

financial sector also tend to be systematically abused. Occasional infiltration provides criminals with a certain degree of flexibility and the possibility to quickly change partners, infrastructure, routes, service providers, etc.

Criminal networks set up new companies or infiltrate existing business structures to take advantage of the façade of legitimacy, as existing companies with an established and healthy financial and tax record often attract less attention from tax authorities and law enforcement. They can also take over companies on the brink of bankruptcy, that can then be used as a front for their criminal activities. For example, during and after the COVID pandemic, several criminal networks supported businesses in need by lending them money during the crisis (loan sharking). In this way, they target distressed companies with a view to later acquiring control over them and using them as a cover for their illegal ventures. Criminal networks also abuse the names of bona fide existing companies to facilitate their criminal activities, while those abused remain unaware of it. They sometimes also set up companies with similar names to existing companies.

LBS may be registered in the name of the leaders, core members, or frequently low-ranking members of a criminal network. Strawmen without criminal records, often relatives or friends of network members, are also used to register the LBS or the accounts linked to the real or bogus legal business entity. Financial and legal consultants are essential for the functioning of the criminal business, especially since networks usually operate through legal business structures across multiple jurisdictions.

All business sectors are at risk

All business sectors are potentially at risk for criminal exploitation, each of them presenting different types of risks for abuse for criminal purposes. For the purpose of this report, we have clustered businesses in the following sectors: financial, cash-intensive, real estate/construction, manufacturing, trade, logistics, and technology and communication.¹⁴

The data on the 821 most threatening criminal networks show clearly that LBS are infiltrated or abused by criminal networks across almost all sectors.

Three sectors are particularly affected by criminal infiltration or abuse: logistics (i.e. transport and import/export companies), cash-intensive businesses (in particular hospitality) and construction. The companies are used in all crime areas with the exception of cyber-attacks.¹⁵

LBS in the logistics sector (transport and import/export) are mainly used in drug and waste trafficking, but also in almost all other crime areas – counterfeiting of goods, migrant smuggling, organised property crime (for example, stolen vehicles) and weapons trafficking. Besides the common facilitation of illicit goods overseas and the transport throughout the EU by haulage companies, this can also include the abuse of taxi companies to move money or people, for example.

LBS in cash-intensive businesses, particularly the hospitality sector, are often exploited for the purposes of drug trafficking, extortion and racketeering, migrant smuggling, organised property crime and weapons trafficking. Establishments operated in this sector are convenient as meeting places for criminal partners, as selling points for drugs or as a front for money laundering schemes.

¹⁴ For further descriptions of each of these sectors, please see the Annex.

¹⁵ Europol, 2024, Decoding the EU's most threatening criminal networks, available at <https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks>.

In the construction sector, LBS are used to facilitate criminal activities and money laundering in almost all crime areas: drug trafficking, extortion and racketeering, fraud against the public interest of the EU or Member States and online fraud, migrant smuggling, organised property crime, waste trafficking and weapons trafficking. Construction companies can be used to invest laundered criminal proceeds or can be set up as a cover for renting warehouses to conduct illicit activities.

The sectors and types of LBS that a criminal network may infiltrate, and the motivations behind these choices, can vary considerably. Examples include infiltration of the construction, catering and real estate sector for money laundering, the retail sector for VAT fraud, and the car industry for vehicle trafficking. The next chapter provides details per crime area on how the abuse of LBS facilitates (part of) the criminal process.

LEGAL BUSINESS STRUCTURES ENABLING THE CRIMINAL PROCESS

LBS as multifunctional tools for serious and organised crime

Legal business structures are a key instrument in the toolbox of criminal networks, as they are useful in multiple ways. They may help commit the crime, obscure the crime, and/or launder the proceeds of crime.

They are essential for some crime areas and optional for others. Certain criminal activities cannot be carried out without the abuse of legal business structures. Economic and financial crimes especially, and all those criminal businesses that are carried out via commercial operations that occur in the legal economy, are the crime areas where LBS are of course mostly abused. All types of fraud schemes targeting individuals, private companies and public institutions, but also intellectual property crimes and environmental crimes, are perpetrated behind the façade of legitimate businesses. In other crime areas, LBS facilitate or conceal the criminal activities or identities of criminal actors.

Crime-specific exploitation at every step of the criminal process

The criminal process refers to the sequential stages in which a criminal activity is committed. While the stages in the criminal process differ per crime area, overall, the following ones are of relevance to gain insight into how criminal markets function and at what stages they are enabled by LBS:

- Planning
- Recruitment/Production
- Transportation/Storage
- Marketing/Distribution/Exploitation
- Money laundering

Some LBS are abused throughout the criminal process, others only in one or a few stages. The most relevant LBS and the stage(s) in which they are abused differ between the crime areas. The chapter below outlines per crime area which LBS facilitate the committing of the criminal activity, in which step(s) of the criminal process, and how.

Fraud

VAT and MTIC fraud

The whole essence of tax fraud relies on the abuse of commercial entities and the abuse of tax mechanisms. Carousel or MTIC fraud involves the sale of goods or services from one trader to another, going round as in a carousel. In cases of fraud, the first company in the chain charges VAT to a customer but does not pay this to the government, becoming what is known as a 'missing trader'. Several billion euros are lost annually to carousel fraud schemes taking place in the EU, causing significant tax revenue losses.¹⁶

Criminals create complex networks of companies to conceal the actual connections between the scheme participants. In one case of carousel fraud, 76 companies were set up to carry out a criminal business (through a network of missing traders and buffers) that provided more than EUR 9 million in illicit proceeds and VAT refunds of almost EUR 5 million.

CASE EXAMPLE – CREATION OF LEGAL BUSINESS STRUCTURES FOR VAT FRAUD AND MONEY LAUNDERING

In February 2021, law enforcement tackled a criminal network involved in value-added tax fraud and large-scale legalisation of criminally obtained funds. With the assistance of a legal company official, the criminals established 10 different bogus companies indicated as trading glass packaging in the VAT register. With the assistance of the accomplice, fictitious transactions were generated to create the illusion of legitimate economic activity, which included transferring criminal funds to the buffer companies' bank accounts and engaging with state institutions. The total sum of the transactions, excluding VAT, exceeded EUR 1 million, potentially causing damage to the state budget of no less than EUR 300 000 between June 2019 and February 2021.

Criminal networks set up companies and make them disappear at the right moment. Business entities with few or no employees and with no physical business premises are also used. Individuals in economic difficulty are often recruited to act as a front. In some cases, fraudsters take control of a legitimate business's VAT number and issue false invoices in its name. Companies on the brink of bankruptcy also appear in fraudulent schemes, declaring themselves bankrupt when tax authorities seek to retrieve VAT. In one case, the company was intended to be abused for about just over a year before going bankrupt. The frequency of the abuse would be expanded and maximised at the end of the company's 'lifetime'. In another case, more often than not the fictitious owners/employees of the front company would rotate after three to six months. It is not uncommon for a company to be used by several criminal networks, especially as a missing trader, if such use is already known in the criminal environment.

LBS dealing with electronic products, particularly mobile phones and components, are among the most widely reported LBS abused for MTIC fraud. IT goods and accessories also appear in carousel fraud. Food products and beverages (including alcohol and spirits), are another common commodity, also due to the difficulties in following the flow of goods. High-demand food products and fast-moving consumer goods (FMCGs), such as soft drinks and confectionery, as well as second-hand cars, including luxury second-hand cars, are often targeted. Precious metals, including gold, are an emerging commodity in VAT fraud schemes through misdeclaration. Carousel fraud schemes

¹⁶ Europol, 2023, The other side of the coin. An analysis of financial and economic crime in the EU. European analysis of Financial and Economic Crime in the EU (EFACTA), available at <https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime>.

with intangible goods, such as VoIP primarily, but also advertising, marketing services, construction services, and counselling, continue to be reported in the EU. Intangible goods remain a threat in MTIC fraud and authorities increasingly face difficulties with trade in intangible goods, classified as ‘services’ for VAT purposes.

CASE EXAMPLE – CRIMINAL NETWORK USES LBS FRONT FOR MTIC FRAUD

A criminal network established a legal business to commit MTIC fraud by selling electronics through an e-commerce platform in October 2022. Financial experts, including accountants, helped register the business as a limited liability company, with share capital provided by the criminal group. The leader controls the business and its bank accounts. Key members hold Swedish citizenship and have a strong understanding of the country’s economic and legal system, while ‘strawmen’ with resident permits and stolen identities are used to obscure the criminal operations, making it harder for authorities to trace them. The business, primarily trading electronics, is intended to be exploited for about a year, with activity culminating right before liquidation. The mastermind behind the criminal scheme monitors and controls activities from a distance and has a wide international network, owning several other companies in the EU and third countries involved in trading goods and money transactions.

Business entities perform several roles in the fraudulent schemes¹⁷:

- **Missing trader:** a VAT-registered trader who acquires goods or services without paying VAT, then supplies them with VAT, which he keeps rather than paying it to the tax authority.
- **Defaulter or default trader:** submits statements but fails to pay the VAT.
- **Buffer:** buffer companies are used to distance the broker from the missing trader. They usually buy goods or services from the missing trader and sell them to the broker with a small profit margin, on which they pay VAT.
- **Broker:** the broker claims and receives reimbursement for VAT payments that never occurred.
- **Conduit company:** at the start of a fraud scheme, the conduit sells goods or services across a border VAT-free to a missing trader in another Member State. At the end, the conduit acquires the goods or services back from the broker across the border; the transfer is VAT-free and the broker can claim the VAT that has been charged, but never paid by the missing trader.
- **Remote missing trader:** like a conduit company, a remote missing trader does not submit VAT statements. It is a company incorporated in a Member State other than the declared destination of the goods, used to mask the real destination.
- **Cross-invoicer:** buys commodities from another Member State with zero-rate VAT and sells them to a buffer company applying the domestic rate of VAT. To offset the output VAT, the cross-invoicer then declares acquisition from a national missing trader of goods or services that he subsequently delivers or exports to third countries.
- **Invoice mills:** companies that are set up solely to generate invoices that allow recovery of VAT, exploiting the practical impossibility of crosschecking every invoice against evidence that earlier tax has been paid.

¹⁷ Europol, 2023, The other side of the coin. An analysis of financial and economic crime in the EU. European analysis of Financial and Economic Crime in the EU (EFACTA), available at <https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime>.

Excise fraud

Criminal networks engaging in excise fraud create or abuse LBS throughout the criminal process. They create companies to enable the importation of precursors and equipment for the **production** of the excise goods; they create shell companies to be declared as consignees; they infiltrate or create **transport** and shipping companies to smuggle the goods to the final destination; and they sometimes register companies to facilitate the **handling of criminal profits**. In some cases, legal tobacco producing factories are involved in the illicit trade, deliberately overproducing tobacco products and diverting these to be sold on the black market.

Subsidy fraud

In the case of subsidy fraud, criminals operate through legitimate companies, often created ad hoc just to perpetrate the criminal activity and not carrying out any real economic activity. In one case, in order not to raise suspicion, criminals were taking over only businesses with some pre-existing operating activities (not setting up new ones) – regardless of the sector. In another case, the criminal network even created a fictitious bank in a jurisdiction on the other side of the world, to simulate the existence of a strong financial institution with a long-established history, so that it could mislead various European companies benefiting from contracts financed by European funds. The companies participate in public procurement competitions. Some agree with associated suppliers to submit specific tenders and agree on bidding prices. Others apply for public funds and compensation schemes on false grounds (this happened often in the aftermath of COVID-19).

CASE EXAMPLE – SUBSIDY FRAUD LINKED TO COVID-19 COMPENSATION SCHEME

Several criminal networks committed systematic fraud of the National Business Compensation Scheme during the COVID-19 pandemic, initially aimed at companies suffering financial losses related to the pandemic. The application system was based on self-reporting without any control mechanisms, making it vulnerable to criminal abuse. To appear eligible, the criminal networks registered a large number of fictitious employees in pre-existing companies they already controlled or owned. The companies used were established within cash-intensive industries such as construction, cleaning services, car workshops, and transport. The same legal business structures were used by criminal networks in various crime areas, including drug-related crimes, money laundering, and tax fraud. The criminal scheme was exploited by numerous criminal actors which cooperated and assisted each other in finding potential companies eligible for the compensation scheme.

Various types of companies are used for subsidy fraud, such as construction, packaging, transport, security companies, real estate, orthopaedic aids, and cleaning services. With the EU focusing on a more sustainable, digital and resilient economy, subsidy fraudsters are set to increasingly target sectors such as renewable energy, research programmes and the agricultural sectors - some of the 'pillars' of the EU Next Generation Fund (NGEU).

CASE EXAMPLE – CRIMINAL ABUSE OF SUBSIDIES FOR MEDICAL AIDS

A criminal network established front companies selling orthopaedic aids to commit subsidy fraud. The perpetrators discovered a legal loophole in the system, as the orders for medical aids were not controlled, while the state offered a 90 % refund to the distribution companies. The criminals – acting as managing directors of these companies – bribed two doctors and their three assistants to provide them with fictitious prescriptions for orthopaedic aids. To do so, the medical personnel used the medical data of unsuspecting patients. The criminals then submitted refund claims to the National Insurance Fund, without actually manufacturing these medical aids. The operation generated a turnover of several million euros. The perpetrators invested their illicit proceeds in real estate, investment services, vehicles and gold bars and caused more than EUR 700 000 in damages to the state.

Food fraud¹⁸

Fraud involving food presents significant hazards for public health, but is attractive for criminal actors due to the potentially high profit margins. Food or drinks in a poor state of conservation or expired/spoiled are relabelled and reintroduced into the supply chain. In some cases, waste disposal centres are complicit in this criminal business, **selling** the food to the criminal actors rather than proceeding with its destruction (for which they had already received payment). Other types of food fraud involve the illegal use of protected designation of origin and protected geographical indications, or the fraudulent attribution of the organic category for standard products, misleading the consumer.

CASE EXAMPLE – SOPHISTICATED FOOD FRAUD

A criminal network imported and sold saffron altered with gardenia, a toxic substance unauthorised as food in the EU. The substance closely resembled saffron at a molecular level, evading detection. The network created a legal business structure for these activities, with specific functions for each entity. This included ad hoc production by a Chinese legal business structure located in China, personnel dedicated to facilitating the entry of the illicit product into the EU, technicians specialised in counteracting detection techniques and a sales department. The criminal network had been conducting these criminal operations since at least 2013 until 2022 in a systematic manner.

Mortgage fraud

Criminal networks are increasingly using mortgage fraud as a financial tool to generate profits, launder money and exploit vulnerabilities in the real estate and lending sectors. This type of fraud often involves complex schemes that can manipulate home prices, by falsifying borrower information. Criminal networks provide falsified information, including fake employment records or inflated income statements from one of their businesses to secure loans.

¹⁸ Europol, 2023, The other side of the coin. An analysis of financial and economic crime in the EU. European analysis of Financial and Economic Crime in the EU (EFACTA), available at <https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime>.

Online fraud schemes¹⁹

Criminal networks involved in online fraud schemes make extensive use of legal business structures. The types of business entities vary according to the fraud typology and the level of complexity of the money laundering schemes.

Criminal networks either make fraudulent use of legitimate businesses (especially of online services, trading platforms, IT service providers) or deliberately set up companies to carry out their illicit operations. Bogus companies such as investment and trading companies, call centres, delivery and shipping services, logistical and IT service providers, are quickly established and dissolved. To conceal their real identities, criminals have several frontmen on the payroll, often vulnerable individuals targeted because of their poor economic condition. Fraudsters active in cryptocurrency investment fraud also set up training companies to better hook victims and sound more professional.

For fraud schemes using social engineering and phone communication (especially investment, tech-support scams, e-commerce fraud, and refund and recovery fraud) criminal networks frequently establish **call centres**, which are run in rented apartments, warehouses or office spaces. Some call centres appear so legitimate that employees think that they are working for legitimate investment firms, and do not realise that the invested money is being stolen. In other cases, call centre operators are aware of the unlawful tasks, however sometimes they do not acknowledge the whole criminal business process (in one case, the employees of the call centres were encouraged not to invest themselves nor to propose investments to their relatives and friends). Young staff with little work experience are likely to be employed. In several investment fraud cases, the same call centres marketed different investment products simultaneously, using numerous fraudulent websites to **lure victims**. Criminal networks making use of call centres have proven to be resilient and capable of relocating them quickly, keeping the same managers and accountants.

In business e-mail compromise (BEC) fraud, the role of the intrusion into the business activities of a legitimate company, the hacking of their communication services and the exfiltration of critical information that can be used to impersonate management or business partners is essential.

E-merchants and bank institutions are the preferred victims of digital skimming attacks.²⁰ Some criminals are behind several linked cases of bank phishing, with affiliates managing various fake web shops in parallel, redirecting victims to fake banking and payment web pages.

CASE EXAMPLE – CROSS-BORDER ONLINE FRAUD LEVERAGING VARIOUS LEGAL BUSINESS STRUCTURES

¹⁹ Europol, 2023, The other side of the coin. An analysis of financial and economic crime in the EU. European analysis of Financial and Economic Crime in the EU (EFACTA), available at <https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime>.

²⁰ Europol, 2024, IOCTA 2024, available at <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>.

A criminal network obtained the personal data of victims from a company's website and mass-sent them text messages via a legitimate US marketing service. Victims were tricked into clicking on a link in the text which rerouted them to a false website that looked like the victim's banking website. This website was hosted by legitimate web services in Malaysia, Indonesia and the UK. The victims unknowingly provided their banking details, granting the criminals access to their bank accounts. The stolen funds were funnelled through numerous accounts, including neo-banks, before reaching the final account. Each account was used for a different purpose, such as personal spending or payments to the criminal enterprise.

Cybercrime

Criminals abuse online platforms, search engines, hosting services and intermediary services offering network infrastructure, to spread illegal content and illegal goods and services.²¹

Cyber-attacks

Criminals have to abuse legitimate businesses to carry out cyber-attacks, as this allows them to leverage brands, digital infrastructure and other digital tools. They hack the IT infrastructure of companies (i.e. servers, website, cloud services) to take control of them and distribute malware or launch DDoS attacks, but they also intrude on the communication systems between business partners.²²

Child sexual exploitation

In both online child sexual exploitation (CSE) and child trafficking cases, social media provides perpetrators with an easily accessible arena to **search for potential victims**. Offenders abuse mainstream platforms to engage with their victims. In these environments, they interact with minors often behind a false identity, pretending to be a peer. In some cases, they do not conceal their real identity. The hacking of social media accounts with the aim of uploading and circulating child sexual abuse material (CSAM) is increasingly being reported. Recent law enforcement investigations have highlighted the growing dependence by CSE offenders on end-to-end encrypted communication platforms for the exchange of CSAM as well as for communication among offenders. Offenders seem to prevalently use communication applications that are popular in specific regions.

Social media platforms have been an important environment for CSE offenders to perpetrate their crimes. The fact that more tech companies are adopting the use of end-to-end encryption (E2EE) in their communication channels is a great concern for those investigating CSE. When communication is encrypted, providers are not able to access it anymore and therefore to detect and refer CSAM.

Criminal activities online are often concealed with the support of enablers such as virtual private networks (VPNs), residential proxies and bullet-proof hosting (BPH), making efforts in tracing and identification more difficult. Scripts to automatically

²¹ Europol, 2024, IOCTA 2024, available at <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>.

²² Ibid.

change EXIF²³ data, resize images and thus change hashes are widely used by offenders.

Law enforcement investigations have unveiled the abuse of professional photographic studios dedicated to child modelling for the **production** of CSAM. These photographers either have their own production of CSAM sets for **sale** or act as facilitators between customers and victims. The locations of the photo shootings are usually professional studios but also privately rented apartments.

Environmental crime²⁴

Criminals infiltrate legal businesses and organisations aimed at protecting the environment. Legal business activities, be it industrial production, waste management, trade in fauna and flora, or production and sale of fuel, function as the main facilitator for environmental crimes and, at the same time, as the perfect façade to conceal illicit activities. The majority of environmental crime actors are opportunistic legal business owners/operators who decide to increase their chances of profit by establishing a criminal venture.

Waste must be collected, treated and transported before its disposal or recycling according to binding legal regulations. This waste management involves various legal business structures that can be abused throughout the process. As a **countermeasure**, companies used in waste crime schemes frequently change management and are terminated after a short period of activity, while a new trading entity, created by the same group of suspects, takes over the business. Networks also use trading companies not directly involved in the waste management business, which just buy and sell (accompanied by forged documentation) waste electrical and electronic equipment (WEEE) to brokers located outside of the EU, who then organise the resale of the waste by local businesses operating on the black market. But criminal networks involved in waste trafficking also contract specialised waste transport companies, using fraudulent documents.

In wildlife crime, criminals use legal business structures such as pet stores, antique shops, jewellers, local restaurants, meat shops, international fairs, gardening stores, breeding companies, and even zoos to **facilitate the trade** of protected and non-protected species, both in source and destination countries, as well as for the **laundering of illicit proceeds**.

Illegal trade in wildlife is a cash-intensive criminal business. Illegally traded birds are sold online, in pet shops as well as at national and international fairs, which confirms once again the systematic links between legal business structures and illegal bird trafficking. Some networks also sell dead specimens as food in restaurants or to food processing factories.

²³ EXIF stands for Exchangeable Image File Format and includes all the background information related to the image, such as location and time, device used and other specifics.

²⁴ Europol, 2022, Environmental crime in the age of climate change, available at <https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment>.

CASE EXAMPLE – ILLEGAL INTERNATIONAL PET TRAFFICKING

The EU prohibits transporting puppies under 15 weeks old within its borders due to rabies concerns. However, demand for puppies younger than 12 weeks remains high in countries like Italy, Spain, France, and Germany, creating opportunities for criminal activity. Breeders in Eastern Europe falsify documents to make puppies appear older and fit for transport. Distributors, often running small legal businesses comprised of family members who are experts in animal trading, obtain forged rabies vaccination records and age documents through bribed veterinarians. The puppies are then sold to pet shops in Western Europe, bypassing legal transportation restrictions with fake licences and false paperwork. Transport is mainly carried out by the distributors themselves, but they sometimes sell the puppies to subcontractors located in countries less suspicious for illegal pet trade, which then transport the dogs to pet shops in Western Europe.

Considering the increasing efforts of the EU towards a more sustainable economy, various types of fraud are set to flourish in the green economy business. In the fraudulent trade of carbon offsets, also known as Verified Emission Reductions (VERs), a variety of business entities may be infiltrated. Criminal networks allegedly set up environmental projects in the name of registered companies with the façade of counterbalancing carbon emissions and consequently, generating VERs. The VERs, which are then marketed either through legal traders or sold directly to LBS, can further resell the carbon offsets to other companies or claim a lower net emission and formally offset them. The trade of fraudulent carbon offsets among companies also presents opportunities for money laundering.

Intellectual property crime

Legitimate businesses, including factories, may be set up to hide illicit **production**. In the specific context of pharma crime, the infiltration and abuse of pharmaceutical companies and pharmacies is critical, especially when the modus operandi involves the diversion or theft of legitimate goods. In the case of diversion, legally manufactured goods are rerouted from their legitimate distribution channels to illicit markets using false statements and declarations.²⁵

Commercial warehouses, transport companies, and shipping services, for example, may be relevant in the **transport** phase.

In the **distribution** phase, any physical store or retail outlet may be involved, as well as online web stores, marketplaces, social media, and E2EE applications.

²⁵ Europol, 2024, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact, available at <https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime>.

CASE EXAMPLE – COUNTERFEITING CRIMINAL NETWORK OWNS COURIER COMPANIES²⁶

In June 2022, law enforcement conducted investigations into a criminal network involved in trading counterfeit luxury goods through a website and 13 social media profiles. The group had been operating since February 2020, during which time it had managed to distribute over 364 000 parcels to customers and obtain more than EUR 18 million in illicit profits, laundered via other business companies owned by the network. The group also owned two courier companies that would exchange goods and money multiple times to avoid detection and conceal their criminal activities.

Drug trafficking

Legal business structures play a key role in various stages of the production and trafficking of drugs, including the acquisition stage, the disposal of waste, transportation and distribution stages.

Criminals involved in the cultivation of cannabis, the production of synthetic drugs or the extraction of cocaine may resort to real estate agencies to find a location fit for these activities. Farmers have also been approached for the use of their barns for drug production. In most cases, they are fully aware of the criminal purposes.

Some of the tools and chemicals needed for the drug production can be bought freely and legally, others not. Various types of LBS may be abused to facilitate the **acquisition** thereof. Setting up a legitimate pharmaceutical or chemical company is particularly useful for this purpose, as it provides a credible façade for diverting the necessary goods from legal supply. Instead of creating a company, criminals can defraud existing companies, using their data to procure what they need. In some cases, logistics companies act, unknowingly, as intermediaries between companies selling and criminals buying chemicals.

CASE EXAMPLE – LBS SET UP TO SOURCE PRODUCTS NEEDED FOR SYNTHETIC DRUG PRODUCTION

One of the leaders of a criminal network involved in the production of synthetic drugs has set up a company abroad to source necessary chemicals and equipment. Via this company, orders are placed with various other companies which trade in the required products. As such, the goods are bought legally and then diverted to be used for drug production. Vans rented from different companies are used to transport the chemicals and equipment to the production locations.

Car rental or car trading companies are sometimes abused by drug producing networks to **transport** chemicals or to dispose of the waste that is generated.

Drug trafficking networks make ample use of LBS to transport drugs from source to destination. To avoid detection, drugs are concealed in many different ways.

²⁶ Europol; 2024, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact, available at <https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime>.

Import/export companies – including repackaging and forwarding companies – and transport companies play an important role in this phase of the criminal process.

Investigations indicate that existing companies in these sectors are often unknowingly abused. Management is not aware, but employees may be involved in the criminal activities. Criminals prefer companies with years of experience and a good reputation, as these raise less suspicion and can be used systematically over extended periods. Drug trafficking networks can also set up their own international companies in these sectors, mixing legal and illegal activities.

CASE EXAMPLE – LBS SET UP TO TRANSPORT COCAINE

A criminal network engaged in the import of cocaine, concealed in loads with bananas, via the port of Antwerp, has created its own transport company to route the drugs to the country of destination. The network has contacts inside the port to keep control of relevant containers. The containers are transported to a company, owned by the network, that serves as consignee of the imported bananas.

Large quantities of drugs are transported by sea in containers. Criminal networks need access to these containers to hide and retrieve the drugs. Companies operating in ports, handling these containers, are vulnerable to criminal infiltration or abuse. The misappropriation of container reference codes, by infiltrating shipping companies to obtain this code, is just one example. This practice makes it possible to release the container from the port terminal, pretending to be the legitimate client.²⁷ Also, companies that maintain and repair containers play a key role in hiding and retrieving drugs, in particular when the drugs are hidden in the structure of the container. Owners and employees of said companies are aware of the criminal activities and are, therefore, complicit.

Online marketplace stores are deliberately set up for trading drugs. Parcel and express courier companies are used for the **distribution** of the drugs. In most cases, this happens unwittingly, although employees may be complicit.

CASE EXAMPLE – CHINESE CRIMINAL NETWORK INFILTRATES COMPANIES AND ABUSES PARCEL SERVICES FOR DRUG TRAFFICKING

A Chinese criminal network, whose members operate in various countries, is involved in supplying new psychoactive substances (NPS) from the EU via a global parcel service to New Zealand, Hong Kong, Canada, and the United States. The dispatch preparation and processing of the drugs are carried out by two companies partly influenced by members of the criminal group. The first company, involved in import/export, is unknowingly abused. The second company, active in repackaging and forwarding, uses the name of the first company to profit from favourable conditions. The latter was founded by a member of the criminal network and used for the drug trafficking. The drugs are concealed in shipments of acrylic tubes, mahjong stones, and cardboard packaging. The illicit profits are subsequently laundered through the bank accounts of members of the criminal group.

²⁷ Europol, 2023, The Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam, 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, available at <https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement>.

Migrant smuggling

Criminal networks exploit legal business structures to pursue smuggling activities in various steps of the criminal process.

For the **recruitment** of irregular migrants, social media platforms and E2EE communication applications are used unknowingly.

In the **planning** phase, travel agencies are involved in the organisation of the trip and booking the tickets, in some cases knowingly, for migrants with counterfeit documents. They may even be set up by the criminal network as a cover for their migrant smuggling business. The travel agencies may be located in the country of origin of the irregular migrants or within the EU, for example in Greece for the booking of tickets for onward secondary movements.

Both the retail (mini markets, mobile phone shops, barbers) and hospitality (restaurants, cafes) sectors function as a cover to facilitate **meetings** and to make agreements among migrants and smugglers. They may also function as a hawala office where the migrant places a deposit and where the fee is released to the smuggler upon arrival of the migrant.

A key feature when misusing visas to facilitate entry into the EU, is the abuse of commercial entities for fictitious job offers giving access to work visas. Criminal networks buy existing companies or establish new ones and submit applications for temporary residence for the purpose of employment in these companies. The legal entities declare the creation of jobs and issue letters of guarantee, for which work visas are then obtained. Upon arrival, instead of taking up the employment, the third country national leaves the Member State. It concerns legal businesses in a range of sectors, including construction, cleaning, hospitality, sports associations, employment agencies, etc. The name of the company is changed as the investigation proceeds – as a countermeasure.

In the **transportation** phase, for this crime area in which physical smuggling is inherent, it is logical that the transport and logistical sector is abused - to transport irregular migrants into, within, or from the EU, or to send counterfeit documents to their intended users. Any type of transport lends itself to smuggling irregular migrants, the most common being trucks or lorries, where the involvement of the company as a whole is less common than the direct cooperation of truck drivers with the criminal network.

Also key are rental car companies, that are most often abused unknowingly, particularly for secondary movements. The criminal networks often change rental companies, not only within the country but also within neighbouring countries. Some car rental companies have vehicles that are adapted for the purpose of transporting irregular migrants.

Services such as car-sharing platforms, taxi-companies and international busses are used as cover for illicit activities. In some cases, such companies or their staff are aware and cooperate knowingly and willingly.

Similarly, smugglers may make use of the hospitality sector's facilities to temporarily **accommodate** irregular migrants. Hotels and guesthouses are used as safehouses along the route. Bookings can be made online via booking.com.

For the purchase of nautical equipment for migrant smuggling in small boats to the UK, sport stores and online providers are used. In some cases, criminal networks set up companies as a cover for storage, or to act as a buyer for nautical equipment.

Trafficking in human beings

Many criminal networks involved in the trafficking of human beings set up LBS or abuse existing LBS to facilitate their criminal business. This is particularly the case for networks involved in labour exploitation. They purposely establish companies, such as employment agencies and sub-contracting companies, to **recruit** victims. The forging of identity documents, certificates and contracts via these companies is not uncommon. They may also cooperate with such companies to provide a façade of legality. In the latter case, the LBS are unknowingly used for criminal purposes.

In the area of sexual exploitation, companies operating online sites that advertise sexual services may also be unaware of the criminal **exploitation** of their sites.

Victims of sexual exploitation are exploited in short stay accommodations, hotels, massage parlours, night clubs. Victims of labour exploitation are exploited in a wide variety of cash-intensive sectors where low-waged and seasonal workers abound, including transportation, construction, agriculture, forestry, food processing, hospitality, factory assembly lines, hospitality, retail, carwashes, beauty and cleaning services, housekeeping and domestic assistance. These businesses are often owned by members of the criminal networks.

CASE EXAMPLE – MASSAGE PARLOURS AS DISGUISE FOR SEXUAL EXPLOITATION

Within the prostitution industry, criminal actors set up structures to facilitate their criminal activities, such as massage parlours. These offer legal massages services, as well as illegal sexual services. An Asian human trafficking network organised the sexual exploitation of around 20 victims in massage parlours, in several cities throughout France. Victims were forced to live in the massage parlours to save on accommodation costs. Strong control was exercised over the victims, as bells and video surveillance systems enabled the criminals to monitor the activity in each salon.

Organised property crime

Motor vehicle crime

In the perpetration of motor vehicle crime, legal business structures play a key role in different stages of the criminal process, including the acquisition phase, the transfer of stolen vehicles and parts as well as the final stage of disposal/fraudulent sales.

In the case of embezzlement of motor vehicles, the infiltration into legal business structures comes into play at the initial stage, when cars are fraudulently **acquired** from legally operating companies. In some cases, criminal networks set up front companies to obtain vehicles through fraudulent lease or rental contracts. In most cases, this is likely carried out without the knowledge of the rental or lease companies. In some cases, if the embezzlement of vehicles is also linked to insurance fraud, it is probable that the company has been infiltrated by the criminal network.

Once the vehicles or parts are acquired, they are transferred via transportation/logistics companies. Before the **trafficking** of stolen vehicles and parts, some are also stored for a cool down period in warehouses linked to legal business entities. To facilitate the transfer of stolen vehicles, criminal networks may set up or infiltrate car import and export companies to have shipping documents issued, as well as recycling companies and scrap yards.

CASE EXAMPLE – LBS SET UP TO TRADE STOLEN VEHICLE PARTS

A criminal network made up of more than 50 individuals was involved in the systematic theft of catalytic converters, with the goal of selling and exporting the extracted precious metals abroad, namely to Germany, the United Kingdom, and South Korea. A company, active in the recycling of (precious) metals and the dismantling of electrical and electronic equipment, was created ad hoc for this purpose. The stolen goods were sold via this company. The company also had an online catalogue to attract potential customers.

More than 7 000 stolen catalytic converters could be associated with this company. The criminal proceeds are estimated at EUR 3.5 million.

In order to facilitate the **sales** of stolen vehicles and parts, criminal networks infiltrate car dealerships, car repair shops and vehicle inspection companies. In some cases, companies are aware of the origin of motor vehicles and parts and are complicit in selling the illegal merchandise. There are also companies, that are established by the criminal networks themselves, to facilitate the sales transactions.

Cultural goods trafficking

The infiltration into legal business structures in the context of trafficking cultural goods plays a key role in the facilitation of **sales** of illicitly acquired and forged cultural goods. Various types of commercial entities are infiltrated for this purpose, including international art fairs, art markets and dealers, galleries, auction houses and other retail stores, such as antique shops. While in some cases these legal entities are infiltrated unknowingly, in the area of cultural goods trafficking it is common that members of trafficking networks set up their own companies or are embedded in the businesses facilitating the sales of cultural objects.

CASE EXAMPLE – LBS SET UP TO TRADE CULTURAL GOODS

A member of a criminal network active in cultural goods trafficking operated a commercial business for the sale of works of art and coins. In several cases, an accomplice abroad sold works of art through an internationally renowned department store, at which he was employed.

Restoration companies of antiques, such as stolen archaeological goods, also often facilitate the criminal process in a complicit manner.

Organised robberies

In the context of organised robberies, legal business structures are infiltrated by criminal networks during the **preparation** phase and most notably in the final stage of the criminal process in order to **fence** the stolen goods. In terms of the former, robbers may infiltrate (security) companies to acquire information on the transportation of money.

Stolen jewellery, stolen watches and other valuables may be knowingly or unknowingly sold by vendors operating in the diamond and jewellery retail sector or in pawn shops. Criminal networks may also set up their own companies to facilitate the sale of stolen items.

Organised burglaries and thefts

Criminal networks infiltrate legal business structures mainly for the **storage, transportation and sale** of stolen goods. Criminal networks active in organised burglaries and thefts also infiltrate car rental companies to rent cars to **facilitate the perpetration of the offence**. Stolen goods and, in some cases, money, are further transported using freight and courier companies, but also through foreign chartered buses. Sales channels include retail stores and online marketplaces. Companies used for the transport or sale of stolen goods are in some cases set up by the criminal networks themselves.

Money transfer companies are used to **send money** to the home country or other persons or the leader of criminal networks.

Firearms trafficking

A portion of illegally circulating firearms and heavy pyrotechnics are diverted from legal supply, with the involvement of employees. In some cases, criminal networks also infiltrate weapons manufacturers and divert weapons from the legal production line before the firearms are assigned any serial number, markings, weapon number or proof mark of the company. Criminal networks also set up LBS to facilitate the **procurement** of firearms or firearm components. In the latter case, criminal networks and actors purchase freely available firearm parts, supplement them with illegally manufactured or diverted parts, and assemble these into fully-functioning firearms.

Firearms traffickers abuse a variety of legal business structures to enable their **trafficking** activities without the knowledge of the company operators. Examples of such abuse include when firearms, firearm parts and ammunition are illicitly transported using transport companies, rented cars, long distance bus companies, or parcel services. However, courier companies may be also set up by criminal networks themselves to facilitate the smuggling of weapons.

Money laundering

The most threatening criminal networks in the EU use real estate as one of the main techniques to launder their illicit profits (41 %). In particular, money laundering activities can take place during the following steps of the real estate process: purchase of property and terrain development, building process, economic exploitation of the property. When laundering through investments in real estate, some criminal networks launder their profits through the purchase of physical and financial assets often linked to private companies or by financial and legal experts who are in some cases unaware of the criminal origin of the assets. The ownership of these assets is, when necessary, exchanged between companies, either as a means of payment for other criminal activities and/or as an investment. This blending of the illicit profits with legal assets and the fact that there are no financial transactions involved during the

transferral of assets makes it challenging for investigators to link the movement of assets to a criminal venture²⁸.

Creating a complex web of companies, often without real activity, with strawmen as administrators and located in various countries, is another technique used for money laundering purposes. False contracts and invoices make it possible to transfer large amounts of money via the bank accounts of these companies. Other techniques include searching for companies on the brink of bankruptcy in order to buy these out, placing money in off-shore companies and bank accounts of third parties, fraudulent book keeping, and the issue and use of invoices of non-existent business activities.

CASE EXAMPLE – LAUNDERING THE ILLICIT PROCEEDS OF DIGITAL CONTENT PIRACY THROUGH INVESTMENT IN REAL ESTATE AND LUXURY CARS

Internet Protocol Television content and television networks protected by a payment wall were decrypted by a criminal network and sold to a large number of customers. Members of the network have also been conducting money laundering activities, using a variety of methods to launder their illicit proceeds. These include investment in real estate and high-value goods, such as luxury goods. Money laundering activities take place both in and outside of the EU.²⁹

Dedicated expertise is indispensable when it comes to money laundering, and experts are often considered critical and irreplaceable in the criminal process. The availability of such expertise for criminal networks is linked to a higher threat, as it allows them to bring criminal money into the legal economy and gain more power in society.

A few amongst the most threatening criminal networks are **specialised criminal service providers** engaging solely in the provision of money laundering services to other criminal networks, without being active in any other crime area.

CASE EXAMPLE – MONEY LAUNDERING NETWORK OFFERING TRADE-BASED MONEY LAUNDERING SERVICES

A specialised criminal service provider network, composed of Italian, Albanian, Colombian, Moroccan, and Syrian nationals, has built up an international network of companies to launder illicit proceeds. The criminal network offers professional services to hide the origin of proceeds generated from illegal drug trafficking in South America. In order to launder drug profits, the network offers a service of trade-based money laundering. The drug producers would provide drugs to Italian buyers as a form of credit. The profits generated from the sale of the drugs in Europe are then picked up by brokers, introduced into companies, and used for ordering goods such as mobile phones from China. These goods are then shipped to the United States and further transported to Colombia, where they are offered on the market. Upon being sold, the cartels receive the cash and thus their veiled payment for the drugs provided to European sellers³⁰.

²⁸ Europol, 2024, Decoding the EU's most threatening criminal networks, available at <https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks>.

³⁰ Europol, 16 February 2024, Properties worth EUR 48 million frozen after cocaine sweep in Ecuador and Spain, available at <https://www.europol.europa.eu/media-press/newsroom/news/properties-worth-eur-48-million-frozen-after-cocaine-sweep-in-ecuador-and-spain>.

In one case, the criminal network developed a LBS that comprised 15 enterprises located in the same city, whose accounts (all online) allegedly recorded movements of funds in four years that reached a total of 50 million euros. The fact that the accounts were opened online was crucial, as in the past they tried to open accounts in person but failed to meet the requirements and necessary documents.

When the criminal activity is carried out by opportunistic entrepreneurs that abuse their own company in order to make extra profits by performing their work unlawfully (i.e. illicit waste management, wildlife crimes, VAT fraud,) the laundering of the criminal proceeds is usually done via the same company(-ies), as there is no need to create parallel structures devoted to money laundering.³¹

Groups on end-to-end encrypted applications seem to have replaced peer-to-peer platforms (i.e. LocalBitcoins) to connect people who want to exchange cryptocurrency for cash and vice versa and avoid compliance checks. Sometimes, cash is converted back to stablecoins as well, for example USDT. The involvement of underground banking solutions and criminal finances for the laundering of crypto assets also appears to be increasing, probably as a result of the more stringent implementation of EU-wide anti-money laundering regulations. The use of cryptocurrency debit cards has also re-emerged, as these can be used to quickly convert cryptocurrency into cash at ATMs.

In 2023, an increase in swapping services has been observed. Swapping is mostly done to ensure the security and stability of criminal funds – for security, cryptocurrencies are swapped to privacy coins, while for stability, cryptocurrencies are swapped to stablecoins. Generally, swapping services provide information on the origin, conversion and destination address to law enforcement agencies.³²

The acquisition of legal business structures at risk

Criminal networks often exploit businesses in financial difficulty. Criminal networks offer 'investment' to business owners in exchange for partial or full ownership, or they may extend high-interest loans to owners, with the aim of gaining control over the business if the owner defaults. The potential for abuse is heightened during economic downturns or crises (like the COVID-19 pandemic), when many legitimate businesses in the hospitality sector struggle financially and may be more vulnerable to acquisition by criminal networks.

³¹ Europol, 2022, Environmental crime in the age of climate change, available at <https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment>; Information contributed to Europol.

³² Europol, 2024, IOCTA 2024, available at <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>.

A BORDERLESS PHENOMENON

Global links between organised crime and legal businesses

Legal businesses that facilitate organised crime in the EU are situated in the EU and beyond. The majority of the most threatening criminal networks active in the EU do abuse legal businesses that are also situated in the EU. A large part of the criminal business processes do indeed take place in the EU and, therefore, criminal networks also use LBS situated in the EU as an indispensable part of the modus operandi or to facilitate it. 70 % of the most threatening criminal networks abuse LBS only in the EU.

Nevertheless, there is a significant share of criminal networks that are involved in legal structures located in other places in the world. Criminally infiltrated LBS are situated in almost 80 countries across the globe. 20 % of the most threatening criminal networks abuse LBS both in and outside the EU, and only 10 % outside the EU.



Most abused LBS are situated in the EU or in the EU's neighbourhood

All 27 EU Member States host legal business structures that are being abused or infiltrated by organised crime actors. No Member State is immune.

CASE EXAMPLE – LBS ABUSED MULTIPLE TIMES BY SEVERAL CRIMINAL NETWORKS INVOLVED IN SYNTHETIC DRUG PRODUCTION AND VAT FRAUD

In 2023, a criminal network comprised of individuals from Czechia, Slovakia, Poland and Romania, involved in the illegal manufacture and distribution of precursors for methamphetamine production, was dismantled. Two members of the criminal group operated a legitimate pharmaceutical company while establishing ad hoc companies to facilitate the supply of the illegal product. This criminal scheme involved nearly 40 companies across Europe, enabling the criminals to commit VAT fraud through the cross-border trade of goods and services, including legally purchased packaging materials and transport, used for the criminal activity.

This shows the borderless nature of the most threatening criminal networks, including when it comes to their use of LBS as an enabler. Abused LBS are indeed located throughout the globe, with countries mentioned in Europe, Asia and the Pacific, the Americas, and Africa.

Yet, just like the most threatening criminal networks tend to constrain their criminal activity to a limited number of countries³³, misused LBS are also more often located in the EU's neighbouring countries. Only in the case of need, they are able to misuse LBS in other regions of the world also.

The non-EU European countries where LBS are abused most by the most threatening include Albania, Belarus, Bosnia and Herzegovina, Georgia, Iceland, Moldova, Montenegro, North Macedonia, Norway, Russia, Serbia, Switzerland, Türkiye, Ukraine and the United Kingdom.

Occasionally, criminal networks abuse LBS in other global regions outside the EU: in Africa, Asia (including the Middle East) and the South Pacific (Australia, New Zealand), and the Americas (including the Caribbean, North- and Latin America).

Logistics and transport worldwide most vulnerable to criminal exploitation

When considering the sectors that are abused in the various locations, the logistics sector appears most frequently, and this is all over the world. Within this sector, the transport sector is the most vulnerable.

CASE EXAMPLE – LBS IN LATIN AMERICA AND THE EU ABUSED MULTIPLE TIMES FOR COCAINE SMUGGLING

Two companies involved in the legal shipment of bananas, a Latin American export company and a European importer, were repeatedly used by criminal groups engaged in cocaine smuggling into European ports. The discovery of cocaine concealed in containers by the police linked this criminal activity to a powerful criminal group connected to a criminal network from the Western Balkan region. The two companies appear in several cocaine seizures involving different criminal groups with a similar modus operandi. Yet, there is no evidence that the companies were aware of these criminal activities.

³³ Europol, 2024, Decoding the EU's most threatening criminal networks, available at <https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks>.

Cash-intensive businesses are another key sector that stands out and this applies globally. These LBS are mainly situated in the hospitality and retail sector and are abused for money laundering activities.

Also, LBS in the construction sector, including the real estate sector and the financial sector, including financial institutions, bank and insurance, money exchange and transfer and trading companies, are often abused for money laundering.

CONCLUSION

This report has demonstrated the vast scope and depth of criminal networks' abuse of legal businesses for illicit purposes. The infiltration spans all business sectors, from cash-intensive enterprises to real estate, construction and logistics, but all sectors are vulnerable to potential exploitation. Criminal networks utilise these structures at every level – from wholly-owned criminal enterprises to legitimate private sector firms unwittingly facilitating illicit activities.

Legal businesses are misused to support every aspect of criminal operations, from committing and concealing crimes to laundering profits. They facilitate criminal objectives across both online and offline environments, affecting all stages of the criminal process. This issue is prevalent across all EU Member States and global regions, with nearly all criminal networks relying on legal business structures to sustain their activities and expand.

Effectively addressing this pervasive threat demands a comprehensive, multi-layered strategy. Such an approach must bring together law enforcement, regulatory bodies, the private sector, international allies, and initiatives like the European Multidisciplinary Platform Against Criminal Threats (EMPACT). A truly robust response requires both reactive measures, targeting in particular High Value Targets via operational taskforces, and proactive initiatives, such as the development of risk indicators to detect vulnerable companies susceptible to criminal interference.

An integrated approach, combining proactive prevention with reactive enforcement, is essential to dismantling the stronghold of criminal networks on legal business structures.

ANNEX

For this analysis, businesses are clustered in sectors. There may be an overlap between the sectors.

- ▶ **Financial:** the financial sector refers to the businesses and institutions that manage money and provide intermediary services to transfer and allocate financial capital in an economy. Key entities of the financial sector are banks (retail and investment), insurance providers, investment managers, exchanges, payment processors.
- ▶ **Cash-intensive businesses:** a cash-intensive business involves a high volume of cash flows in return for the provided products and services. It is a category that encompasses businesses active in a wide range of sectors, such as hospitality and leisure (including gambling), retail and consumer goods, art and luxury, automotive and transportation, health and personal care, crafts and trades, various types of services.
- ▶ **Real estate/construction:** Real estate refers to the land above and below the earth's surface, including all things that are permanently attached to it either natural or artificial. The construction sector is related to real estate, as it concerns the supply of materials, contracted and sub-contracted building and maintenance services.
- ▶ **Manufacturing:** Manufacturing encompasses the entirety of interrelated economic, technological and organisational measures directly connected with the processing and machining of materials, such as all functions and activities directly contributing to the making of goods.
- ▶ **Trade:** Trade refers to the exchange of goods (tangible and non-tangible) or services between two or more parties, often involving the transfer of money as payment. Trade can occur between individuals, businesses and it can take many different forms, including direct bartering, cash transactions and electronic payments. The **energy sector** relates to producing or supplying energy as a trading commodity. It includes companies involved in the exploration and development of oil or gas reserves, oil and gas drilling, and refining. The energy industry also includes integrated power utility companies such as renewable energy and coal.
- ▶ **Logistics:** Logistics is the network of services that supports the physical movement of goods, trade across borders and commerce within borders. It comprises an array of activities beyond transportation, including warehousing and storage, terminal operations (e.g. in ports and airports), express delivery, customs brokerage, as well as data and information management³⁴.
- ▶ **Technology and communication:** The technology sector encompasses businesses revolving around the manufacturing and sale of electronics, creation of software, computers, or products and services relating to information technology (IT), including artificial intelligence. Communication services encompass a wide array of services and technologies that enable people to connect, share information and communicate, such as phone services and digital platforms like the internet.

³⁴ The World Bank, Connectivity, Logistics & Trade Facilitation, Facilitating Trade at the Border, Behind the Border, and Beyond, available at <https://www.worldbank.org/en/topic/trade-facilitation-and-logistics>.

LIST OF ABBREVIATIONS

ATM	Automated Teller Machine
BPH	Bullet Proof Hosting
C2	Command and Control
CHSG	Common Horizontal Strategic Goal
CSAM	Child Sexual Abuse Material
CSE	Child Sexual Exploitation
DDoS	Distributed Denial of Service
E2EE	End to End Encryption
EFECTA	European Financial and Economic Crime Threat Assessment
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
EU SOCTA	European Union Serious and Organised Crime Threat Assessment
EXIF	Exchangeable Image File Format
IOCTA	Internet Organised Crime Threat Assessment
IT	Information Technology
ISP	Internet Service Provider
LBS	Legal Business Structures
LEA	Law Enforcement Agency
MTIC	Missing Trader Intra-Community
MLAT	Mutual Legal Assistance Treaty
NPS	New Psychoactive Substances
OA(P)	Operational Action (Plan)
OFS	Online Fraud Schemes
THB	Trafficking in Human Beings
VAT	Value Added Tax
VER	Verified Emission Reductions
VPN	Virtual Private Network
WEEE	Waste electric and electronic equipment