EUROPOL | EFECC
European Financial and Economic Crime Centre

Enterprising criminals

Europe's fight against the global networks of financial and economic crime

Foreword

CATHERINE DE BOLLE

Executive Director, Europol

The fallout from the COVID-19 pandemic has weakened our economy and created new vulnerabilities from which crime can emerge. Economic and financial crime, such as various types of fraud, money laundering, intellectual property crime, and currency counterfeiting, is particularly threatening during times of economic crisis. Unfortunately, this is also when they become most prevalent. The European Economic and Financial Crime Centre (EFECC) at Europol will strengthen Europol's ability to support Member States' and partner countries' law enforcement authorities in fighting the criminals seeking to profit from economic hardship. EFECC will serve as a platform and toolbox for financial investigators across Europe. We look forward to making lasting partnerships with them and fighting economic and financial crime together.

Key findings

» Money laundering and criminal finances are the engines of organised crime. Without them, criminals would not be able to make use of the illicit profits from their various serious and organised crime activities in the EU.

» Various fraud schemes are among the fastest-growing criminal threats in Europe. Fraud targets private citizens, small and medium enterprises, global corporations and critical infrastructure. During the COVID-19 pandemic, various types of online fraud have been among the most visible criminal activities.

» To effectively disrupt and deter criminals involved in serious and organised crime, law enforcement authorities need to follow the money trail as a regular part of their criminal investigations with the objective of seizing criminal profits.

» Throughout the COVID-19 pandemic, organised crime groups (OCGs) involved in the production and distribution of counterfeit goods have once again proven highly adaptable in terms of shifting product focus, marketing and packaging.

» Missing trader intra-community (MTIC) fraud is the most commonly encountered type of value added tax (VAT) fraud in the EU. Countries applying high VAT rates on specific goods or services are more likely to be targeted by MTIC fraudsters. Based on studies and cases supported at EU level, Europol estimates between €40 to 60 billion[1] is lost annually to MTIC fraud schemes taking place in the EU[2].

This report has been prepared to complement the launch of the European Financial and Economic Crime Centre (EFECC) at Europol in June 2020. The document provides an overview of the most threatening phenomena ***in the area of economic and financial crime including*** various types of fraud, the production and distribution of counterfeit goods, money laundering and others.

1 Europol 2018, MTIC fraud investigation and LEA's cooperation improving, accessible at https://www.europol.europa.eu/publications-documents/mtic-fraud-investigation-and-leas-cooperation-improving

2 EU Commission 2018, The concept of the Tax Gap, accessible at https://ec.europa.eu/taxation_customs/news/vat-gap-report_en - accessed at 01/06/2020.

Setting the (crime) scene

Economic and financial crimes are not victimless

Economic and financial crimes are a highly complex, significant threat that affects millions of citizens and thousands of companies in the EU every year. These crimes undermine our economy and financial sector, which deprives us of prosperity, economic growth and employment. Although indirect, the impact these crimes have on society cannot be underestimated.

Financial and economic crimes encompass a range of different criminal activities, from simple fraud to large-scale sophisticated financial schemes, often combining licit and illicit financial transactions. This mix of legal and illegal often makes it challenging for law enforcement to investigate the true extent of these illegal activities. By exploiting legal financial systems, criminals are able to launder criminal money and strengthen their criminal operations.

Economic crimes, such as the counterfeiting of goods, erode trust in legal businesses and put the health and safety of consumers in the EU at risk.

Despite all measures taken to combat economic and financial crimes, opportunities for these types of crimes have increased as the market for legal financial services has diversified and technology continues to change the way and speed of how financial transactions occur.

Low risk, high profit

Economic and financial crime currently offers a relatively low risk of discovery and prosecution with potentially very high profits. This dynamic makes these criminal activities very attractive to organised crime. The complexity of these crimes and the sophisticated expertise necessary to carry them out have always made them difficult to detect and investigate. However, technical innovation and the digitalisation of financial transactions have presented additional challenges for law enforcement authorities. Many of these crimes are now even less visible than before and more challenging to investigate.

Fraud schemes too often remain undetected. Successful law enforcement actions against these complex schemes require close international cooperation across several jurisdictions, often involving non-cooperative offshore tax havens, as criminals operate without regard for international borders. Organised crime groups (OCGs) operating internationally benefit from differences in national legislation. Individual and organisational vulnerabilities such as insufficient awareness on the part of victims and low risk perception by criminals are enabling factors for most types of fraud[3].

There is increased awareness that certain acts within the financial sector that were once considered to be merely poor business practice may in fact have been criminal. Widespread reckless investment, misrepresentation of financial statements and conspiring to manipulate inter-bank interest rates fall within the definition of serious and organised crime. The huge losses associated with high-level financial fraud undermine social security systems and destabilise economies.

3 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

The number of fraud schemes targeting individuals, companies and the public sector is increasing. The COVID-19 pandemic in Europe has provided ample evidence that criminals are quick to adapt these schemes to changing conditions in order to exploit fears and vulnerabilities.

The fallout from the COVID-19 pandemic will test the resilience of our economic and social infrastructure for years to come. Law enforcement authorities across Europe must prepare themselves to counter an increasing number of cases involving economic and financial crime.

What is happening today that may impact the economic and financial crimes of tomorrow?

Technology drives change in behaviours

Customers are changing their financial behaviour and the tools with which they access and manage their finances. Financial technology (fintech) solutions are now emerging as the standard way for consumers to interact with financial service providers.

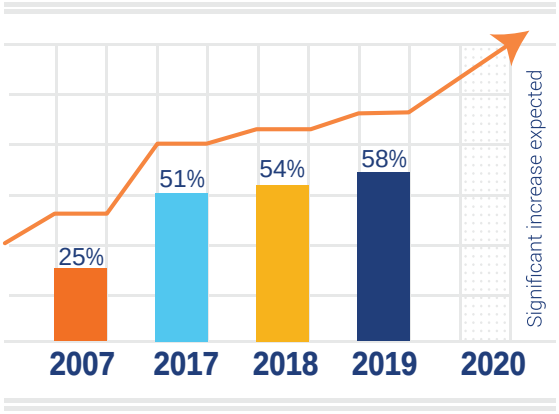
Altogether, 58% of customers banking in the EU now regularly use digital online solutions such as websites or applications to carry out transactions. While this has represented a leap in usability and accessibility of financial services for customers and financial service providers alike, this development also entails some risks.

Customers are not necessarily proficient users of these services and a lack of technical knowledge and experience may make them vulnerable to attacks by cybercriminals deploying phishing techniques and malware solutions in order to gain access to online accounts.

On the side of the financial services, increasing digitalisation and less direct interaction with customers has the potential to weaken know-your-customer (KYC) procedures, which were put in place to prevent tax fraud, money laundering and using the financial system to finance crime and terrorism.

Weakened KYC regimes increase the vulnerability of financial services to be used for various criminal activities including online banking fraud.

Research shows that mobile banking engagement has risen by 50% since the end of 2019. The COVID-19 pandemic and the steps taken to combat it are likely to accelerate the move to digital and/or fintech solutions[4].



Use of online banking services, percentage of online users compared to total number of customers, EU.

Source: EUROSTAT

As fintech solutions become established, innovation in financial technology must advance in terms of cybersecurity to protect an increasing number of customers against financial cybercrime threats.

The dark web has provided a platform for cybercriminals to exchange tools, expertise and contact details to orchestrate attacks and scams. This level of coordination is new and has resulted in more sophisticated attacks against targets in the EU.

One of the key challenges is the convergence of different types of criminal activities such as fraud, cybercrime and financial crime as one threat.

4 Forbes 2020, Coronavirus drives 72% rise in use of fintech apps, accessible at https://www.forbes.com/sites/simonchandler/2020/03/30/coronavirus-drives-72-rise-in-use-of-fintech-apps/#356fae2b66ed

Economic downturns create opportunities for crime

While a recession entails hardship for the licit economy, criminal ventures are placed to take advantage and exploit opportunities emerging as a result. In particular, a number of sectors are more adversely affected by negative economic conditions, such as construction, hospitality, travel and tourism. Companies operating in these sectors in difficult times are often vulnerable to infiltration or takeovers by criminals.

Difficulty in accessing capital through loans during a recession pushes some individual and companies to make use of unregulated financial services, which increasingly operate online as unlicensed banks or lenders that offer different types of loans and, in some cases, scam their customers.

Lack of accessible capital also potentially opens up struggling businesses and individuals to the investment of funds stemming from criminal activities. In the past, this type of vulnerability has been particularly observed in the real estate sector.

Economic stimuli such as those proposed in the wake of the COVID-19 pandemic will be targeted by criminals seeking to defraud public funding. In some cases, they are likely to attempt to use corruption in order to access these funds.

Various types of investment fraud flourish in times of economic hardship. It can be expected that some of these cases of fraud will emerge with a COVID-19 spin in the event of a sustained recession. This may involve fraudulent investment offers into companies producing hygiene and sanitary products such as masks and other personal protective equipment (PPE). Some of these companies will be set up to fail and are only operated to extract investments.

Previous investigations have shown that investment fraud schemes can generate profits of hundreds of millions of euros per year and are typically operated by networks of 10 to 20 suspects.

Corruption

Some high-level investigations into organised crime involving corruption may lead one to assume that corruption is on the rise. Almost all significant cases against serious and organised crime involve corruption ranging from low-level bribery to high-level political corruption.

Corruption remains systematically under-investigated. The use of online transfers of criminal money and the use of cash for lower-level bribery often make it difficult to detect financial flows and to uncover corruption.

Intellectual property crime: counterfeit and substandard goods

Counterfeiting and piracy comprise a range of illicit activities relating to the infringement of registered trademarks and patents (for counterfeit goods) and copyright and design (for piracy). Together, these constitute intellectual property offences. The value and usage of intellectual property rights continues to expand, providing growing incentives for criminals to exploit and infringe these rights.

Counterfeiting and piracy are lucrative criminal activities while at the same time, similar to other economic crimes entail a relatively low risk of detection. Criminal sentences for counterfeiting are also considerably lower than for many other criminal activities, such as drug trafficking, document fraud or currency counterfeiting. Several Member States have shifted their focus away from fighting intellectual property crime to other criminal activities such as drug trafficking, migrant smuggling, trafficking in human beings and terrorism.

At the same time, OCGs are increasingly involved in the production and distribution of counterfeit and pirated goods. They have adopted increasingly sophisticated and complex modi operandi, facilitated by technological advancements and complex global distribution channels. Online marketplaces are increasingly becoming an important source of income for criminal groups involved in the sale of counterfeit and pirated goods.

The economic impact of intellectual property rights infringements is considerable. The distribution of counterfeit and pirated goods cuts revenue for legitimate businesses, negatively affects their reputation and deprives governments of tax revenue.

This type of criminal activity also hampers innovation and leads to job losses. A series of studies over recent years by the EU Intellectual Property Office (EUIPO) estimates that 13 market sectors particularly vulnerable to counterfeiting have experienced direct annual losses. Collectively, these sectors lose €60 billion a year, or 7.5 % of their total sales.

In addition to harming the economy, counterfeit goods can have a serious impact on the health and safety of consumers, as well as negative environmental consequences. Reliable quantitative assessments of this type of harm are generally not available, but law enforcement authorities in the EU frequently detect counterfeit goods that could pose considerable dangers to consumers or the environment. In recent years, there has been an increase in everyday consumer items targeted by counterfeiters, many of which pose considerable risks to the health and wellbeing of consumers. These common consumer items include cosmetics, electronics, food and drinks, pharmaceuticals, spare vehicle parts and toys[5].

During the COVID-19 pandemic, OCGs involved in the production and distribution of counterfeit goods have once again proven highly adaptable in terms of shifting product focus, marketing and packaging.

Some of the platforms used to advertise and sell these goods predate the COVID-19 pandemic and have been monitored by law enforcement authorities. In addition to these established platforms, a significant number of new websites were created for the express purpose of profiting from the pandemic. These websites sell fake COVID-19 home test kits and offer unconfirmed and often incorrect

5 EUIPO and Europol 2019, Intellectual Property Crime Threat Assessment 2019, accessible at https://www.europol.europa.eu/newsroom/news/new-threat-assessment-confirms-links-between-counterfeiting-and-organised-crime-in-eu

advice on the treatment of COVID-19[6].

Some criminal groups may seize opportunities during the COVID-19 crisis to offer counterfeit or substandard food items more widely due to increased demand following fears of a perceived food shortage. Particular attention should be paid to developments and criminal innovation if a genuine vaccine for COVID-19 is developed as this will likely prompt a wave of offers for counterfeit vaccines.

While some product offers for counterfeit goods related to the COVID-19 pandemic have appeared on the dark web, the product offerings available there remain limited compared to the surface web, which continues to host the primary distribution platforms for counterfeit goods.

6 Europol 2020, Viral marketing: Counterfeits in the time of pandemic, accessible at https://www.europol.europa.eu/sites/default/files/documents/report_covid_19_-_viral_marketing_counterfeits.pdf

Fraud

Fraud comprises offences committed with the intention to defraud using false and deceitful pretexts resulting in the voluntary but unlawful transfer of values, goods or an undue advantage to the fraudsters[7]. It is difficult to estimate the financial loss and criminal profits resulting from online fraud as many instances go unnoticed or unreported by the victims.

Investment fraud relies on social engineering techniques – the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes – making it particularly hard to counter. This type of fraud can be highly lucrative.

Below are the most common investment fraud schemes in the EU.

Boiler room schemes, where fraudsters cold call their victims and pressure them into investing in non-existent or very low-value stocks. The criminals often use false documents and certificates to present their company and stock as legitimate.

Ponzi schemes, also known as pyramid schemes, where fraudsters attract a group of initial investors with promises of very high returns in a very short time. To attract more victims, the fraudster will start to repay the initial investors using funds accrued from additional investors. Ultimately, the investors are left empty-handed when the fraudster disappears with the funds, which have been laundered through multiple bank accounts held by various front companies in different jurisdictions.

In mass marketing fraud criminals use a variety of communication means, such as telephone calls, social media, mass mailing, television or radio, to contact victims and solicit money or other items of value in one or more jurisdictions.

Payment order fraud, also called CEO fraud or business email compromise (BEC), relies on social engineering techniques and malware. Typically, criminals transfer stolen funds through a series of accounts in various countries before they reach destination accounts outside the EU.

Insurance fraud describes the defrauding of private and public insurance providers. OCGs are increasingly involved in fraud schemes targeting the healthcare sector.

EU subsidy fraud entails the submission of fraudulent applications for EU grants or tenders. Typically, these applications are based on false declarations, progress reports and invoices.

Procurement rigging involves the use of bribes to elicit information or directly influence the evaluation of bids in order to win public service tenders in competition with legal businesses. This type of manipulation is particularly notable in the energy, construction, information technology and waste management sectors.

Benefit fraud involves the targeting of social and labour benefit schemes and is strongly linked to trafficking in human beings and migrant smuggling.

Loan and mortgage fraud involves fraudsters using fraudulent documents to obtain bank loans which are never paid back.

7 Europol, Analysis Project Apate.

> **CASE EXAMPLE**

Masterminds behind CEO fraud ring arrested after causing more than €18 million in damage[8]

On 28 May 2018, the French National Gendarmerie - Section de Recherches of Bordeaux, supported by the Israeli authorities and Europol, arrested the main suspects of an organised crime group behind a total of 24 cases of CEO fraud across Europe to the detriment of Belgian and French-based commercial companies, causing more than €18 million worth of damage.

In the framework of this large-scale CEO fraud operation, seven individuals had been already arrested in previous phases of the investigation in Belgium and France through coordinated actions, also supported by Europol. This investigation is the follow-up of systematic operational activities initiated in 2016 when two French **companies fell victim to CEO fraud, incurring an estimated €1.2 million financial loss.**

Over the course of the action, four suspects were arrested, and relevant house searches were performed in Israel, also resulting in the seizure of computers, phones **and financial information. The operation was developed by France in cooperation** with investigators from Belgium, Israel, Romania and continued support from Europol.

Fraud schemes are among the fastest-growing criminal threats in Europe. Fraud targets private citizens, small and medium enterprises, global corporations and critical infrastructure. During the COVID-19 pandemic, these types of online fraud have been among the most visible criminal activities.

Advance fee fraud schemes are increasingly perpetrated online involving payments using alternative payment methods such as online vouchers. Many investment fraud schemes now exclusively take place online or involve the advertising of investment opportunities on social media. Fraudsters increase their involvement in online investment opportunities including Forex trade platforms, binary options and online crowdfunding[9]. During the COVID-19 pandemic, this type of modus operandi has been frequently reported.

Fraudsters also rely on social media and instant messaging applications to obtain sensitive information from their victims. Fraudsters are able to buy access to personal data as part of crime-as-a-service offers.

8 Europol 2018, Masterminds behind CEO fraud ring arrested after causing more than EUR 18 million of damage [Press Release], accessible at https://www.europol.europa.eu/newsroom/news/masterminds-behind-ceo-fraud-ring-arrested-after-causing-more-eur-18-million-of-damage

9 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

Stolen data can easily be purchased online.

Criminal groups involved offering crime-as-a-service online act like major corporations. The leaders of these OCGs are typically based outside the EU. They operate through a layer of middle management based inside the EU. This includes OCG members who are experts in the areas of taxation, banking, legal and finance, cybercrime and ICT, and money laundering. Lower-level members of these groups have little expertise and work as money mules, call centre operators, cash couriers, among others. Some operate call centres, which employ hundreds of staff working in shifts and generate up to €100 million revenue in a few months.

These OCGs involved typically operate as loose networks made up of experienced fraudsters. Fraudsters establish an extensive network of mule accounts and shell companies across the world to obscure the destination of stolen funds. Criminals often route profits to under-regulated jurisdictions, which makes it challenging and sometimes impossible for law enforcement authorities to trace and investigate.

Tax fraud

All EU Member States suffer substantial revenue losses as a result of sophisticated frauds. VAT is a considerable tax, contributing to about one-fifth of the total tax levied by Member States. €137.5 billion or about 12% of the VAT is lost annually. Known as the VAT Gap, part of the difference in VAT revenue and that collecte, can be linked to VAT fraud and evasion[10]. MTIC fraud[11] generates criminals billions of euros in profit. Excise tax fraud also deprives national budgets of billions of euros.

Law enforcement authorities countering these phenomena are challenged by the inherent cross-border nature of these activities, the necessity to cooperate with multiple authorities including customs authorities and the role of non-cooperative jurisdictions during the asset recovery phase.

In 2019, the European illicit cigarette market represented 43.6 billion cigarettes or 8.6 % of EU consumption. The distribution of counterfeit and contraband tobacco products is estimated to cause annual revenue losses of up to €10 billion to governments in the EU[12].

Tobacco remains the main commodity subject to excise fraud in the EU. Designer fuel fraud is increasing and has resulted in multi-million-euro losses in revenue for Member State governments. This type of fraud entails the non-payment of taxes on fuel, either by using high diesel content alternatives (lubricants, rust agents, base oils) or by mixing liquids so fuels fall outside the excise duty regime.

10 EU Commission 2018, The concept of the Tax Gap, accessible at https://ec.europa.eu/taxation_customs/news/vat-gap-report_en - accessed at 01/06/2020

11 MTIC fraud occurs when a supplier – the so-called conduit company – established in one Member State supplies (VAT-exempt) goods to a second company located in another Member State, the so-called missing trader. The missing trader takes advantage of the VAT-exempt intra-community supply of goods and resells the same goods in the domestic market of the second Member State at very competitive prices. This missing trader is usually not a real person, for instance a new company with no real seat or activity.

12 KPMG 2019, Stella Report: A study of the illicit cigarette market in the EU.

MTIC fraud

VAT fraudsters generate multi-billion-euro profits by avoiding paying VAT or by fraudulently claiming repayments of VAT from national authorities following a chain of transactions. The most commonly encountered types of VAT fraud in the EU is MTIC fraud. Countries applying high VAT rates on specific good or services are more likely to be targeted by MTIC fraudsters.

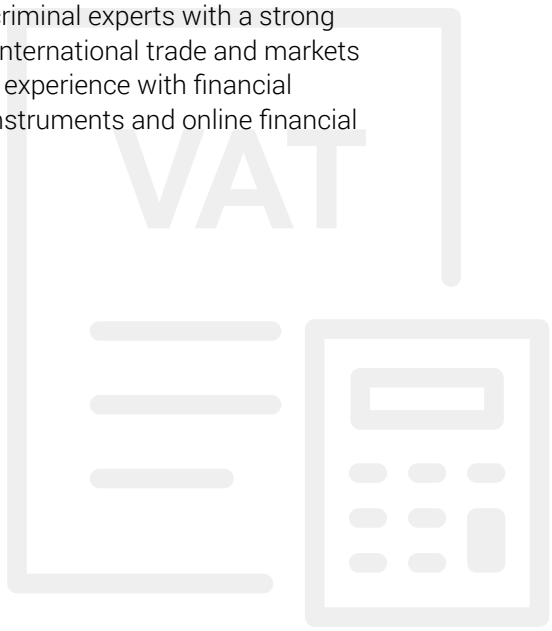
Based on studies and cases supported at EU level, Europol estimates that between €40 to 60 billion[13] is lost annually to MTIC fraud schemes in the EU[14].

Any goods or services can be susceptible to VAT fraud. The most commonly targeted products are currently food products, electronics, vehicles, metals, intangible goods and the energy sector (oil, gas, electricity, carbon credits and green energy certificates).

OCGs involved in VAT fraud are highly specialised, adapting easily to legislative changes and other administrative measures put in place by the EU and national authorities. They shift markets and commodities to exploit gaps in tax legislation[15]. They continuously shift from one commodity market to another to avoid reverse charges and discovery by law enforcement or other regulatory authorities. They systematically set up new companies and use different figureheads[16].

The OCGs involved in VAT fraud are highly specialised and typically only engage in this type and similar types of fraud[17]. However, in some cases these OCGs also offer their services to launder criminal proceeds to other OCGs involved in more traditional types of criminal activity such as drug trafficking.

OCGs rely on criminal experts with a strong knowledge of international trade and markets and extensive experience with financial markets and instruments and online financial trading.



13 Europol 2018, MTIC fraud investigation and LEA's cooperation improving, accessible at https://www.europol.europa.eu/publications-documents/mtic-fraud-investigation-and-leas-cooperation-improving

14 EU Commission 2018, The concept of the Tax Gap, accessible at https://ec.europa.eu/taxation_customs/news/vat-gap-report_en - accessed at 01/06/2020.

15 Europol information.

16 Europol information.

17 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

> CASE EXAMPLE

EU-wide VAT fraud organised crime group busted[18]

Between 18 and 20 April 2018, 58 suspects were arrested in Belgium, Germany, Portugal and Spain and more than 100 premises were searched in various EU countries. As a result, law enforcement seized 52 luxury cars, numerous documents, €400 000 in cash, IT material and one weapon.

The investigation began in 2015 when Spanish authorities were alerted to a criminal organisation specialised in VAT fraud and money laundering. The group carried out or simulated imports and purchases of electronic goods, both real and fake, which were sold online.

False invoices amounting to €250 million

The criminal organisation was composed mainly of Italian, Portuguese and Spanish nationals. The group had a network of more than 100 companies (most of them shell companies registered under the name of frontmen) across Belgium, Bulgaria, Cyprus, Germany, Hungary, Italy, Portugal, Romania, Spain and the USA. The network also owned a production centre to create false invoices to perform VAT fraud on electronic goods and on the import of luxury vehicles below invoice price. Investigations revealed that the group issued false invoices for a value of over €250 million in three years.

€140 million laundered in two years

Investigations also revealed that the money was layered among the large network of shell companies before being funnelled to Bulgarian or Hungarian bank accounts. In particular, the organisation moved more than €140 million in two years through two shell companies.

The group then used different methods to integrate its profits, such as investments in real estate and real businesses, or the purchase and sale of luxury vehicles. The **final destinations of the proceeds of crime were Italy, Spain and the USA.**

Europol supported the investigation by providing analytical and operational support.

18 Europol 2018, EU-wide VAT fraud organised crime group busted, accessible at https://www.europol.europa.eu/news-room/news/eu-wide-vat-fraud-organised-crime-group-busted

Money laundering

Money laundering is connected to virtually all criminal activities generating criminal proceeds in the EU. Money laundering allows OCGs to invest the illicit proceeds of their criminal activities in the legal and illicit economy. Almost all criminal groups need to launder profits generated from criminal activities. However, the way in which the money is laundered greatly varies on an OCG's level of expertise and the frequency and scale of money laundering activities. There are significant obstacles to identifying eventual beneficiaries of criminal proceeds as OCGs make effective use of anonymisation tools and process transactions quickly. A growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial service providers. This makes money laundering a technical challenge for law enforcement authorities to investigate.

Exploitation of the financial system, shell companies and professional facilitators

The following chapter highlights the ten most prominent modi operandi related to money laundering. All these money laundering techniques rely on the use of intermediaries who use multiple bank accounts, exploit the financial market and financial service products such as loans, insurance, bonds, and stock market trading.

Money launderers frequently set up and use shell companies that possess no significant assets and do not perform any significant operations, only serving the purpose of laundering funds. The shell companies used to send and receive money transfers are typically embedded in complex corporate structures which conceal the links to account beneficiaries. In many cases, these companies are registered in offshore jurisdictions.

Money laundering-as-a-service

In exchange for a commission of between 5% and 8%, these syndicates offer complex laundering techniques and carry out the laundering operations on behalf of other OCGs[19]. Professional enablers such as solicitors, accountants, company formation agents provide the skills and knowledge of financial procedures necessary to operate these schemes[20]. Although only a few groups are known to provide these services, they launder large amounts of money and have a considerable impact on the ability of other OCGs to disguise and invest criminal proceeds. These syndicates are a significant obstacle to tracing criminal assets. The criminal groups that possess the expertise or have access to skilled online money launderers are potentially of a bigger threat than those using traditional money laundering tools such as cash.

Money laundering techniques

Informal value transfer systems

Underground banking systems are financial networks operating outside of regulated financial systems to transfer money or value internationally and outside regulations of conventional banks. They can operate in multiple jurisdictions and allow hidden transactions between users facilitating the laundering of large amounts of money[21].

19 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

20 Europol 2016, Threat assessment on money laundering, syndicates and professional enablers.

21 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

Abuse of money services business

A number of criminal groups generating smaller but regular amounts of cash still use this alternative financial service as a suitable conduit to place and transfer their criminal funds.

Trade-based money laundering

Legal entities remain a key tool for money laundering activities and are instrumental in enabling trade-based schemes, which limit the movement of cash and provide a façade of legitimacy to money transfers[22].

Virtual assets solutions (cyptocurrencies)

Bitcoin and Ethereum are the two cryptocurrencies that form 80% of the market value. The growing popularity and adoption of cryptocurrencies have also led to their increasing use in money laundering schemes. Drug traffickers use bitcoin automated teller machines (ATMs) to convert criminal cash into virtual currency.

Money laundering networks use the €500 banknote to store and transport proceeds using cash couriers travelling to destinations outside of the EU. Larger amounts are easier to transport using high denomination banknotes. While the production of €500 banknotes has stopped, the banknote has not been fully withdrawn from circulation and continues to be legal tender.

> CASE EXAMPLE

Cryptocurrency laundering as-a-service: members of a criminal organisation arrested in Spain[23]

In a Spanish investigation supported by Europol, criminals carried out several money-laundering schemes involving the transfer from fiat currency to virtual assets to hide the illegal origin of the proceeds. Some of the identified modi operandi used crypto ATMs and smurfing, a criminal method used to split illicit proceeds into smaller sums and placing these small amounts into the financial system to avoid suspicious transaction reporting. During the investigation, it was identified that the criminal group was receiving transfers of criminal proceeds and collecting criminal cash and converting it into virtual assets. The estimated amount of laundered funds in the span of one year is €9 million. During the action day, one cannabis cultivation facility with 165 plants was dismantled, seven house searches were performed (including one money exchange office with two bitcoin ATMs), nine people were detained and 16 charged. Extensive amounts of evidence and assets were seized: four real estates, more than 200 bank accounts, 11 vehicles, €18 000 in cash, 30 mobile devices, jewellery, documents, identity cards used for structuring purposes.

22 Europol 2017, European Union Serious and Organised Crime Threat Assessment (EU SOCTA), accessible at https://www.europol.europa.eu/socta-report

23 Europol 2019, Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain, accessible at https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain

Abuse of banking services and digital banking services (open online accounts, mule accounts, cheap international transfers, offer of e-money services)

Alternative value transfer commodities

OCGs originating from North Africa, the Middle East and China are heavily involved in compensation schemes using gold or diamonds. The misuse of gold has been addressed in Regulation (EU) 2018/1672 on cash control, which expands the definition of cash to cover gold and imposes declarations upon those entering or leaving the EU with a value exceeding €10 000[24].

Interest free loans

Criminals offer interest-free cash loans in Europe to be repaid in a country of destination, usually in the Middle East or South America, within a set period of time. This allows an OCG to franchise their money laundering activities[25].

Real estate

Despite measures taken across the EU to decrease the laundering of money via real estate, investing criminal money into property development to launder money remains a threat.

A number of modi operandi are used, such as partial payment via cash, over- or under-valuing real estate and using non-transparent companies and trusts or third parties.

Gambling and hospitality

Cash-intensive businesses and gambling services continue to be used to launder criminal proceeds.

Cash movements

Using money mules to traffic cash has been the traditional modus operandi used in money laundering schemes. However, the COVID-19 pandemic has diminished, and in some places even almost eliminated, the use of cash as a payment medium as cash-intensive businesses in the hospitality sector have closed and many other businesses have switched to payment card transactions exclusively. It remains to be seen whether this will have a longer-term impact and reduce the attractiveness of cash to money launderers.

24 Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

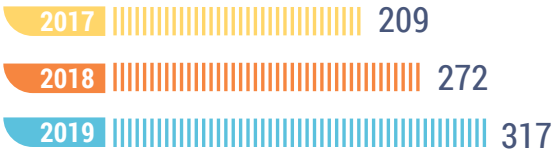
25 Europol information.

A European Response - The European Financial and Economic Crime Centre at Europol

Hundreds of international financial crime investigations are conducted in the EU every year. They often conclude with exceptional results in terms of arrests and dismantling of criminal groups. However, the EU still shows mediocre results when it comes to the recovery of criminal assets. Several obstacles seem to hinder this particular activity, including limited access to and sharing of financial and beneficial ownership information across borders. Today, more than 98% of criminal assets are still not recovered.

Not every investigation into organised crime in Europe is complemented by a corresponding financial investigation in the same targets.

The number of international investigations into economic and financial crimes supported by Europol
Source: Europol, Consolidated annual report 2018, 2019, 2020[26].



As highlighted throughout this report, economic and financial crime is highly profitable and a key enabler for all other types of serious and organised crime.

The COVID-19 pandemic and its anticipated economic fallout will likely exacerbate the threat from these types of crime and create new vulnerabilities. While restrictions to movements and commerce may have affected some criminal markets, it is also clear that criminals are determined to take advantage of the present situation and any opportunity that the recovery phase will bring.

It is essential to protect private and public finances during a time of crisis. This will require working together seamlessly to deprive criminal groups of their illicit gains. In order to provide an enhanced response to this threat, Europol has created the new European Financial and Economic Crime Centre (EFECC). This development follows Europol's Strategy 2020+ and has been welcomed by Member States and EU institutions.

EFECC will enhance Europol's operational support to EU Member States and EU bodies in the fields of financial and economic crime and promote the consistent use of financial investigations. The new centre will forge alliances with public and private entities to trace, seize and confiscate criminal assets in the EU and beyond.

EFECC will support European cross-border investigations in a wide range of domains, from money laundering, corruption and counterfeiting to various types of fraud, including those against national and European budgets. Initially, the centre will collect and analyse information on cases investigated by Member States in the framework of eight different analysis

26 Europol, Consolidated Annual Activity Reports (CAAR), accessible at https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-reports-caar

projects[27] on fraud against public and private finances, money laundering, asset recovery, corruption, product and currency counterfeiting.

EFECC will be at the centre of a systematic multilateral approach to combating fraud, money laundering and corruption, which will entail close involvement of public and private sector stakeholders.

EFECC will also be a privileged partner of the newly established European Public Prosecutor's Office to promote and support financial investigations into crimes that affect the financial interests of the EU.

The new centre is the common platform to enable cooperation across a broad range of diverse stakeholders. EFECC will enhance information sharing and provide state-of-the-art operational, analytical and technical support.

For law enforcement authorities in the Member States and Europol's partners, the creation of EFECC constitutes a unique opportunity to re-invest resources in the fight against economic and financial crimes and adopt common strategies to curb illicit profits.

The creation and launch of EFECC comes at the right time as the economic impact of the COVID-19 pandemic crisis deepens vulnerabilities of our financial system and tests the resilience of our economic and social infrastructure.

27 AP Smoke, AP Apate, AP MTIC, AP SUSTRANS, AP Asset Recovery, AP Sports Corruption, AP Copy, AP Soya.

ENTERPRISING CRIMINALS – EUROPE'S FIGHT AGAINST THE GLOBAL NETWORKS OF FINANCIAL AND ECONOMIC CRIME

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

www.europol.europa.eu