ctif cfi

BELGIAN FINANCIAL PROCESSING UNIT CTIF-CFI

27th ANNUAL REPORT 2020

TABLE OF CONTENTS

I. PREFACE BY THE DIRECTOR AND THE FEDERAL PUBLIC PROSECUTOR

The publication of CTIF-CFI's 27th annual report 2020 is an opportunity to thank everyone who, despite the health crisis, has made it possible to maintain the preventive AML/CFT system as well as all of the staff at CTIF-CFI for the work done in 2020.

It is also the opportunity to, on the one hand, share this preface with Mr Frédéric Van Leeuw, Federal Public Prosecutor, highlighting CTIF-CFI's judiciary goal and, on the other hand, to thank the Prosecutors across the public prosecution service for their continuous interaction with CTIF-CFI.

CTIF-CFI received a large number of disclosures of suspicions and notifications (a total number of 31.605 disclosures and notifications in 2020) and a large number of files were disseminated to the judicial authorities (1.228 files involving an amount of EUR 1.885 million).

The pandemic and the health crisis demonstrate that fraudsters and criminals adapt very quickly to changing economic circumstances or the emergence of extreme circumstances under the motto "never waste a good crisis". This ties in with the words of Henri-Frédéric Amiel who wrote: "a being that does not adapt to its environment suffers and will perish"[1].

At the height of the health crisis we faced an increase in fraud mechanisms. At the start of April CTIF-CFI pointed to the short-term consequences of the health crisis, mainly fraud involving personal protective equipment and counterfeit medicines, as well as unduly paid unemployment benefits or COVID allowances.

CTIF-CFI subsequently highlighted the long-term consequences of the health crisis. The possibility that parts of our economy in difficulty would turn to criminal individuals cannot be excluded. Many hospitality businesses, textile companies in difficulty, which cannot get bank loans could potentially see no other option but to turn to criminal individuals for money or could become easy targets and take part in money laundering.

CTIF-CFI's annual report also provides an opportunity to present the latest evolutions on the prevention of money laundering and terrorist financing. This report describes the different advanced fraud and money laundering mechanisms identified in 2020.

Fraud techniques evolve constantly (investment fraud, fraudulent transfers) as well as the financial channels used (money mules, payment service providers -PSPs- and crypto assets) and are becoming increasingly advanced.

Serious fiscal fraud, social fraud and organised crime increasingly feature as interrelated issues. Well-organised (inter)national networks are revealed with links to organised crime. These networks are used for laundering the proceeds of other crimes such as trafficking in human beings and trafficking in narcotic drugs.

In 2020, CTIF-CFI worked in full synergy with the Federal Public Prosecutor's Office on the issue of large-scale social fraud and Brazilian and Portuguese networks.

Over the past several years CTIF-CFI has found that Brazilian or Portuguese nationals set up or take over companies, usually in the construction industry and industrial cleaning industry. CTIF-CFI recently found that other sectors were also involved, in particular goods transport, and that other nationalities were also involved.

Based on the files disseminated to the judicial authorities in 2020, CTIF-CFI has found that Trade-Based Money Laundering is increasingly used. Several trends were identified, which were also confirmed in the recent joint FATF-Egmont Group Report on Trade-Based Money Laundering.

[1] Henri-Frédéric Amiel, *Journal Intime*, April 1877-1879, Part XI, page 676, *Editions l'Âge d'Homme* 1993.

Even though CTIF-CFI was established as a result of a preventive law, it does contribute to the punishment of money laundering and terrorist financing. Over the last ten years, 533 judgments and rulings were issued by courts and tribunals in files disseminated by CTIF-CFI. Fines and confiscations of more than EUR 360 million were imposed.

It is, however, important to remember that CTIF-CFI's turnaround time is not the same as for the judicial authorities. CTIF-CFI disseminates a file to the Public Prosecutor's Office when CTIF-CFI finds serious indications of money laundering or terrorist financing, the judicial authorities need to provide proof that the financial transactions are linked to money laundering or terrorist financing.

Finally, the impact of the preventive measures should not only be measured on the basis of judicial decisions, judgments or confiscated amounts. CTIF-CFI sent 1.154 operational or strategic information notes to the Public Prosecutor's Offices in labour matters [*auditorats du travail*], the Federal Public Service Economy, the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD].

We hope you enjoy reading the report.

Philippe de KOSTER
Advocate-General – Public Prosecutor's Office Cassation
Director of CTIF-CFI

Frédéric VAN LEEUW
Federal Public Prosecutor

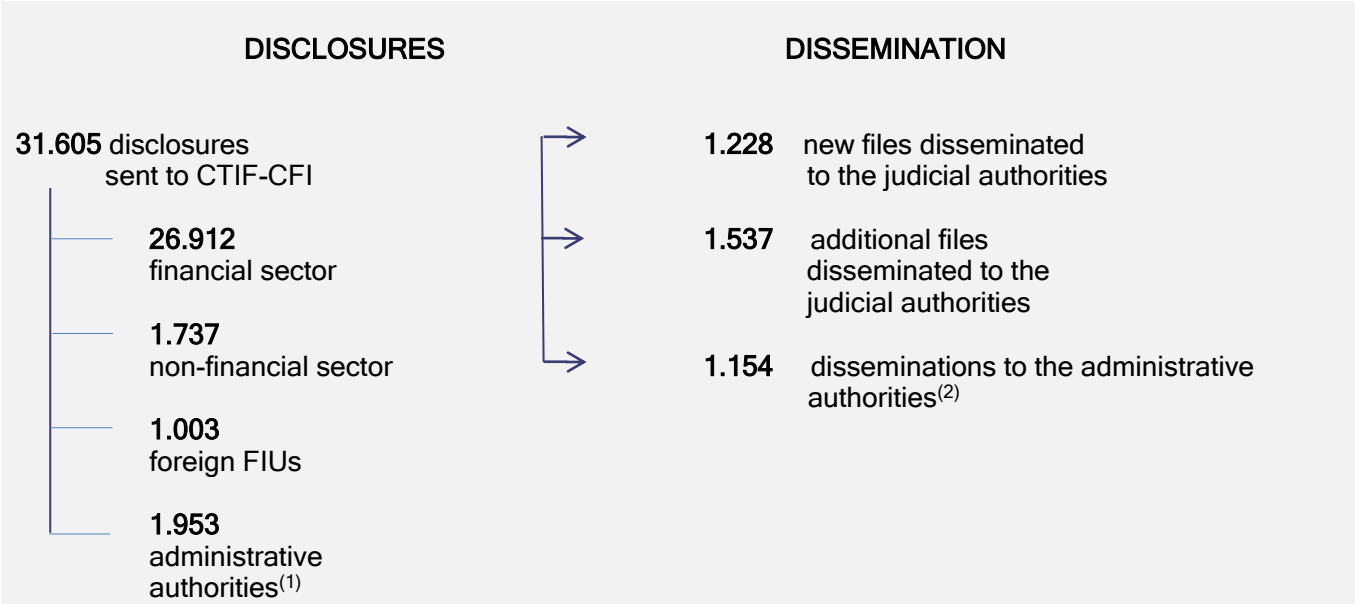
II. COMPOSITION OF CTIF-CFI[2]

Director:	Mr	Philippe de KOSTER
Vice-President:	Mr	Michel J. DE SAMBLANX[3]
Deputy Director	Mr	Boudewijn VERHELST
Members:	Mr	Johan DENOLF
	Mr	Fons BORGINON
	Ms	Chantal DE CAT
Secretary-General:	Mr	Kris MESKENS

[2] Situation on 31 December 2020
[3] Acting Vice-President from 1 September 2017

III. KEY FIGURES 2020

CTIF-CFI's mission is to receive disclosures of suspicious transactions from obliged entities mentioned in the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash[4], from foreign FIUs as part of international cooperation and from other services of the State, as referred to in the law. CTIF-CFI uses its designated powers to analyse and enhance this information. In case of serious indications of money laundering, terrorist financing, or proliferation financing, CTIF-CFI disseminates the result of its analysis to the judicial authorities.



(1) Disclosures of cross-border transportation of currency, fiscal regularisation certificates, disclosures by officials of administrative services of the State (including the State Security Department [VSSE], the General Intelligence and Security Service of the Armed Forces [SGRS-ADIV] and the Coordinating Unit for Threat Analysis [OCAM-OCAD]), by the Public Prosecutor's Office, as part of an inquiry or preliminary inquiry related to terrorism and terrorist financing and the supervisory authorities, in accordance with Article 79 of the AML/CFT Law.

(2) Information communicated to Public Prosecutor's Offices in labour matters [*auditorats du travail*], the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Federal Public Service Economy, the European Anti-Fraud Office OLAF, the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD], in accordance with Article 83 of the AML/CFT Law and the supervisory authorities of obliged entities in accordance with Article 121.

CTIF-CFI is legally required to exchange and report certain information from these files to other national authorities: to the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance when the notification to the Public Prosecutor contains information regarding laundering the proceeds of offences that may have repercussions with respect to serious fiscal fraud, whether organised or not, to the Customs and Excise Administration when this notification contains information regarding laundering the proceeds of offences for which the Customs and Excise Administration conducts criminal proceedings; to the supervisory authorities of obliged entities and the Federal Public Service Economy when this notification contains information regarding laundering the proceeds of an offence for which these authorities have

[4] Hereinafter referred to as the Law of 18 September 2017. Belgian Official Gazette of 6 October 2017 - Chamber of Representatives (www.lachambre.be) Documents: 54-2566.

investigative powers; to the Social Intelligence and Investigation Service [SIRS-SIOD] when the notification to the Public Prosecutor contains information regarding laundering the proceeds of offences that may have repercussions with respect to social fraud; and to the Public Prosecutor in labour matters [*auditeur du travail*] when the notification to the Public Prosecutor contains information regarding laundering the proceeds of smuggling of human beings (including trafficking in illegal workers, now included in the main concept of smuggling of human beings) or trafficking in human beings.

CTIF-CFI can also inform the Central Office for Seizure and Confiscation [OCSC-COIV] when assets of significant value, of any nature, are available for potential judicial seizure.

To tackle the security threat CTIF-CFI also cooperates closely with the civil and military intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD]. CTIF-CFI can contextualise requests for assistance/information it sends to these three authorities. As part of mutual cooperation (Article 83 § 2, 4° of the AML/CFT Law), CTIF-CFI can also send useful information to the intelligence services and to OCAM-OCAD.

- **31.605** disclosures sent to CTIF-CFI
- **1.228** new files disseminated to the judicial authorities in 2020 and information from **2.765** disclosures was used in files disseminated to the Public Prosecutor's Offices and the Federal Public Prosecutor's Office for a total amount of **€1.885,31 million.**
- **1.154** information notes (or copies of investigation reports) were also sent to the Public Prosecutor's Offices in labour matters [*auditorats de travail*], the Federal Public Service Economy, the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordination Unit for Threat Analysis [OCAM-OCAD], in accordance with Article 83 of the AML/CFT Law and the supervisory authorities of obliged entities in accordance with Article 121 of the AML/CFT Law.

Part IV contains an overview of money laundering and terrorist financing trends in 2020. A detailed overview of the statistics of 2020 is included in part V.

IV. MONEY LAUNDERING AND TERRORIST FINANCING TRENDS

1. Money laundering trends

1.1. Evolution of criminal threats

1.1.1. The crisis related to the COVID-19 pandemic and the consequences with regard to money laundering

Trends identified

Crises in the past have shown that criminals quickly adapt to changing circumstances, under the motto "never waste a good crisis". The COVID-19 crisis is no exception, as highlighted in reports published by Europol[5], Interpol[6] and the FATF[7].

In Belgium, CTIF-CFI's experience confirms that criminals can adapt. The official economy slowed down due to the health crisis, yet the underground economy continued to flourish. The economic crisis and the ensuing social changes give flexible criminal organisations the possibility of exploiting the extreme circumstances to adapt their existing modi operandi or to develop new criminal activities. Several trends were identified in this period, highlighting the importance of following the financial trail when fighting crime, particularly in times of crisis.

Evolution of criminal threats

- Fraud

Fraud has been one of the main predicate offences in CTIF-CFI's files for a number of years now. From the start of the health crisis several files showed that fraudsters exploited the increased global demand for medical supplies to commit fraud with the sale of masks, disinfecting gel, ventilators or testing kits. The urgent nature for individuals in the private and the public sectors to purchase this material resulted in increased vulnerability, which fraudsters exploited. The modus operandi of fraudsters was generally simple, the ordered medical supplies were not (all) delivered. The money was laundered through cash withdrawals or national and international transfers between accounts.

Conventional forms of cybercrime were also identified. Mass fraud, such as phishing, advance fee fraud or emotional fraud, was on the rise again. In several fraud schemes the COVID-19 crisis was used as an excuse. In phishing mails cybercriminals posing as a financial institution asked to update the security data due to the exceptional circumstances. The measures taken to reduce the spread of COVID-19 have further increased the social isolation of some vulnerable groups, extending the "pool" of potential fraud victims. Even though this is not new, the COVID-19 crisis has intensified the problem because young people in financial difficulties were more inclined to operate as money mules, without necessarily realising they were taking part in criminal activities[8].

CTIF-CFI also dealt with fraud files in which fraudsters clearly misused the compensation and support measures provided by the federal and the regional governments to support people and companies economically affected by the COVID-19 pandemic. This related to temporary unemployment due to the COVID-19 pandemic, support for companies for the (re)payment of debts, aid for companies and self-employed people. These files revealed that fraudsters used fake documents such as forged bank statements to request aid for companies to which they were not linked in any way.

---

[5] https://www.europol.europa.eu/newsroom/news/how-criminals-profit-COVID-19-pandemic
[6] https://www.interpol.int/How-we-work/COVID-19
[7] https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-COVID-19.html; Update-COVID-19-Related Money Laundering and Terrorist Financing Risks.pdf (fatf-gafi.org)
[8] To make young people aware of the issue of money mules and to warn them of the dangers this entails Febelfin, the Belgian federation of the financial sector, started a campaign on social media. https://www.febelfin.be/fr/communique-de-presse/gagner-de-largent-rapidement-est-une-illusion-ne-pretez-jamais-votre-compte

Typological case 1: Cash withdrawals related to unduly obtained unemployment benefits or aid due to COVID-19

CTIF-CFI received various disclosures regarding accounts opened by natural persons and legal persons on which suspicious transactions had been taking place since May 2020: very substantial unemployment benefits were received, which had not been the case before, and transfers referring to aid due to the COVID-19 pandemic. Over the period of few months this totalled to an amount in excess of EUR 1 million. The money was subsequently primarily withdrawn in cash.

At the same time, CTIF-CFI received a request from the Federal Public Prosecutor's Office on the basis of Article 84 of the AML/CFT Law, regarding an ongoing investigation into criminal organisation involving several people. These people were suspected of having set up false companies with fake identities to request benefits for temporary unemployment and receive aid. These facts related to the accounts mentioned in the various disclosures received by CTIF-CFI.

Based on all of this information CTIF-CFI concluded there were serious indications that unemployment benefits and other related payments in whole or in part ensued from the facts in the investigation. By making this connection CTIF-CFI was able to quickly disseminate the financial information to the Federal Public Prosecutor's Office.

- Social fraud and serious fiscal fraud

For over ten years CTIF-CFI has found that companies are being used to exploit illegal workers with regard to social fraud and serious fiscal fraud. Due to the economic crisis as a result of COVID-19 the activities in several sectors slowed down or even came to a standstill. Companies in sectors traditionally considered to be susceptible to social fraud and/or serious fiscal fraud (construction industry, industrial cleaning, goods transport) have continued to develop illegal activities.

CTIF-CFI found that companies, managed by front men, use groups of undeclared workers. Although the origins of this type of fraud go back to the financial crisis of 2008, the COVID-19 crisis contributed to an increased risk of the use of (too) cheaply employed subcontractors. The rise in unemployment also led to an increase in the range of workers willing to carry out undeclared work. In this regard networks attracted by illegal work in vulnerable sectors[9] still form a substantial money laundering risk. In these

[9] In 2020 CTIF-CFI, which coordinates the activities of the Board of Partners [*Assemblée des partenaires*] of the Board for coordinating the fight against money laundering [*Collège de coordination de la lutte contre le blanchiment*], actively took part in updating the national risk assessment 2017, for determining the money

files the companies involved receive aid because of the crisis even though numerous payments referring to invoices are still carried out on their accounts.

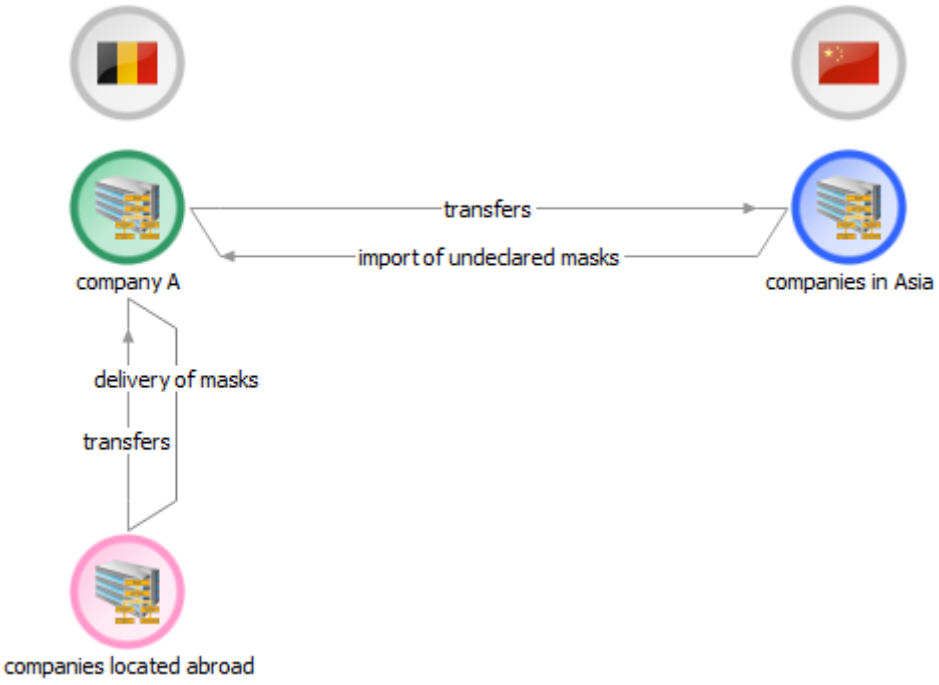
Apart from links with social fraud and serious fiscal fraud by networks there are other files involving fiscal fraud (VAT carousel fraud) related to illegal commercial activities with medical supplies.

Typological case 2: Laundering the proceeds of serious fiscal fraud related to the trade in respiratory masks

The accounts of Belgian textile company A showed a sharp rise in turnover in 2019. Numerous international transactions from foreign companies took place on these accounts, this money was then transferred to Asia.

From 2020 onwards the turnover on these accounts increased greatly. The main financial transactions -amounting to several EUR million- were linked to the trade in masks, an activity that the company started early 2020. The transfers referred to orders of respiratory masks.

Information from the Federal Public Service Finance showed that a tax investigation into VAT carousel fraud had already been launched prior to 2020. As to the transactions in 2020, the turnover declared by the company in the first months of 2020 did not match the turnover on the accounts. Information from the customs authorities also revealed that the company did not import any respiratory masks in 2020.



- Trafficking in narcotic drugs

According to the United Nations border closures and other restrictions to manage the COVID-19 pandemic created a shortage on the drug market, resulting in a price rise and a reduction in purity of substances. Drug traffickers focussed on maritime routes, in particular to transport cocaine from South America to Europe. The online trade via the darknet, which favours anonymity, and shipping by post have nevertheless increased[10].

The crisis provides both challenges and chances for criminal organisations trafficking narcotics with respect to money laundering. Due to the restrictions there were fewer possibilities of injecting cash in companies that traditionally use of lot of cash and are used as a cover. Although there are now large

laundering threats as well as the money laundering vulnerabilities. The department strategic analysis was one of the partners involved in the national threat assessment and in determining the sectors with a substantial threat.

[10] UNODC, World Drug Report 2020.

amounts that are temporarily kept out of the financial system CTIF-CFI found in several files related to trafficking in narcotic drugs that the intensive use of cash makes the hospitality industry and retail trade vulnerable to investments and takeovers of criminal origin. This is certainly true in times of economic crisis when many companies are in danger of disappearing and are vulnerable to criminal interference.

Interference by criminals may occur through a direct takeover of shares or an investment, sometimes in combination with appointing a new manager. Often illegal income is combined with the turnover of a company that primarily works with cash. Large cash deposits by companies with a limited actual turnover or an abnormal repayment of bridging loans given to companies in difficulties are indications of potential criminal interference. Unexplained transfers to hospitality businesses or retail establishments by order of companies in completely different sectors, such as the construction industry, point to potential laundering by using the offsetting mechanism.

Typological case 3: Injection of cash from trafficking in narcotics on account of a restaurant

Apart from state aid related to the COVID crisis, an amount of 130.000 EUR was also deposited into the bank account of a restaurant, at a time when the turnover should have been much lower. Transfers with reference to the car trade also took place on the account.

Analysis showed that the manager was involved in trafficking in narcotics, he deposited part of these proceeds on the restaurant's account. He also purchased vehicles in cash (in Germany), which he resold and the payments for these transactions were made to the corporate account to conceal the illegal origin of the cash.

Action taken

Publication of COVID-19 warnings by CTIF-CFI

To warn obliged entities and help them assess the risk as best as possible CTIF-CFI published warnings illustrating trends, typologies, examples and concrete indicators. The information was based on CTIF-CFI's experience, open sources and studies by domestic and international partners and organisations.

On 6 April, CTIF-CFI published a first warning[11] on its website alerting obliged entities to the immediate consequences of the COVID-19 crisis. The focus was on the short-term consequences of the health crisis, mainly linked to fraud involving the trade in medical supplies. CTIF-CFI also asked obliged entities to highlight potential links with the COVID crisis by mentioning the term "COVID-19" in online disclosures.

On 27 April, CTIF-CFI published a second warning[12] to make obliged entities aware of the possible medium-term consequences of the changed economic situation with regard to money laundering. CTIF-CFI mentioned the possible evolution of several offences (cybercrime, trafficking in narcotics, corruption, social fraud and serious fiscal fraud) in order to identify related suspicious financial transactions.

After a few months the economic and social consequences of the crisis became clearer and a number of money laundering trends stood out. On 21 August, CTIF-CFI published a third warning[13] with an overview of these trends, aimed at assessing the previous warnings on the basis of recent files, information from partner authorities and open sources.

Domestic and international cooperation

Cooperation with domestic and international partner authorities remains one of the cornerstones of CTIF-CFI's policy for combating money laundering and terrorist financing.

To be able to play an efficient role in this time of crisis, information from partners is crucial to CTIF-CFI. Conversely, the financial information that CTIF-CFI has at its disposal received from various types of obliged entities undoubtedly also adds value for partners combating crime and derived money

[11] https://www.ctif-cfi.be/website/images/FR/covid19fr.pdf
[12] https://www.ctif-cfi.be/website/images/FR/covid19fr2.pdf
[13] https://www.ctif-cfi.be/website/images/FR/avertissementcovidaout2020.pdf

laundering such as the Public Prosecutor's Office, the police, the intelligence services, customs and the Federal Public Service Economy. Information is also exchanged with the supervisory authorities of the financial sector, the National Bank of Belgium and the Financial Services and Markets Authority enabling ML/TF risks to be assessed by obliged entities in these exceptional circumstances.

Internationally CTIF-CFI cooperates with its foreign counterparts on a bilateral basis or through formal networks such as the Egmont Group based on prompt information exchange. This make it possible to exchange relevant information and is clearly an added value in an environment where the international dimension is one of the features of the dynamics of money laundering. The way the crisis is handled may differ among countries but recent close cooperation with foreign counterparts shows that the money laundering and terrorist financing challenges are similar.

1.1.2. Trafficking in narcotic drugs

Trends identified

More than a year after the start of the COVID-19 crisis it has become clear that the exceptional health situation has most certainly not led to a decrease in crime forms analysed by CTIF-CFI. Criminal activities only needed to be suspended for short periods of time and the economic crisis ensuing from the health crisis often even offers criminal organisations additional money laundering possibilities.

This is certainly true for trafficking in narcotic drugs. Research by Sciensano shows that during lockdowns less party drugs such as ecstasy were used because hospitality venues were closed, but that this decline was probably offset by a rise in cannabis use. Moreover, recent investigations by the police in Belgium and in the Netherlands point to the abundant production of synthetic drugs. In addition to ecstasy and speed (amphetamines), labs for methamphetamine or "crystal meth" were dismantled for the first time. The number of cannabis plantations discovered in recent months does not point to a drop in production either, a hypothesis that was confirmed by the *European Monitoring Centre for Drugs and Drug Addiction* (EMCDDA)[14].

The situation with regard to trafficking in narcotic drugs is even more alarming. Despite the lockdowns there was a record amount of cocaine seized in Belgium in 2020. In the port of Antwerp alone in excess of 65 tonnes were seized, which is another increase compared to the record amount of 62 tonnes in 2019. As part of a large-scale investigation into a criminal organisation smuggling cocaine to Belgium a total amount of nearly 15 tonnes was confiscated[15]. The total street value of these drugs amounts to nearly EUR 1 billion. Such astronomical income gives criminal organisations unseen power and can completely disrupt a society's social and political structures. In March 2021, the largest investigation ever into organised crime and drug trafficking[16] gained momentum. By accessing an encrypted communication network the Public Prosecutor's Office and the police gained a clear insight into the structure and the operations of the international criminal organisations coordinating the import of cocaine via the port of Antwerp. Again this revealed the links between the legitimate world and underworld, partly due to the enormous financial interests of the cocaine trade.

Recent investigations clearly show that CTIF-CFI has an important role to play in investigating the financial aspects of drug trafficking. For years the FIU has been giving high priority to laundering the proceeds of drug trafficking, which seems entirely justified.

Drug trafficking is one of the most important predicate money laundering offences, in terms of the number of files as well as the amounts involved. The files analysed in 2020 mainly relate to cocaine trafficking and the trafficking in and production of cannabis and synthetic drugs. Several files reveal financial transactions of the "intermediate level" of this trafficking: natural persons with credit transactions on their accounts between EUR 30.000 and 100.000 per year, largely in cash and which cannot be (fully) explained by a legitimate professional activity. Information from the police shows that those involved are actively linked to the world of drugs. The financial institution is unable to get more information on the suspicious transactions, or the explanation provided is completely implausible. Analysis of the accounts shows that those involved often get petrol, in Belgium as well as abroad, which could point to a possible role as a courier as part of a network. When the account reveals inexplicable

[14] EMCDDA: European Drug Markets – Impact of Covid-19
https://www.emcdda.europa.eu/system/files/publications/13097/EU-Drug-Markets_Covid19-impact_final.pdf
[15] Operation 'Costa'
[16] Operation 'Limit'

cash deposits as well as the payment of a salary, professions such as port staff or (international) freight drivers are often involved.

Another substantial part of the files relates to the use of companies for laundering the proceeds of drug trafficking. The use of cash-intensive companies to mix illegal cash with legitimate income is frequently used as a money laundering technique. The activities of the companies used are varied, but often feature wholesale and retail trade in food, the hospitality industry and car trade. The suspicious transactions are mainly cash deposits or transfers between companies, with amounts between EUR 300.000 to 800.000 per year.

Lastly, the use of professional money laundering networks (cf. infra section 1.2.1) was identified in several files linked to drug trafficking as well as several other types of predicate offences. Organisations specialise in laundering the proceeds of various criminal activities and use the offsetting technique to channel cash to illegal sectors in need of cash, such as illegal labour.

Although there are a substantial number of files related to laundering the proceeds of drug trafficking, these amount are nowhere near the estimated size of the drug trade in Belgium based on confiscations. A possible explanation for this discrepancy, as mentioned by specialised police services, is that the leaders of criminal organisations importing cocaine would be located abroad. The amounts detected in Belgium would originate from the logistical organisation of the drug trafficking and would not be the ultimate profits circulating in Belgium.

CTIF-CFI's financial information confirms this hypothesis to some extent, given that even in the files solely related to the logistical aspects of drug trafficking many links with foreign countries are identified. It is clear that laundering the proceeds of drug trafficking is organised on an international scale, even if the import or production takes place in Belgium. The separate financial and commercial flows in international drug trafficking is an additional challenge for analytical teams. The financial flows mainly involve our neighbouring countries, in particular the Netherlands, as well as Turkey and Dubai (United Arab Emirates).

Another possible explanation for the fact that the detected amounts linked to laundered proceeds of drug trafficking are tens and not hundreds of millions, as is to be expected based on the quantities seized, is the involvement of professional money laundering networks. Substantial amounts are involved in these files and are the proceeds of various predicate offences. Possibly part of the proceeds of drug trafficking is detected but no longer identified as such. It is plausible that part of the funds are the proceeds of drug trafficking and are moved by professional money laundering networks using the offsetting technique to activities linked to social fraud or other criminal activities. In a number of files this link between various criminal worlds -facilitated by professional money launderers- was also actually identified.

Typological case 4: Offsetting scheme and drug trafficking

A pattern was identified involving a number of related companies: money from the construction, cleaning and transport industries were transferred to companies whose activities were not clear, followed by large purchases of gold. The different activities of these companies raise questions as to the economic reality of the financial transactions. This is a typical feature of the offsetting technique.

Several of these companies were unfavourably known to CTIF-CFI. They feature in files disseminated to the judicial authorities or are known to the police. The transactions are presumably part of an offsetting scheme, aimed at getting cash. The gold purchased is probably exchanged for cash originating from drug trafficking.

During a number of recent house searches the police found drugs as well as large quantities of gold. The cash was then used in the construction, cleaning and transport industries where this cash is used to pay (illegal) workers. The trade in gold is an additional step in the money laundering process to make it more difficult to follow the transaction chain.

Action taken

The preventive anti-money laundering system was initially aimed specifically at tackling drug trafficking. More than thirty years on, financial investigation is more relevant than ever. Legal structures being

infiltrated through money laundering remains one of the main threats from criminal organisations involved in drug trafficking, as became clear from recent examples.

To be able to contextualise financial data from disclosures good cooperation between CTIF-CFI, the Public Prosecutor's Office and police services specialising in drug issues is crucial. A number of multidisciplinary partnerships were further strengthened in 2020. CTIF-CFI was part of the Multidisciplinary Ad Hoc Consultation [*Multidisciplinair Ad Hoc Overleg – MAHO*] as part of the so-called Stream Plan [*Stroomplan*] in Antwerp and CTIF-CFI cooperated with the Public Prosecutor's Office and the Federal Judicial Police of Brussels on the so-called *Global Drug plan*.

Apart from national synergies, strengthening cooperation and exchange with Europol is an important challenge given the international nature of trafficking in narcotics, as well as the money laundering mechanisms used to launder proceeds of this trafficking. CTIF-CFI has already been in touch on specific issues, and the transposition of Directive (EU) 2019/1153 on the cooperation between FIUs and Europol[17] should boost this cooperation in the coming months and years.

1.1.3. Fraud

Trends identified

The number of disclosures related to different types of fraud has been very high the last ten years. The financial sector directly faces a great increase of this phenomenon[18]. Fraud is by far the main predicate offence in terms of the number of files disseminated to the judicial authorities. Other competent authorities involved in combating fraud such as the police, the Federal Public Service Economy, the Financial Services and Markets Authority and the Public Prosecutor's Office identify the same trend.

This issue can partly be explained by the expansion of the internet and the increased digitalisation of society. These elements have led to an enormous increase in different types of "mass fraud" identified in numerous files. Regardless of the specific type of mass fraud, a huge target group of potential victims is always approached, resulting in vast profits for criminals, which are difficult to apprehend with regard to law enforcement.

Criminal organisations committing fraud are very flexible. As the public becomes aware of the risks of mass fraud, fraudsters develop a different tactic and approach their victims in a more targeted way. This approach, called "spear phishing" or "whaling", large victims ("whales") are selected after careful examination and their weak points are exploited using social engineering in order to commit fraud. These attacks are generally aimed at companies or organisations but sometimes also natural persons. Criminals usually obtain access to e-mails through hacking and collect information on their victims through (publicly available) social media. CEO fraud or Business Email Compromise (BEC) is also part of this type of fraud. Criminals need to go through more effort but the potential profit is also much higher than with mass fraud. Investment fraud, examined by the Financial Services and Markets Authority and fraud with business directories combated by the Federal Public Service Economy are other examples of more targeted types of fraud.

Investment fraud: reactive and complex networks

Financial authorities of numerous countries remain concerned over the increasing number of online trading platforms operating on the Belgian market[19]. This fraud is perpetrated using online ads for fake investments. After the victims have clicked the ad and have given their contact details, the victims are usually swiftly called by fraudsters presenting a concrete investment proposal (in shares, alternative investment products, virtual currencies, etc.). The system uses specialised call centres in Eastern Europe, in Belarus, in Cyprus, in Israel. Operators are trained to convince victims to invest increasingly larger amounts.

Networks remain flexible with this type of fraud. Analysis of the files shows that these dynamic and international networks are looking for new possibilities and multiple types of fraud are used: fraud with fraudulent transfers, CEO fraud, fraud with unregulated trading sites, offers to invest in diamonds,

[17] Article 12 of the Directive.
[18] https://www.febelfin.be/fr/communique-de-presse/phishing-en-2020-les-chiffres
[19] https://www.fsma.be/en/warnings/fraudulent-online-trading-platforms-fsma-updates-its-list-suspicious-sites-3

platforms for trading cryptocurrencies. The files show that these types of fraud are often committed by the same networks.

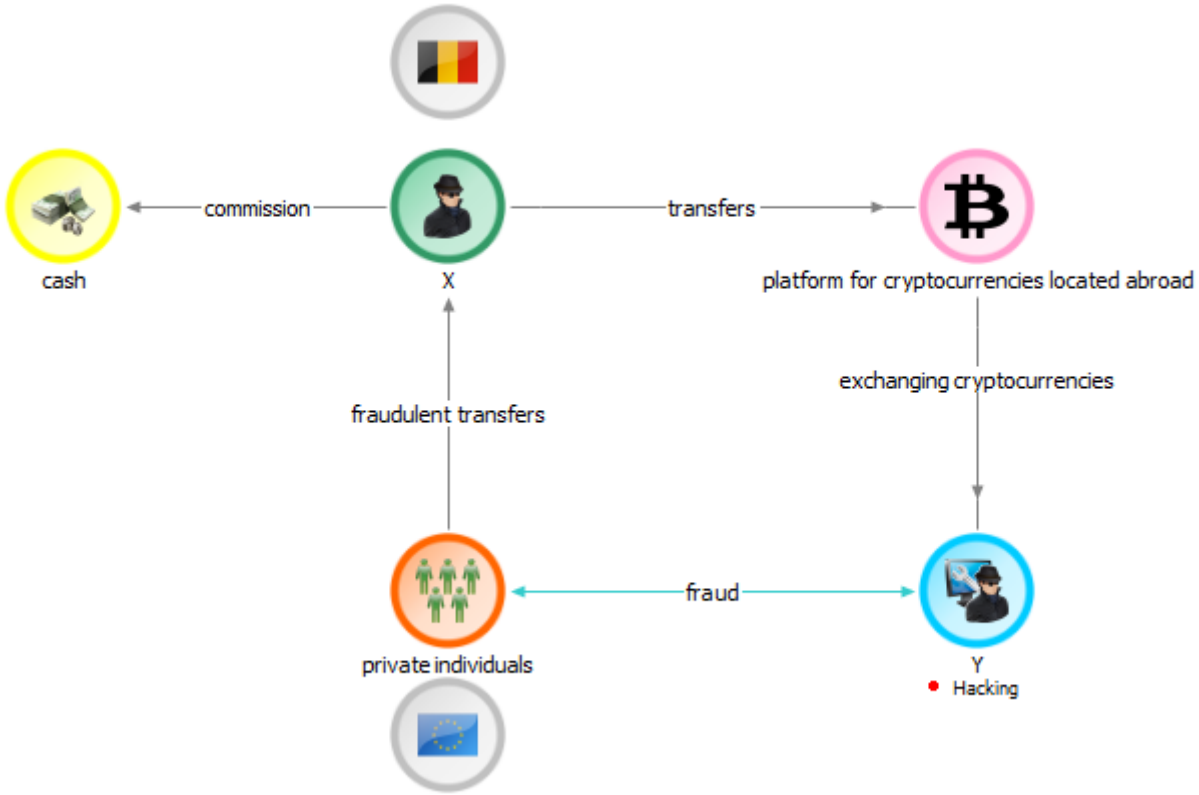
This involves highly organised international crime with specialised providers and complex money laundering schemes. The system is largely based on the role of money mules. These criminals have a large network of bank accounts belonging to mules and they rely on them to facilitate laundering the proceeds of this fraud. After having used several banking systems in Europe (in particular in Poland, the Baltics and Portugal) the fraudsters turn to other countries as the fraud is discovered. Several files show that the money is subsequently distributed to Asia and is then returned to the fraudsters as part of a money laundering scheme using the offsetting technique. In other files the money laundering takes place by purchasing cryptocurrencies.

Typological case 5: Money mule and money laundering with cryptocurrencies

The account of the Belgian national X received transfers from several private individuals with an account abroad. The collected funds were mainly transferred to a platform for exchanging cryptocurrencies located abroad. X stated that he had registered with this platform after being approached by Y to be the intermediary to buy cryptocurrencies in exchange for a commission.

Although X's claims were consistent with the financial transactions on his account a foreign bank suspected that the money on the accounts of some of its customers that was transferred to X was linked to laundering the proceeds of fraud.

X is said to have acted as a money mule: in exchange for a commission X received money from foreign accounts on his account. He transferred this money to his account with a platform to exchange this into cryptocurrencies and subsequently sent these cryptocurrencies to the criminals who initiated this fraud.



Laundering related to fraud through accounts of shell companies

Several files related to fraud show that these facts take place at the end of the process, when shell companies whose accounts were first used to channel funds related to social fraud were subsequently used to launder the proceeds of fraud. Transactions linked to fraud with fraudulent transfers (via

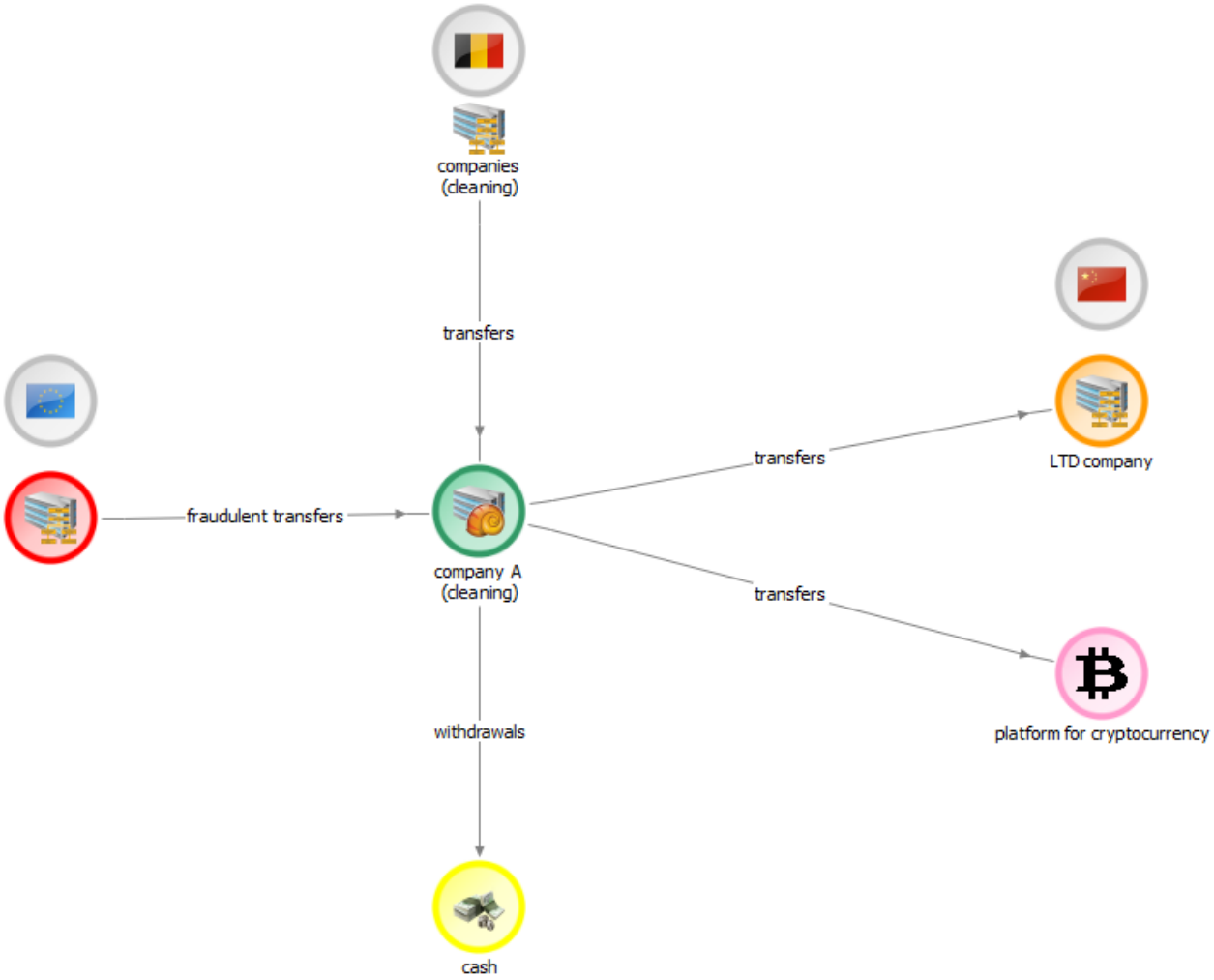
hacking) were carried out on these companies' accounts. The money was subsequently transferred abroad.

Typological case 6: Dual usage of a channelling account for money laundering purposes related to social fraud followed by fraud

A recently established cleaning company, company A, held accounts with several banks. The company's accounts were used to receive money from different counterparties in the same industry as soon as these accounts were opened. The money was subsequently withdrawn in cash.

A few months later one of the company's accounts received a transfer amounting to several million EUR from an account abroad. This was a fraudulent transfer that took place through hacking. Part of the money was transferred to a platform for cryptocurrencies and to an account in Asia.

The bank was able to block a large part of the money. Due to the serious and urgent nature of the case CTIF-CFI issued a freezing order for company A's account. As a result of this freezing order no debit transactions could take place on company A's account for five workdays. In the meantime the file was disseminated to the judicial authorities as a matter of urgency. In the light of these elements it became clear that company A was presumably solely set up to commit social fraud and subsequently, at the end of the company's life (its address had been officially deleted), to commit fraud.



Action taken

Consulting the judicial authorities on money mules

Consistent awareness-raising of the public remains the best preventive measure, for victims as well as for money mules. With regard to law enforcement, prosecuting criminal organisations committing mass fraud and other types of fraud is not easy. The money is withdrawn in cash from the money mules' accounts (and often subsequently sent abroad through money remittance using channelling accounts) or directly transferred abroad using bank transfers or payment service providers.

The Public Prosecutor's Office being the main recipient of information and CTIF-CFI's limited role in terms of raising awareness of the public, CTIF-CFI can add value in files disseminated to the authorities in which the perpetrator of the fraud and/or the money mule have not yet been identified as such by the authorities (no complaint by the victim) and are still active in Belgium.

To combat these different types of fraud more effectively the Public Prosecutor's Office of Brussel set up a "Fraud Team". Cooperation with CTIF-CFI was initiated, enabling consultation on money mules and fostering a more active approach of the issue.

Phishing has become an important social problem. CTIF-CFI is also convinced that the only way to counter this problem is to apply a multidisciplinary approach. Apart from bilateral cooperation CTIF-CFI also takes part in the activities of a working group set up on the initiative of the Board of Prosecutors-General [*Collège des procureurs généraux*], that unites the banking industry, police, Public Prosecution, public authorities and the judiciary. These considerations should shortly lead to a circular letter determining the strategy to counter phishing as effectively as possible, from detection to prosecution.

1.1.4. Social fraud and serious fiscal fraud

Trends identified

Many large-scale files reveal how social fraud, serious fiscal fraud and organised increasingly feature as interrelated issues. The files feature well-organised (inter)national networks with links to organised crime[20].

Serious fiscal fraud as part of organised crime

In 2020, CTIF-CFI disseminated a large number of files related to organised crime. These files involve natural persons and legal persons that are part of an (inter)national network laundering the proceeds of various types of crime, including serious fiscal fraud. These are polycriminal groups that usually use front men, deliberately operate in several judicial districts (to remain undetected as long as possible) and (often) use the offsetting technique and trade-based money laundering (TBML).

The specific method varies according to the network but it has recently been identified that they often use foreign legal persons trading in drinks or vehicles. The foreign companies carry out intra-Community supplies to various Belgian companies that are almost all known to be "missing traders" or reveal VAT irregularities. The foreign companies are suspected to act as "conduit companies" (the organisers of the fraud circuit) and are unfavourably known to the Federal Public Service Finance.

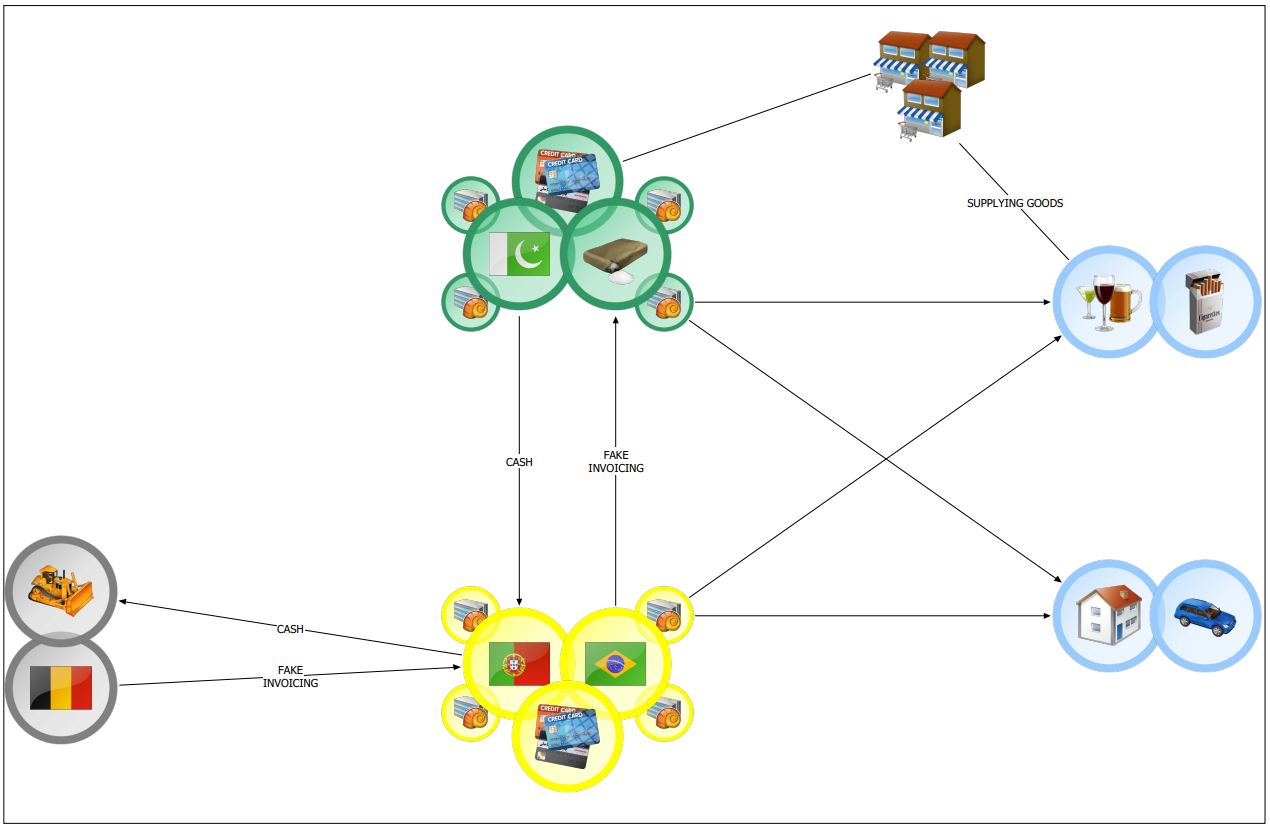
The trade in drinks seems to involve excise fraud. Figures of the Customs and Excise Administration show a sharp increase in smuggled alcoholic products, mainly because of the high excise duties in Belgium. As a result, organised crime groups flood the market with cheap drinks and tobacco products. In case of excise fraud sellers are tempted to purchase counterfeit products or products for which no excise duties and VAT have been paid in Belgium. In 2020, a case of enormous excise fraud was discovered in which beer, alcohol, soft drinks and mixed drinks were purchased in Luxembourg, Germany or the Netherlands and stored in illegal warehouses containing huge stocks. Customers, mostly owners of night shops, would then go to these warehouses to buy their goods.

[20] See section 1.2.1 below Use of polycriminal money laundering platforms.

Typological case 7: Money laundering between a Pakistani criminal organisation and a Brazilian criminal organisation

A Pakistani criminal group with links to illegal trafficking in narcotic drugs hands over cash to a Brazilian-Portuguese criminal organisation. They have a large number of companies, specialising in - after deducting a commission - handing over the cash (in this case the cash from the Pakistani group) to companies susceptible to fraud in need of cash.

There is a suspicion that this Brazilian-Portuguese criminal organisation then utilises these structures to use the money they receive on their accounts from these companies susceptible to fraud for investment purposes (in this case drinks). These investments are presumably made by order of this Pakistani group and these services are paid for by means of commissions.



Social fraud related to networks: issue on the rise

For a number of years CTIF-CFI has found that Brazilian or Portuguese nationals establish or take over companies, usually in the construction industry and industrial cleaning industry. More recently CTIF-CFI also found that other sectors were also involved, in particular goods transport and that other nationalities were also involved, such as nationals from Eastern Europe. These individuals, who also have the profile of front men, open accounts upon their arrival in Belgium. These accounts, used as channelling accounts, receive numerous transfers that refer to wages / provision of services / invoices from Belgian companies, mainly in the construction industry, the industrial cleaning industry or the transportation industry.

The money laundering take place through a combination of techniques, mainly cash withdrawals, transfers to wholesalers in Asia as part of laundering using the offsetting technique and trade-based money laundering (TBML)[21].

CTIF-CFI regularly finds that companies that are part of these networks have their registered office at the address of a so-called business centre. Since 2018, these company service providers have been required to register with the Federal Public Service Economy and to meet specific conditions[22]. These

[21] See section 1.2.2 below Trade-based money laundering (TBML).
[22] Law of 29 March 2018

business centres, who may provide a letterbox address to companies as well as administrative services, are also listed as obliged entities in the AML/CFT law.[23]

Several files show an increase use of the corporate structure of a partnership (*société en nom collectif* or SNC). Setting up this type of company does not involve many administrative requirements, which can make an SNC appealing for criminal purposes. Setting up an SNC does not entail large financial or accounting efforts, starting capital or a financial plan are not required. Nor is it mandatory to publish the annual accounts[24]. Partners are jointly and severally liable for the debts of a SNC. Bankruptcy of the SNC could entail bankruptcy of the partners, which can be seen as a major disadvantage. In case of misuse front men can be used, thus doing away with this disadvantage and criminals have a company at their disposal with little regulation that can be used discreetly.

Several files show that criminals increasingly turn to new players on the financial market such as online payment platforms (PSP) and neobanks, in particular abroad. In the case of networks it became clear that the managers of shell companies opened accounts with PSPs and neobanks abroad in order to receive money and withdraw cash without using the Belgian banking system. These files demonstrate the importance of international cooperation given that CTIF-CFI, thanks to its contacts with foreign counterparts, gained access to financial information on the PSPs and neobanks involved, despite the cross-border nature of the transactions.

Laundering the proceeds of smuggling of human beings prior to using the so-called Brazilian network

CTIF-CFI disseminated files to the judicial authorities with regard to social fraud, in particular the so-called Brazilian network, revealing links to smugglers of human beings. These intermediaries are known to the police as illegal labour subcontractors, who organise the trip of Brazilian nationals who come to work in Belgium and other European countries illegally. In these files numerous credit transfers are carried out with reference to travel cost (airline tickets, accommodation,…). As mentioned before, these files also show that online payment platforms are increasingly used for money laundering purposes. To an increasing extent PSPs are subjected to suspicious transactions related to the so-called Brazilian network.

Typological case 8: Money laundering related to smuggling of Brazilian workers for the so-called Brazilian network

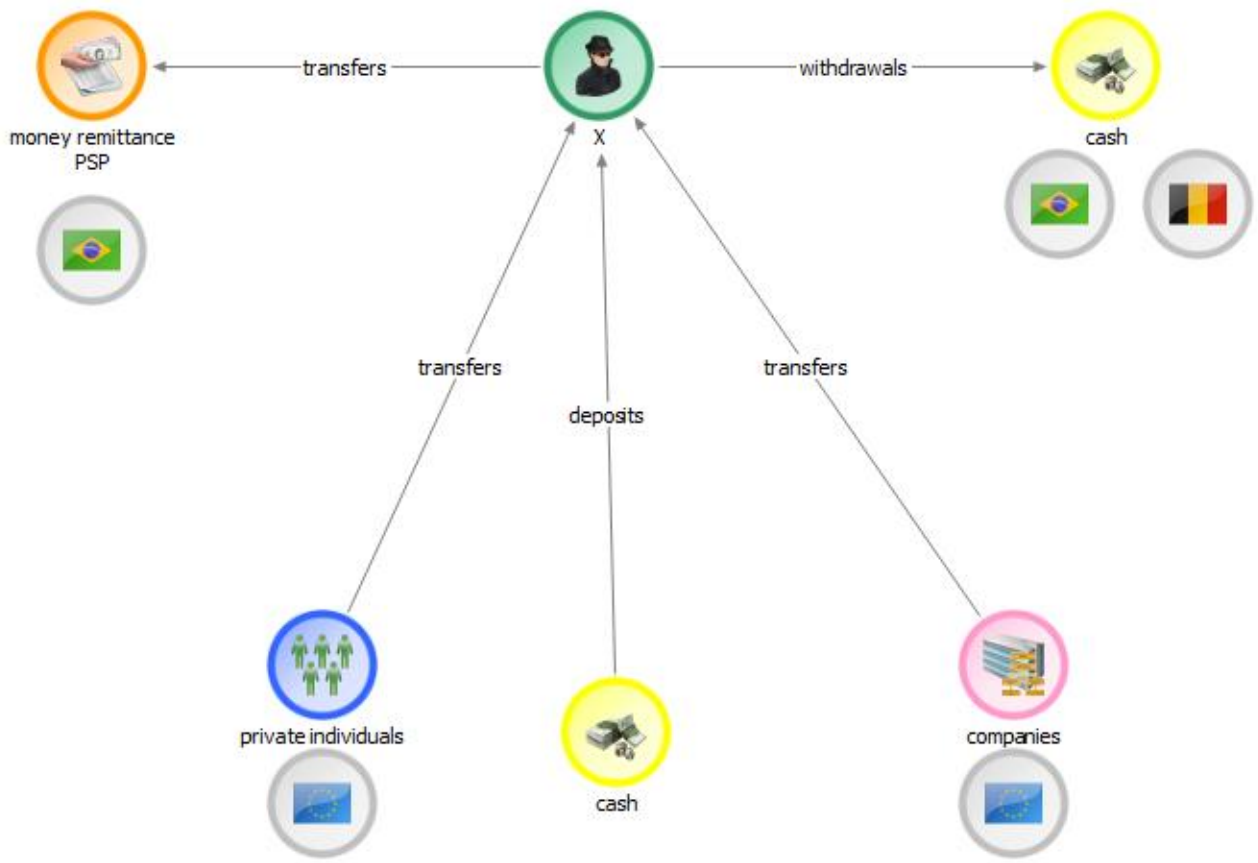
In this file suspicious transactions took place on the account of X. These transactions were spread over several accounts with several banks. On these accounts numerous in/out transactions took place between X's own accounts as well as many cash transactions (deposits and withdrawals). X also carried out numerous transactions with money remittance companies and online payment services companies (PSPs).

The detectable money transfers were mainly incoming transfers from many individuals (and to a lesser extent companies) in Belgium and other European countries. Several counterparties feature in various degrees in files that CTIF-CFI disseminated to the judicial authorities due to links with social fraud and/or serious fiscal fraud. Many transfers contain references to airline tickets, passengers or travelling.

X is known to the police for the smuggling of human beings. He is said to bring workers over from Brazil for several Belgian companies in the construction industry or the industrial cleaning industry, as well as companies in other European countries. Aside from the transfers we can conclude that there are serious indications that the cash deposited on X's different accounts originates from payments or commissions of several companies linked to the so-called Brazilian network looking for undeclared workers.

Given all of these elements we can conclude that X is a key figure in the so-called Brazilian network in Belgium. X regularly travels abroad, as is revealed by the many cash withdrawals and money transfers to himself through payment institutions. X operates as an intermediary and illegal labour subcontractor, he organises the journey and the transfers of Brazilian workers who come to carry out undeclared work, which highlights the scope of the network.

[23] Law of 18 September 2017, Article 5 §1, 29°
[24] On condition that all partners have unlimited liability.



Action taken

Board for combating fiscal and social fraud

The federal government has made combating fiscal fraud one of its priorities. In 2020, the government also revitalised the Board for combating fiscal and social fraud [*Collège pour la lutte contre la fraude fiscale et sociale*]. On 30 November 2020, the Royal Decree of 9 November 2020 establishing the Board for combating fiscal and social fraud was published in the Belgian Official Gazette. The renewed Board consists of several administrations, directorates and institutions involved, including CTIF-CFI, as well as the Members of the Board of Prosecutors-General [*Collège des procureurs généraux*], which have been given specific tasks on fiscal and social fraud) and the Federal Public Prosecutor. The aim is to develop a structured and coordinated policy among the different authorities.

Warning on the corporate structure of a partnership (société en nom collectif) and monitoring the issue of business centres

In recent months CTIF-CFI disseminated several files to the Public Prosecutor's Office related to the corporate structure of a partnership (*société en nom collectif* or SNC) that had recently been created. These companies were conduits for laundering the proceeds of various predicate offences, including serious fiscal fraud, social fraud, organised crime, smuggling of human beings and fraud.

CTIF-CFI found that the SNC that feature in files disseminated to the judicial authorities often officially active in sector with a higher risk of bankruptcy or money laundering (construction industry, transport, hospitality business, etc.). The partners of these SNC are mainly natural persons who are nationals of an EU Member State and with an address in Belgium. There are signs that those involved may in many cases be front men. The suspicious transactions in these files were mainly carried out through bank accounts.

Through a warning on its website CTIF-CFI called on the banks to be aware of potential involvement of SNCs in money laundering schemes and to report suspicious transactions related to this issue to CTIF-CFI.

In April 2021, CTIF-CFI held a meeting with the Federal Public Service Economy to discuss the issue of business centres and to assess to which extent these company service providers comply with their legal AML requirements.

The use of companies in money laundering schemes will be the subject of a strategic analysis that will be finalised in 2021.

1.1.5. Corruption and embezzlement

Trends identified

In 2020, CTIF-CFI disseminated some ten files to the Public Prosecutor's Office in which corruption or embezzlement by public officials was identified as the predicate offence. The number of disseminated files was at the same level as last year. The characteristics of these files were broadly the same as the ones in 2019.

Over half of the files related to politically exposed persons (PEPs) from countries in West and Central Africa and South America rich in natural resources, family members of the PEPs or people from their entourage. In several cases there were charges or accusations of illegal awarding of public contracts, embezzlement of government resources, illegal personal gain, favouritism or conflicts of interest. Moreover, a file regarding a Belgian public official was disseminated and a number of files featured Belgian nationals in the (inter)national business world involved in business transactions with companies or governments at one point in time.

The suspicious transactions in the files disseminated to the authorities could be linked to the familiar phases of the money laundering process (placement, layering, integration):

- There were serious indications that the funds deposited in cash on the public official's Belgian account were bribes taken for delivering official documents to individuals who did not qualify for these documents.
- In a file linked to corruption in the private sector the manager of a transport company received payments from a company in the East through a legal structure located abroad of which he was the economic beneficiary. The payments started in the year when the ordering party of the transactions announced that they had secured an important contract with the employer of the individual involved. The individuals did not use the money for a number of years and then moved it to a personal account abroad.
- Some individuals bought real estate or other precious goods (jewellery, gems, art and antiques,…) in Belgium or abroad. In some cases this was done using money from foreign accounts.

Typological case 9: Laundering the proceeds of high-level corruption

A foreign foundation for the promotion of art opened an account with a bank in Belgium a few months after it had been set up with a bank in Belgium and gave power of attorney to its manager, a Belgian national.

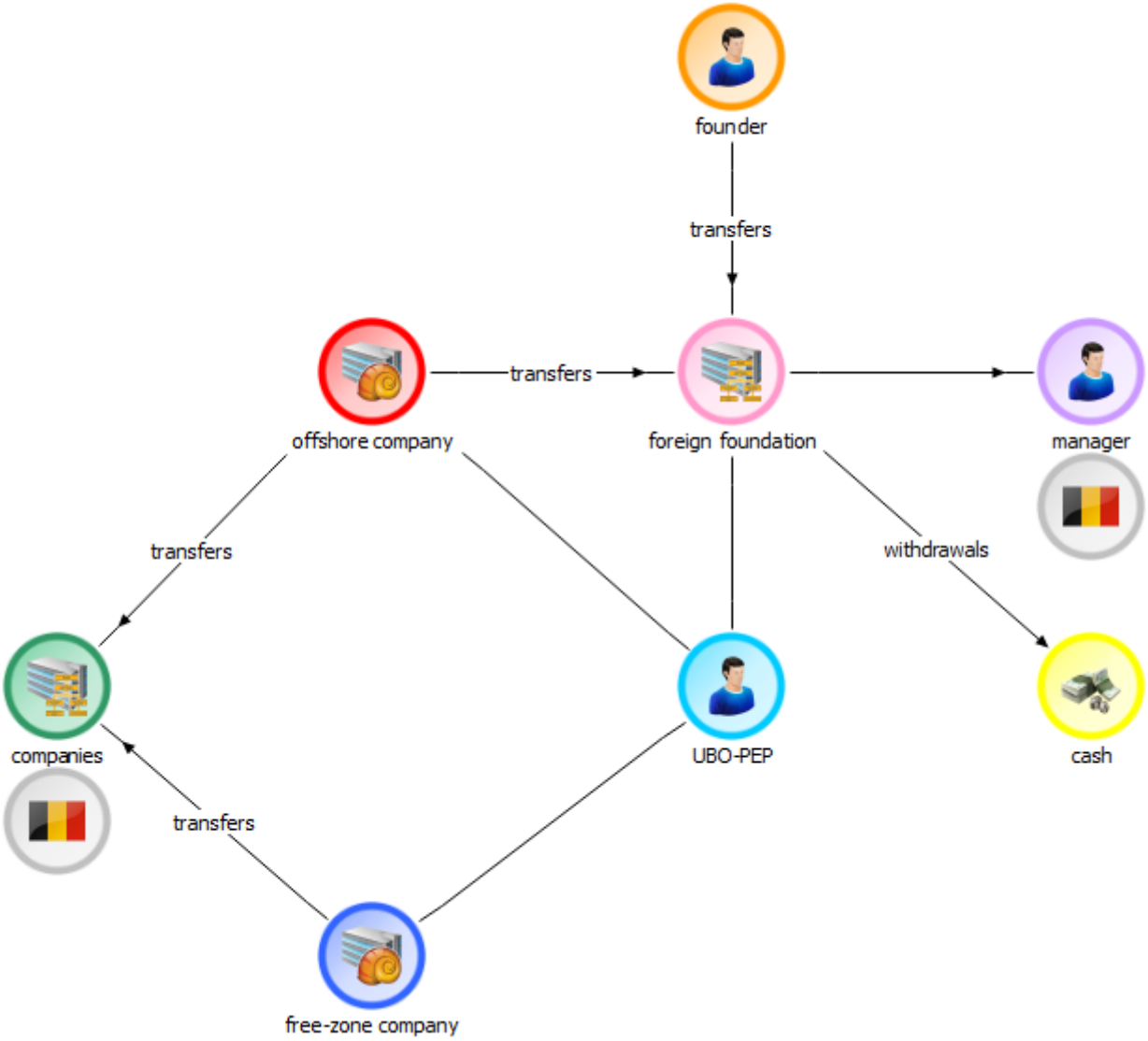
The foundation's account mainly received international transfers by order of the foundation's founder and international transfers by order of a company with a correspondence address in Mauritius. The latter transfers were carried out from account in Cyprus and Cabo Verde. The funds were used for payments related to the aim and the activities of the foundation and for transfers to the manager –not the economic beneficiary- and part of this was withdrawn in cash.

Open source information showed that the economic beneficiary was a family member of a foreign head of state involved in systematic political corruption benefitting the individual's partner and that the couple was accused of embezzling public money and of money laundering through a network of letterbox companies around the world.

The economic beneficiary of the foundation turned out to be the owner of two foreign companies for which suspicious transactions were reported to CTIF-CFI: the company that transferred money to the foundation's account and a company located in a free-trade zone in Dubai (United Arab Emirates). Both entities carried out transfers to different counterparties in Belgium, including individual in the art and antique world, companies specialising in interior and lighting, a dealer in

diamonds, a trader in luxury vehicles and a travel agency. In a few years' time the transactions amounted to several million EUR.

CTIF-CFI linked the international transfers to the foundation's account and the other beneficiaries in Belgium to laundering the proceeds of embezzlement of public funds and corruption.



CTIF-CFI reminds financial institutions and non-financial businesses and professions that they must have appropriate risk management systems to determine whether a customer or the beneficial owner is a Politically Exposed Person (PEP) (FATF Recommendation 12). Foreign PEPs and family members and close associates of these PEPs should automatically be considered to be high-risk and require that enhanced customer due diligence measures be applied.

For the disseminated files related to corruption CTIF-CFI received relevant information from other FIUs of the Egmont Group and used its powers to request (additional) information from obliged entities, police services (including the Central Department for Combating Corruption) and judicial authorities, intelligence services and administrative services of the State.

In accordance with the legal obligation and CTIF-CFI's common practice, the Central Office for Seizure and Confiscation (COSC) was informed when assets of significant value, of any nature, were available for a potential judicial seizure.

Global context

The link between corruption, economic crime and organised crime will be one of the priorities of the G20 Anti-Corruption Working Group[25].

Previously the G20 Ministers responsible for preventing and combating corruption[26] stressed the importance of international anti-corruption standards in the global fight against corruption, including the United Nations Convention against Corruption, the United Nations Convention against Transnational Organised Crime, the Organisation for Economic Co-operation and Development (OECD) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and related instruments, and the FATF Recommendations.

They committed to applying transparency on beneficial owners in practice and if necessary taking additional measures to prevent misuse of legal person and structures for money laundering and terrorist financing purposes. They promised to work together to detect, freeze and confiscate the proceeds of corruption and ensure that illegally obtained assets are returned in a transparent and efficient manner.

The Chair of the Egmont Group addressed the G20 ministerial meeting on the unique role of FIUs and their cross-border ability to track proceeds of corruption. She also stressed the vital importance of operational independence and the autonomy of FIUs.

There is a risk that the anti-corruption programme of a jurisdiction is used to criminalise political opponents and that the FIU of this jurisdiction is pressurised to share incorrect information with a counterpart FIU. Such practices should be avoided at all times.[27].

Combating laundering the proceeds of corruption remains one of the Egmont Group's priorities. CTIF-CFI will continue to focus on this issue. It expects that all obliged entities report any suspicions to CTIF-CFI and comply with their obligations as stated in the Law of 18 September 2017.

1.2. Evolution of money laundering techniques

1.2.1. Use of polycriminal money laundering platforms

Trends identified

Several files disseminated to the judicial authorities by CTIF-CFI point to an increasing trend: different criminal structures use companies with a similar profile, mainly in the construction industry or the industrial cleaning industry. They are a network and operate as money laundering platforms to launder the proceeds of various types of predicate offences referred to in the law.

CTIF-CFI has identified an evolution of the issue of networks[28]. Initially the focus was on gaining proceeds from illegal labour as part of social and serious fiscal fraud. Recent files indicate that networks are used for laundering the proceeds of other types of crime revealing other types of crime indicating ramifications with organised criminal networks. Enormous amounts are involved, on average more than EUR 2.000.000,00 per file.

CTIF-CFI opted for a horizontal approach of these files and mapped specific networks. This enabled CTIF-CFI to link files that initially appeared to be individual files and to demonstrate the scope and flexibility of these networks operating as polycriminal money laundering platforms.

---

[25] Leaders' Declaration, G20 Riyadh Summit, 21-22 November 2020.
[26] G20 Anti-Corruption Ministers Meeting, Ministerial Communiqué, 22 October 2020.
[27] The interpretative note of FATF's Recommendation 29 describes the principles of operational independence and autonomy of an FIU, the Egmont Group further developed these FATF requirements (*Egmont Group of Financial Intelligence Units (2018), Understanding FIU Operational Independence and Autonomy, The Egmont Group of Financial Intelligence Units*, Toronto, Canada).
[28] For more than ten years CTIF-CFI has identified so-called Brazilian networks related to social fraud and serious fiscal fraud. Brazilian / Portuguese nationals set up or take over Belgian companies in the construction industry or the industrial cleaning industry. These companies are often part of a network of different companies that are used for a limited time, the time it takes to carry out fraudulent transactions. They are subsequently replaced by new structures with new managers in order to perpetuate the system.

Profile of shell companies

The companies involved in these networks have a similar general profile: they are Belgian companies that officially operate in the construction industry or the industrial cleaning industry. The address of the registered office is often a "letterbox address" or the address of a business centre, the managers are front men (recently registered in Belgium, without any experience in managing companies); the companies are sometimes set up the same day, and are managed by the same people who arrived in Belgium at the same time.

As to accounting and finances we find that VAT returns are blank or not returned at all. The annual accounts are not submitted to the National Bank of Belgium, for some companies there is a legal obligation to withhold an amount to be paid to the Federal Public Service Finance. Some companies are not registered with the National Social Security Office[29]. The companies are usually not listed as Belgian customers of foreign companies in the Limosa register. These companies have accounts with several banks in order to spread the total amount of the suspicious transactions. A very large number of transactions take place on their account from the start, as well as similar transactions with the same counterparties.

Money laundering schemes

The credit transactions are transfers from different Belgian companies in the construction industry or the industrial cleaning industry. These transfers refer to the payment of invoices or services. In the declaration of works in the Dolsis database there is no subcontracting relationship between the ordering companies and the receiving companies (shell companies).

The debit transactions mainly feature two money laundering schemes:

- Money laundering scheme with cash withdrawals:

Following the credit transactions on the accounts of shell companies, the money is withdrawn in cash and in return for a commission given back to the ordering companies (customers) paying the invoices. They can use this cash to unofficially pay undeclared workers.

Apart from cash withdrawals from accounts of shell companies we also identified cash withdrawals following crossed transfers between the different companies of the network, or following transfers to their managers' (front men) personal accounts or the organisers of the network (actual managers)[30].

- Money laundering scheme with the offsetting technique:

CTIF-CFI has included numerous typologies on the offsetting technique in its annual reports since 2015. As a reminder, with the offsetting technique criminals who have cash proceeds of their illegal activities and criminals who need cash to finance their illegal activities find one another. The first group hands over the cash to a second group, they then -using fake invoices- transfer similar amounts to accounts provided by the first group. This methods prevents the most suspicious transactions, i.e. the ones in cash, from taking placing through the official banking system.

When the credit transactions have taken place on the accounts of the shell companies, the money is transferred to Belgian or foreign companies (with an account in Europe or in Asia) in different sectors or different types of trade. These transfers generally vaguely refer to purchases of goods or the payment of invoices without mentioning an actual reference. The different sectors seem to indicate that the financial transactions are based on fictitious services and that money laundering is taking place using the offsetting technique at national and international level.

[29] When they are registered, they only employ one employee, which seems to be a small number given the volume of the transactions on these companies' accounts.

[30] Apart from direct or indirect withdrawals CTIF-CFI also identified transfers to natural persons with an account in Belgium or Portugal. These transfers refer to the payment of wages but do not tally with the lack of a Dimona-declaration. Searches in the Limosa register in the Dolsis database indicate that these transfers were unwarranted. Most of the counterparties are unfavourably known to CTIF-CFI for featuring in files disseminated to the judicial authorities due to social and/or serious fiscal fraud.

It should be noted that the different money laundering schemes are not used exclusively but are often combined. Criminals want to split their suspicious financial transactions and make financial flows more difficult to detect. As the traditional banking system has become increasingly vigilant and has developed warning tools for transactions related to offsetting, money launderers often use payment service providers, providers of electronic money and neobanks.

Links to various predicate offences: polycriminal money laundering

Mapping the networks that CTIF-CFI identified made it possible to establish financial links between individuals featuring in separate files.

A group of de facto managers were identified to be leading several shell companies that made staff available to other building companies or industrial cleaning companies as part of a well-organised system of **social fraud and serious fiscal fraud**. These individuals had access to the bank cards of the shell companies, were the beneficiaries of transfers by order of these companies or carried out payments to the Belgian Official Gazette for setting up these companies.

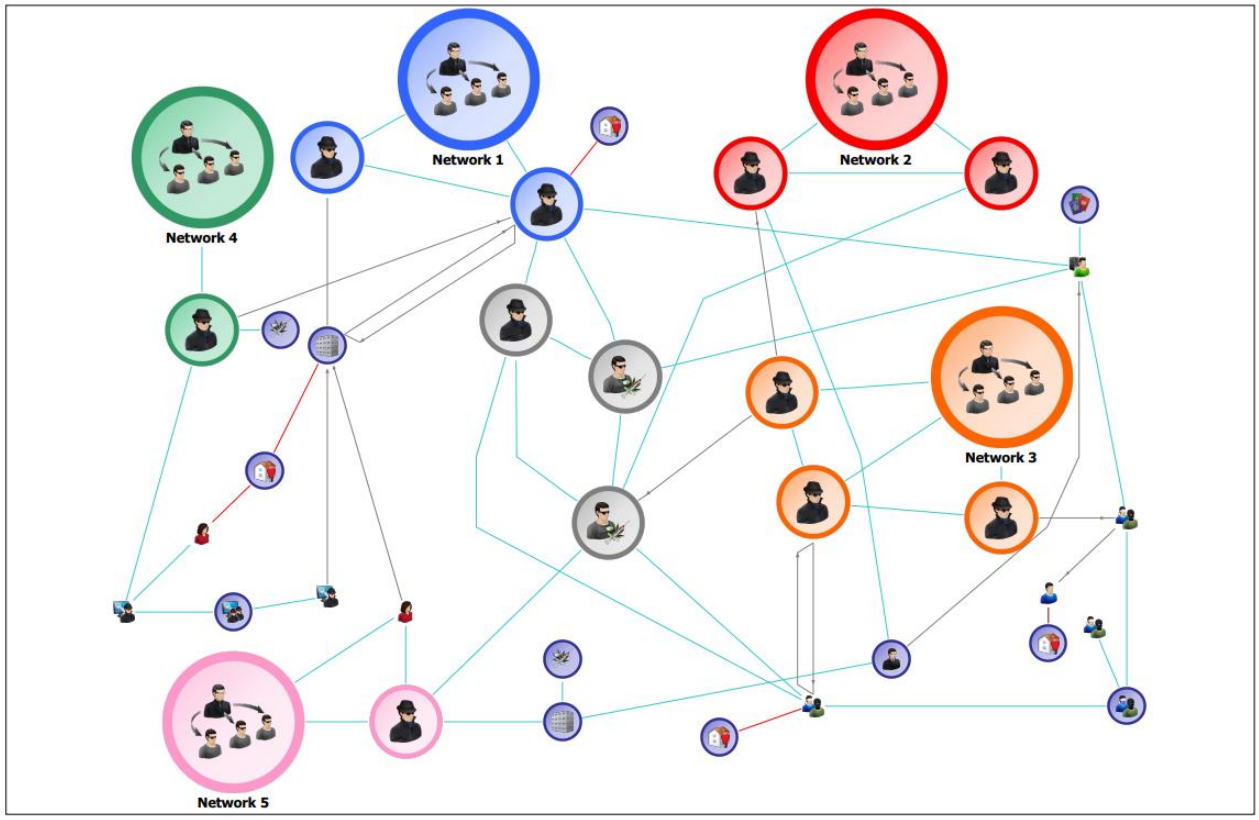
These managers could subsequently be linked to individuals who had committed other offences such as social fraud and serious fiscal fraud.

Further up the chain CTIF-CFI's analysis pointed to individuals operating as smugglers in the network to recruit undeclared workers by organising travel and transfer of Brazilian workers who came to carry out unofficial work in Belgium. Apart from this aspect related to **smuggling of human beings** some individuals with power of attorney on the shell companies were also known to the police due to exploitation of prostitution and/or trafficking in human beings beyond the Belgian borders.

With regard to trafficking in narcotic drugs several de facto managers of the detected networks were linked to an international criminal organisation trafficking narcotic drugs. Part of the cash proceeds of this trafficking was handed over to the shell companies and laundered using the offsetting technique. To this end transfers were carried out to a company in the United Arab Emirates (Dubai) suspected of operating as a professional money launderer.

Several shell companies, initially used to move funds linked to social fraud and serious fiscal fraud, were used for **fraud**. Transactions related to fraud practices such as fraudulent transfers took place on these companies' accounts. The money was subsequently transferred abroad.

Analysis shows that these networks used professional money launderers or facilitators, in particular to set up shell companies, draw up financial plans, and provide a registered office or to have power of attorney on the accounts. In the integration phase the facilitators were involved in real estate investments abroad.



Action taken

Awareness-raising of police and judicial authorities

These effectiveness of these networks is based on the increase of the number of companies involved, the recruitment of front men, crossing financial flows, the scope of the transfers and constant renewal of legal entities and bank accounts. This makes these networks difficult to apprehend.

The map with the main links involved in the identified networks was sent to the judicial authorities to visualise links between files that initially seemed unrelated and to stress the organised nature of these networks operating as polycriminal money laundering platforms.

Following this awareness-raising, several initiatives were set up to strengthen the cooperation between CTIF-CFI, the police and judicial authorities, for the operational analysis of files as well as strategic analysis of the identified modi operandi.

1.2.2. Trade-based money laundering (TBML)

Trends identified

Trade-based money laundering is a money laundering technique in which business transactions are used to conceal, transform or transfer money of illicit origin using business transactions. The main aim of TBML practices, contrary to predicate offences related to trade (illicit trafficking in goods and merchandise, counterfeit goods,…) is not to move the merchandise but the money of illicit origin using business transactions. This mainly involves importing and exporting merchandise and various instruments for cross-border trade being used.

Based on the files disseminated to the judicial authorities CTIF-CFI established that TBML practices are on the rise. Several trends were identified, which were also confirmed in a recent joint report on TBML by the FATF and the Egmont Group[31].

[31] FATF, *Trade-Based Money-Laundering*, 2020. https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html

Internationally different techniques have been described for a number of years[32] now that are used to misuse business transactions for money laundering purposes. These techniques include under-invoicing or over-invoicing of business transactions. Carrying out import and export transactions in which the number or value is overestimated or underestimated makes it possible to move and launder money. The same is true for fake descriptions: the goods on the invoice are not actually sent but the invoices state a price matching these goods. In reality the market value of the goods shipped is much higher or lower. The technique of multiple invoices involves drawing up several invoices for the same goods. Moreover, transactions can be entirely fictitious. These are known as phantom shipments: transfers are documented with invoices related to business transactions although no goods were delivered. This technique makes it possible to move money through a company account. It is also possible to set up a company abroad for the delivery or receipt of goods that have in reality never existed.

More recently, both internationally and in Belgium, other techniques were identified that are not necessarily based on the forgery techniques of merchandise or invoices described above. CTIF-CFI's files reveal that the offsetting technique is used to pay for various goods, which are subsequently imported and then sold on.

Several files featuring networks reveal transfers conducted by Belgian companies in the construction industry and the industrial cleaning industry to wholesalers for purchasing merchandise for criminals who had initially given them the cash. The offsetting technique is combined with TBML, the merchandise is subsequently imported by companies with the aim of selling this on.

Typological case 10: Offsetting technique and TBML are combined

The Belgian company A sells products on the internet. The company has bank accounts with several banks in Belgium and abroad. In 2020, A's accounts received transfers from several Belgian companies in the construction industry and the industrial cleaning industry, for an amount in excess of EUR 5 million. These transfers mainly referred to invoices or services subject to VAT. The money was subsequently transferred to several accounts abroad held by the company or by foreign companies.

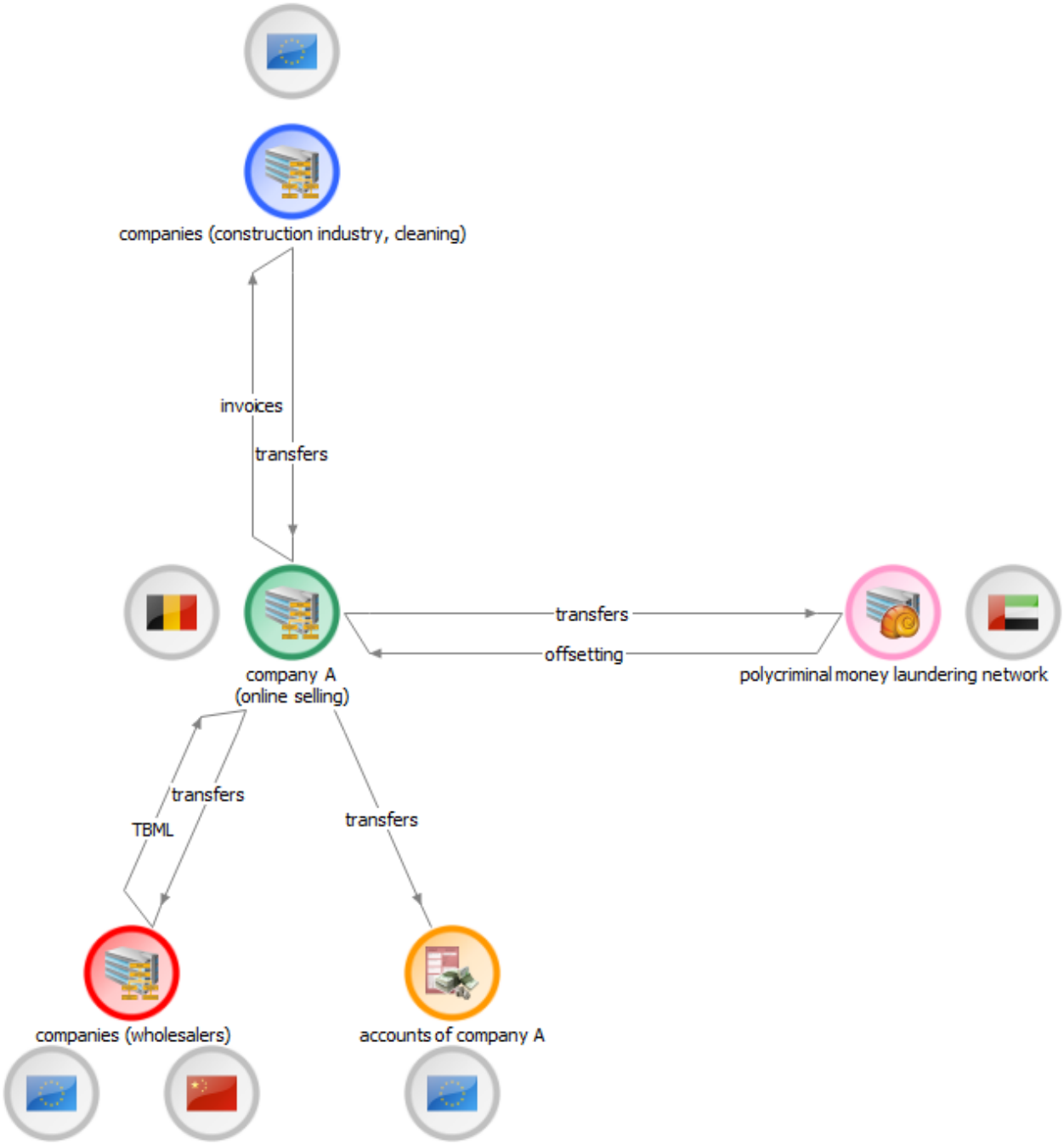
Company A did not have a license for mail order through its website. Moreover, it had not filed any VAT returns for 2020 and it had an obligation to withhold an amount to be paid to the tax authorities. So it was probable that company A did not meet all of its tax obligations.

Company A previously operated in the construction industry, a high-risk industry with regard to money laundering. The manager's address was the same as company A's registered office address, a residential building, which was remarkable given the company's activities. Moreover, most of ordering companies were known to CTIF-CFI in files that had been disseminated to the judicial authorities.

Part of the money was transferred abroad, to several wholesalers in non-food consumer goods as well as companies CTIF-CFI suspected to be operating as polycriminal money laundering platforms.

Given the information collected on the ordering companies and the different counterparties on the debit side of company A's accounts, this company appears to be an intermediary company in a money laundering scheme involving the cleaning industry and the construction industry in Belgium as well as abroad. Transfers to wholesalers could be linked to TBML practices as the merchandise was bought with money of illicit origin and subsequently re-imported in order to resell these goods via company A's online business.

[32] FATF, *Trade-Based Money Laundering*, 2006. https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html



Another technique is based on the use of networks for purchases on behalf of someone else, also referred to as "surrogate shopping networks" by the FATF[33]. In these networks buyers operate as intermediaries to buy goods for criminal organisations. These organisations hand over money of illicit origin to buyers who subsequently buy goods that are then brought to another jurisdictions in favour of criminal organisations. These buyers are mainly students who carry out many purchases, chiefly online.

Typological case 11: TBML related to a network for purchases on behalf of someone else

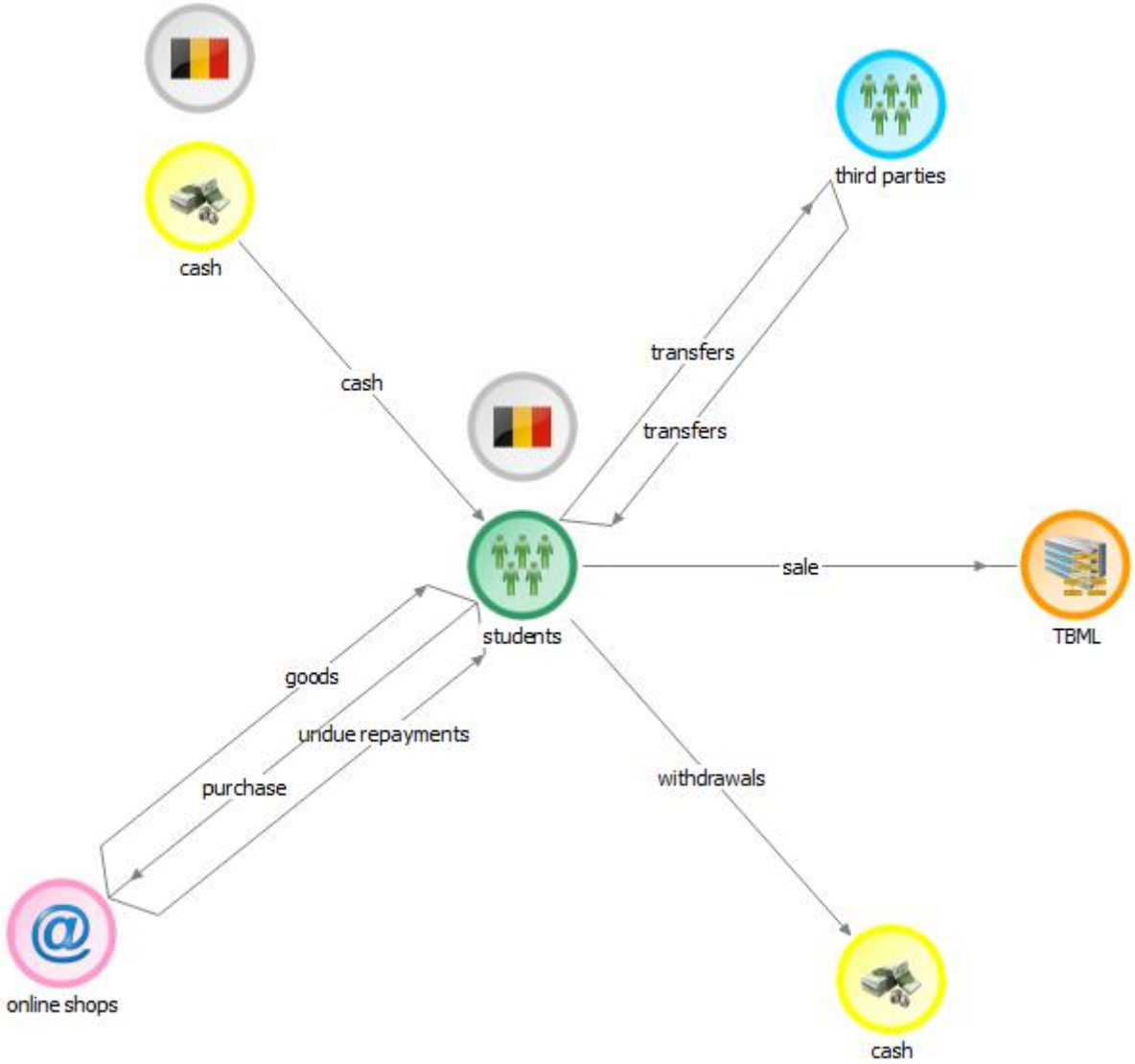
Dozens of people opened accounts with financial institutions. The same modus operandi was identified on these accounts: these people made many purchases by direct debit or with deferred payment. Before they had received their purchases and after the accounts had been debited, the people involved refused the direct debits, which were subsequently cancelled and refunded to their bank accounts. The financial institutions were able to get back some unduly received refunds but were unable to get back the majority of the other refunds. The money that was unduly sent to the account was withdrawn in cash shortly afterwards or transferred to third parties.

[33] FATF, Trade-Based Money-Laundering, 2020.

This modus operandi was always preceded by cash deposits or transfers, carried out by the account holder, or by a third party. The purchases took place online with payment platforms or traders.

No other types of transactions took place on the accounts, which seems to indicate that the accounts were opened with the sole aim of conducting suspicious transactions on this account. The individuals involved did not have any professional activity and were known to be students. Some of them and those crediting their accounts were known to the judicial authorities for trafficking in narcotic drugs.

The money on the account could therefore in whole or in part be the proceeds of illegal activities related to trafficking in narcotic drugs. The money was laundered through purchases for which the payments were subsequently refunded and withdrawn in cash or transferred to third parties. The goods that were fraudulently obtained could then be re-sold.



Apart from TBML CTIF-CFI also identified Service-Based Money Laundering or SBML[34]. Contrary to TBML, in the case of SBML money of illicit origin is moved using business transactions related to services instead of business transactions. These services include consultancy and advice, for which it is difficult to determine whether this involves real or fictitious services. As no goods are moved physically, no import or export data are available.

[34] Also refer to: FATF, *Trade-Based Money-Laundering*, 2020.

Typological case 12: SBML related to organised crime

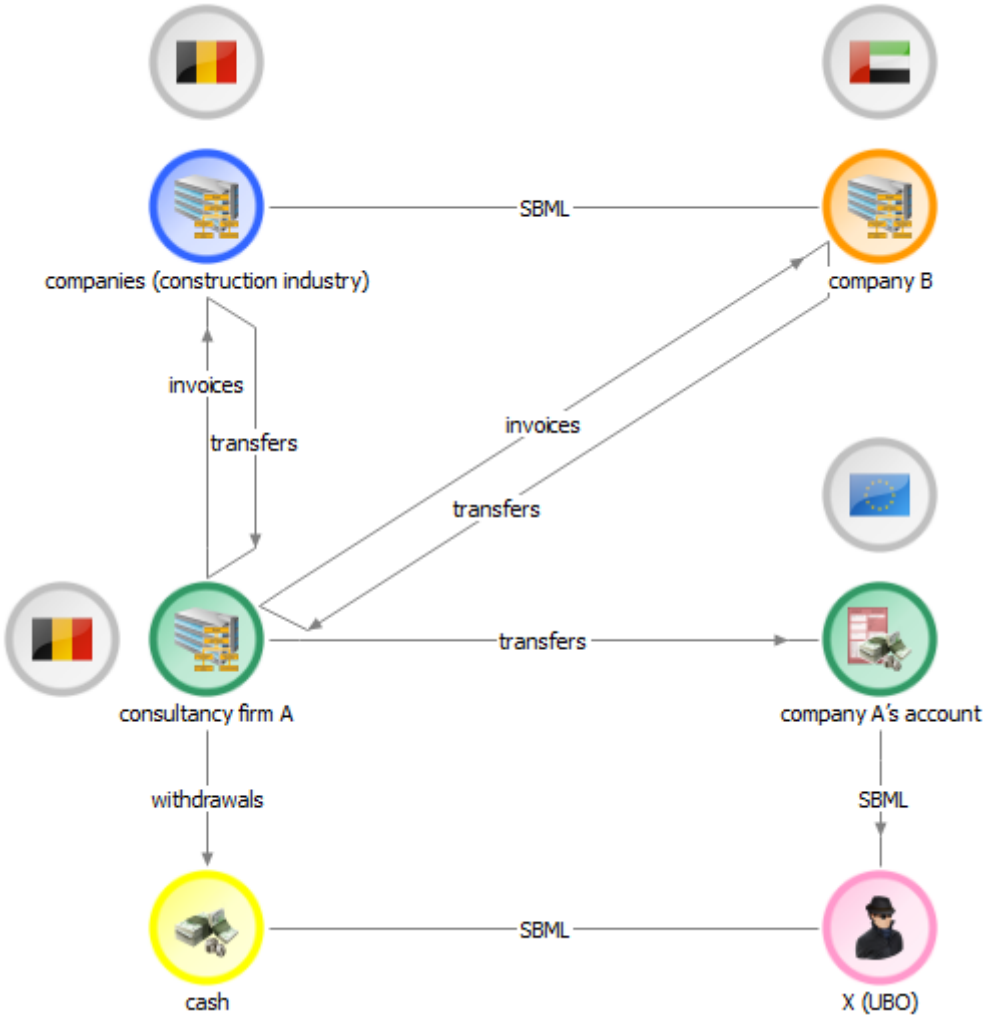
X, a foreign national providing real estate advice, was the economic beneficiary of several companies located abroad, including company A. Company A's account with a bank in Belgium received transfers related to invoices / services from several Belgian companies, for a total amount of nearly EUR 5 million. The money was then mainly transferred to an account held by company A abroad.

Company A's also received transfers from company B in Dubai. Company B used Company A's advice services. Apart from these transfers CTIF-CFI also identified several transfers, not from company B's account but from accounts in Belgium held by Belgian companies in the construction industry.

Most ordering companies operated in the construction industry and featured in files that CTIF-CFI had disseminated to the judicial authorities, mainly linked to social fraud and/or fiscal fraud.

Information from a foreign counterpart indicated that X was known to the judicial authorities because of links to several criminal organisations involved in trafficking in narcotic drugs. X purportedly accepted cash payments for real estate advice and applied this modus operandi by drawing up fake invoices using company A.

The Belgian companies carrying out the payments for company B are potentially part of a criminal organisation laundering money. The transactions could be related to SBML.



Action taken

Awareness-raising of obliged entities

TBML uses the complexity of trading systems, in particular in an international context when the vigilance procedures can be hampered by involving different parties and jurisdictions.

It is not uncommon that third parties feature in the payment chain of business transactions without any economic rationale. Financial institutions seem to be aware of the risk of such third parties. Although they have valuable information to identify TBML based on KYC, documents related to business transactions and the identification of irregularities, the conclusions of the joint report on TBML by the FATF and the Egmont Group states there is still too little awareness of TBML among financial professions.

Moreover, non-financial professions are insufficiently aware of identifying TBML although they have relevant information, especially with regard to commercial documents (invoices), corporate structures (front companies, complex and opaque entities), beneficial owners,…)

CTIF-CFI has found that TBML practices increasingly feature in files disseminated to the judicial authorities, so this is an important issue. As a result, CTIF-CFI published a warning on its website about the publication of the joint report on TBML by the FATF and the Egmont Group. To further raise awareness of obliged entities CTIF-CFI also contacted the Belgian federation of the financial sector Febelfin.

Following the publication of the joint report on TBML by the FATF and the Egmont Group a document with TBML indicators was posted on the respective websites of these two organisations[35].

1.2.3. Use of games of chance

The gaming sector has vulnerabilities that have been identified repeatedly at national and international level[36]. The industry is highly segmented (casinos, gaming halls, betting, etc.) and involves large amounts of money. Each game of chance has a different risk level with respect to money laundering.

Analysis of CTIF-CFI's files shows that the gaming sector is increasingly used by criminals to launder money of illegal origin. As a result of these findings CTIF-CFI conducted a strategic analysis in 2020 in order to comprehend the sector as much as possible and to focus on the challenges and vulnerabilities.

Trends identified

Although money laundering in the gaming sector mainly takes place through the player, the money laundering risk of the gaming provider (the establishment itself) should not be underestimated.

In case of money laundering by the gaming provider some criminals directly use gaming establishments (some online) to facilitate laundering the proceeds of their illegal activities. With the help of accomplices criminal money is directly transferred to the account of their companies in the gaming sector and combined with non-criminal money from other players who are not complicit. Several files indicate that money launderers set up companies in the gaming industry. Operating these companies is a cover to launder money from various criminal activities, in particular trafficking in narcotic drugs, organised crime and social fraud. Part of the cash deposits on these companies' accounts, purportedly related to the gaming sector, in reality originate from criminal activities.

Typological case 13: Setting up and running gaming establishments to launder money from criminal activities

Company A is a Belgian company in the gaming and betting industry, managed by other companies (in the same sector) and two individuals. The company is holder of an F2 licence

[35] https://egmontgroup.org/en/content/joint-eg-fatf-trade-based-money-laundering-risk-indicators

[36] FATF, *Vulnerabilities of casinos and gaming sector*, Paris, March 2009; Moneyval, *The use of online gambling for money laundering and financing of terrorism purposes*, Council of Europe, Strasbourg, April 2013; CFI (2019), 26th Annual Report

enabling the company to organise betting for licence 1 holders (licence required to organise betting).

Analysis of company A's account revealed numerous card payments, presumably payments by customers for games of chance organised by the company, as well as many cash deposits.

According to police information one of the managers is known for several cases of trafficking in narcotic drugs. He is said to import large quantities of cocaine through contacts in South America. He is said to use a business in car parts to transport large quantities to Belgium.

Information from a counterpart FIU showed that relatives of another manager were suspected of operating illegally in the gaming sector abroad.

It should also be noted that company A's registered office was located at the same address as companies in the transport industry that featured in one of CTIF-CFI's files that was disseminated to the judicial authorities due to serious indications of laundering the proceeds of organised crime.

In this regard Company A could be used to launder the proceeds of illicit trafficking in narcotic drugs. The money that was deposited in cash on company A's account and was allegedly related to betting, could in reality have originated in part or in full from illicit trafficking in narcotic drugs.

Criminals who visit casinos without the intention of playing are an example of money laundering by the player. They change the money that needs to be laundered into gaming chips, which they later return without having played. They get the money back and can justify the origin of the money using the receipts they receive from the casino.

The most frequently identified typologies indicate that gaming transactions are a part of larger money laundering operations that often involve the use of other techniques, in Belgium as well as abroad. Money launderers use different channels to make their transactions as opaque as possible and to conceal the origin or the destination of the money. The use of games of chances and payment service providers (PSP) and cryptocurrencies make it more difficult to detect funds. Moreover, new payment instruments such as cryptocurrencies and prepaid cards make it possible to change cash and facilitate anonymous transactions.

In some files CTIF-CFI found that some of a company's assets were used to carry out payments through a PSP to a casino, the winnings are subsequently transferred to the manager's account.

In other files prepaid online means of payment and an online casino are used to launder the proceeds of illicit trafficking in narcotic drugs. The cash proceeds of the illicit sale of narcotic drugs are used to buy vouchers. These vouchers are used to credit an account of an online casino. The account is subsequently debited by transfers to a bank account of an accomplice, even though the money was barely used to gamble or bet on the website.

Files related to fraud reveal that platforms for cryptocurrencies and online betting are used to make financial flows more opaque. Corporate accounts receive transfers from private individuals and cash deposits; these funds are subsequently partly transferred to several payment service providers and partly to platforms for changing cryptocurrencies.

CTIF-CFI's analysis confirms that the gaming sector can be very attractive to certain criminals who prefer to spend part of their money rather than launder these funds. The preference for games of chance is a lead that CTIF-CFI considers as part of its analysis.

Action taken

As mentioned before CTIF-CFI conducted a strategic analysis in 2020 of the gaming sector in order to comprehend the sector as much as possible and focus on the current challenges. This analysis led to different findings, in particular on the evolution of money laundering typologies in this sector. CTIF-CFI presented the results of this analysis to the Gaming Commission in April 2021. This meeting was an opportunity to exchange views on the issues and challenges the sector faces and the best strategies to respond to these in the future.

1.2.4. Money laundering via Dubai

Dubai is an important global financial centre and commercial hub, which attracts legal financial activities and business activities as well as illegal financial flows. The FATF recently assessed compliance with international standards to combat money laundering and terrorist financing of the United Arab Emirates (UAE)[37]. The FATF report points to many vulnerabilities and states that major and fundamental improvements are needed.

CTIF-CFI conducted a strategic analysis of the files linked with the United Arab Emirates, in particular with Dubai. The analysis shows that large amounts are often involved, that different predicate offences are involved and different modi operandi are used, which are often complex.

Trends identified

Criminal typologies identified with regard to money laundering

Several files relate to illicit trafficking in goods and merchandise linked to diamonds. These files, which often also relate to serious fiscal fraud, reveal links with diamond companies located in free-trade zones in Dubai. These companies often use the technique of "round tripping" [38]. Some files, reported by the Federal Public Service Economy, related to reservations by acknowledged experts on the announced value of diamonds[39].

Other files linked to fiscal fraud mainly involved financial flows to accounts in Dubai and revealed the use of fictitious corporate structures set up with the help of professional launderers.

Many files are linked to organised crime and confirm the appeal of real estate in Dubai for laundering the proceeds of organised crime, in particular laundering the proceeds of illicit trafficking in narcotic drugs. Several files also related to the so-called Brazilian network with the use of the offsetting technique: flows to companies in Dubai or to a money laundering platform in Dubai. The use of TBML mechanisms was also identified.

Typologies related to specific sectors

The FATF found the real estate sector in the United Arab Emirates to be very vulnerable to money laundering as it is possible to conceal the identity of those involved and the origin of the money. Open sources show that several individuals, subject to international sanctions, including organised crime figures and large-scale drug dealers, laundered their money in the real estate sector in Dubai. Several files that CTIF-CFI disseminated to the judicial authorities confirm these vulnerabilities.

The FATF also identified several vulnerabilities typical of the diamond sector. Apart from the issue of illegal trade in diamonds, Dubai is the third most important diamond centre in the world, diamonds also feature as a way to launder money. CTIF-CFI's files confirm the risks identified by the FATF.

The trade in gold was identified by the FATF as vulnerable to money laundering. The gold industry is one of the most important economic sectors in Dubai, the centre of the global gold market. The FATF listed many possibilities that make gold attractive to criminals as a way to launder money.

Money laundering techniques

---

[37] FATF, *MER UAE full.pdf* (fatf-gafi.org)

[38] The funds are transferred from one company to another with the use of fake invoices aimed at increasing turnover. There is no economic rationale for the transactions carried out in these files and in some cases no documentary proof was provided.

[39] Overvaluing or undervaluing diamonds with respect to the market value makes it possible to forge profit and turnover figures and therefore facilitates serious fiscal fraud. This alleged difference between the valuation of the expert and the amounts in the documents regarding the transaction is communicated to the relevant department of the Federal Public Service Economy, which then starts and investigation. In this case the dealer in diamonds must substantiate his declaration and the difference between the declared value and the value provided by the expert. Pursuant to Article 8, § 3, of the Royal Decree of 20 November 2019 on measures for the supervision of the diamond sector, the Federal Public Service Economy uses a risk-based approach to report these files to CTIF-CFI.

The modi operandi used are varied and often complex. Several files indicate that the offsetting technique is used. Transfers are carried out to companies with an account in Dubai in various sectors or types of trade. CTIF-CFI also identified flows to Dubai to an offsetting platform in Dubai conducted by a professional money launderer. The FATF's evaluation report mentions the use of professional money launderers as one of the main money laundering risks in the United Arab Emirates.

Some transactions identified correspond to TBML practices, a technique that is often used in the United Arab Emirates according the FATF's evaluation report.

Several files show that opaque corporate structures established in Dubai are used. These are Limited companies or Free-Zone Establishments in Dubai. The FATF evaluation report states that the disordered structure in the United Arab Emirates to register companies hampers authorities' work and hampers the identification of the beneficial owners. CTIF-CFI also established that fake invoices are used for services as a justification for transactions to these companies. The references accompanying the transfers are vague and refer to consultancy fees: "consultancy", "contract", "fee", …

Some files show that bank cards are used for all kinds of expenditure in Dubai. Most of these files are related to illicit trafficking in narcotic drugs.

Several techniques are combined and reveal that non-financial professions and professional money launderers are involved. Apart from using accounting professionals and legal professionals to set up corporate structures for criminal purposes and money laundering purposes some files also reveal that professional money laundering facilitators play an active role (setting up an offsetting platform, setting up complex structures for real estate investments, setting up opaque corporate structures that are connected…).

2. Terrorist financing trends

Trends identified

With regard to terrorist financing the downward trend of recent years, in terms of number of cases processed as well as the amounts involved, continued in 2020. The number of files disseminated to the judicial authorities for terrorist financing and the total disseminated amount is not comparable to years like 2016 and especially 2017. This downward trend was also confirmed by several national and international partners. This trend can be linked to the loss of influence by IS and the related issue of terrorist fighters travelling to Syria, as well as a changed modus operandi used for the most recent attacks in the West.

The loss of territorial importance of IS in Syria does not mean that the threat from this terrorist organisation has disappeared completely. Recent information shows that IS growing in the Euphrates Valley near Syria. South of the city of Al-Hasakah is a region where IS regularly commits attacks. In recent months Syrians were released from the camp of Al-Hol by the Kurds and IS and their doctrine are ubiquitous in the camp itself.

The past has shown that committing a terrorist attack or financing a terrorist group does not require large amounts of money. Recent history shows that the amounts have become even more insignificant for attacks that, apart from creating direct victims, still lead to an enormous shock in society and polarise society. Financial investigation remains a very useful tool and can in some cases be used as proof for objectively mapping links with other individuals or groups. Such a financial autopsy makes it possible to identify certain catalysts that have led to terrorist acts.

In 2020, the smaller number of files disseminated to the judicial authorities for terrorist financing was substantially offset by an extensive use of Article 83, §2, 4° of the Law of 18 September 2017. This article makes it possible to send relevant information to the intelligence services (State Security Department [VSSE] and General Intelligence and Security Service [SGRS-ADIV]) and the Coordinating Unit for Threat Analysis [OCAM-OCAD], within the framework of the fight against the radicalisation process, also when no serious indications of terrorist financing have been identified.

Apart from the valuable cooperation with the Public Prosecutor's Offices and police, the cooperation with the intelligence services and OCAM-OCAD are vital to CTIF-CFI, especially in a period when the imminent terrorist threat is not as great and early detection and cooperation for countering the radicalisation process have become more important.

CTIF-CFI also fulfilled its writing obligation for the Joint Database [*Banque de Données Commune*]. This is a database managed by OCAM-OCAD and the police and is the tool implementing the multidisciplinary approach of "Plan R" aimed at sharing unclassified information in real time with the various departments involved with regard to persons and organisations that need to be monitored with regard to terrorism and extremism, including the radicalisation process. In case CTIF-CFI has relevant information on persons featuring in this database, the relevant available financial information is entered into this database.

In recent years the issue of radicalisation in prison has become a topical issue again. Some prisoners convicted for terrorism are highly regarded in extremist circles and can be used as a figurehead to raise funds. Some of these individuals have now been released but for most of these prisoners their sentence will end in the coming years. In terms of finance, continued vigilance will be required for individuals who remain a risk, in cooperation with other competent authorities. CTIF-CFI had already identified the use of "prisoner accounts" in files with regard to terrorist financing. The question is to which extent this use entails risks of terrorist financing and/or radicalisation. CTIF-CFI repeatedly met on this matter with representatives of the Directorate General for Prisons [*Direction Générale des Établissements pénitentiaires*] (DG EPI)] over the past year in order to clarify the cooperation between both authorities and help EPI comply with its disclosing obligation by listing a number of non-exhaustive elements, trends and typologies that CTIF-CFI had identified in a number of files by way of example. EPI itself is in the best position to assess the suspicious nature of specific transactions -together with the behaviour of the prisoner. In 2020 CTIF-CFI received one disclosure and several interesting information reports from EPI.

Contrary to last year there is no real clear trend in the files disseminated to the judicial authorities in 2020. Although a number of files that were disseminated to the judicial authorities related to the issue of collectors using the usual financing channels we found there was a partial shift to the digital world, which will need to be monitored in the coming months.

This close monitoring by CTIF-CFI is part of subjecting part of the cryptocurrency entities to the Belgian preventative legislation.

New financing method – challenges linked to cryptopayments

In 2020, a new system for terrorist financing was identified, specified by the French FIU Tracfin, guaranteeing the discreet transfer of money to jihadists in Syria. This system is a new step in the evolution of terrorist financing. In recent years CTIF-CFI and the Public Prosecutor's Offices have focussed on dismantling money transfers through the usual channels. This new financing method give jihadists and their financiers the possibility of withdrawing from supervision of the usual money transfers for which identification obligations must be met.

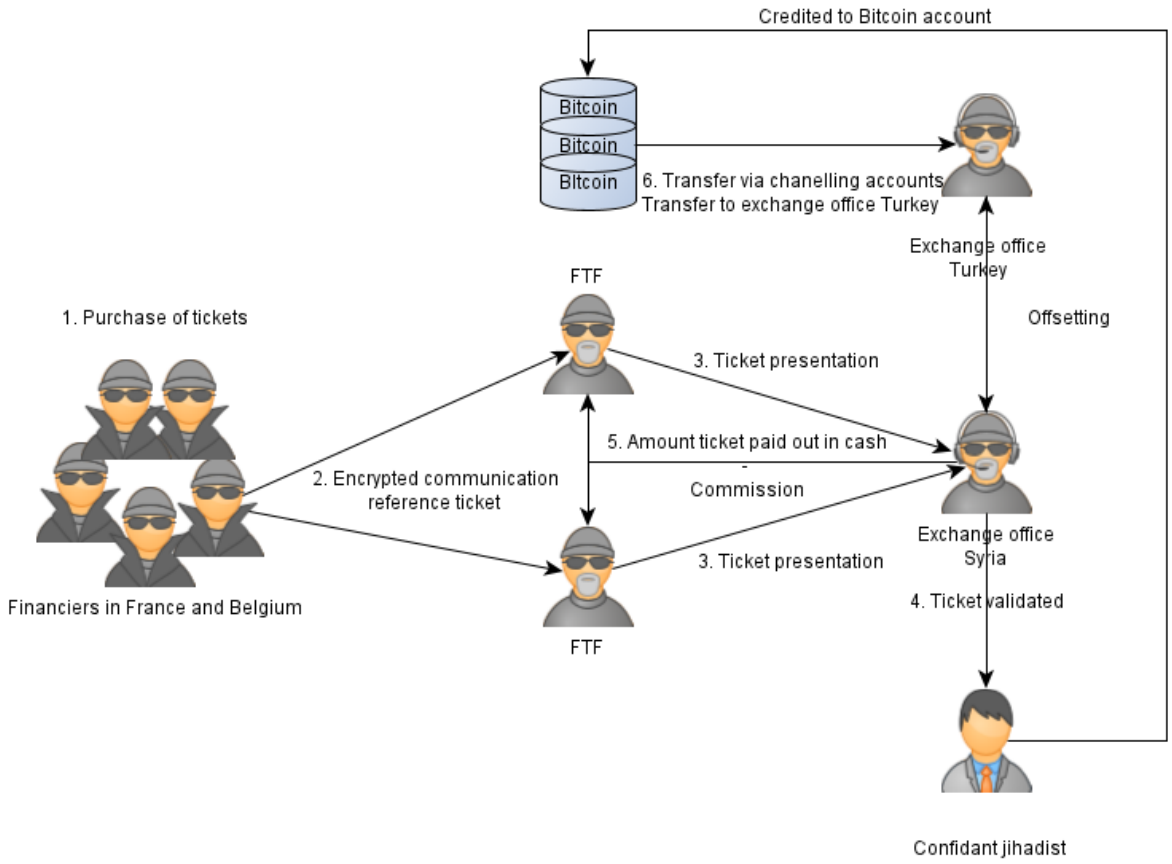
Cryptocurrencies (such as Bitcoin (BTC) and Ethereum (ETH)) can be purchased, stored, received and transferred through a mobile application. It is managed by a cryptowallet linked to the application. Registration only requires a phone number, a link is then sent to download the application, including a secured cryptowallet. The account is finally created by presenting an identity document and sending a video confirming that the person opening the account is the same as the owner of the identity document.

The innovative aspect is that the actual cryptopurchase takes place through a trader (e.g. a newsagent's or night shop) who hands over the following to the customer:

- Either a ticket (voucher) so the actual purchase of bitcoins can be delayed if required to wait for a better time to purchase based on the exchange rate of the cryptocurrency.

- Or through the Direct Bitcoin service so the cryptocurrency is received directly on the application. The price/value is the one applicable at the time of purchase.

The references of the prepaid and anonymous tickets / vouchers purchased by financiers (in France and Belgium) can be transferred through encrypted messaging (Telegram, Threema, Signal…) to jihadists in Syria. Thanks to a network of intermediaries and exchange offices these prepaid tickets are added to cryptoplatforms and the value of the tickets, after deducting a commission, are paid in a currency of their choice to jihadists who are still in northwest Syria or in the detention camp of Al-Hol or Al-Roj.



The number of providers of cryptovouchers in Belgium is currently very limited, but given the rapid digital transformation of the digital landscape, they could quickly gain importance.

It is now possible to purchase cryptocurrencies using nearly any means of payment: bank transfer, gift cards, credit cards, Bancontact, Western Union or even Sodexho cards. Although it has become more difficult to purchase cryptocurrencies in cash, it is still possible to use Bitcoin ATMs or sites that directly join buyers and sellers of cryptocurrencies. These sites operate as a type of market place on which cryptocurrencies are exchanged. Through this channel it is possible to find a buyer/seller who accepts cryptocurrencies in exchange for cash. The cash must then get to the buyer or seller via a courier or physical money transport.

The list of entities subject to the Law of 18 September 2017 was extended in July 2020 to include two types of virtual currency providers: custodian wallet providers and providers of exchange services between virtual currencies and fiat currencies (exchange platforms, crypto ATMs, brokers, etc.). Supervision of compliance with the AML is carried out by the Financial Services and Markets Authority. CTIF-CFI will actively engage with the Financial Services and Markets Authority in order to understand and comprehend the issue of cryptocurrencies and the different players involved as much as possible. The conditions and the registration procedure with the Financial Services and Markets Authority need to be clarified in a Royal Decree that should be adopted this year.

From then onwards, CTIF-CFI will start to receive and process disclosures, which will enable CTIF-CFI to better assess the vulnerabilities, threats and challenges related to this sector. It is likely that the applicable framework will evolve quickly given the ongoing talks at European level to develop a harmonised regulatory framework for all activities related to cryptocurrencies.

Lone wolves – recent attacks, red flags and current developments

A number of Islamic-inspired attacks were committed in Europe in 2020. On 16 October, a teacher was killed in the streets of Conflans-Sainte-Honorine in France. A few days later, on 29 October, an attack took place in the Basilica of Notre-Dame de Nice in Nice, France in which three people were stabbed to death. Shortly afterwards, on 2 November, an attack took place in the city centre of Vienna, Austria. Four people were killed in shootings and dozens were injured. The perpetrator was an IS sympathiser. It is striking that all perpetrators were in their early twenties. None of the perpetrators of the attacks in France were known to the French police or intelligence services for radicalism and/or terrorism.

The perpetrator of the attack in Vienna was in his early twenties and can also be considered to a lone actor (a person committing acts without belonging to any group) but his profile was very different from the perpetrators in France. He wanted to travel to Afghanistan in 2018 to fight for IS but he was stopped in Turkey and tried in Austria. After following a deradicalisation course he was released early at the end of 2019. Last summer the perpetrator tried to buy weapons in Slovakia. In recent years weapons with Slovakian registration numbers have been used for terrorist attacks and other criminal offences in Europe. The perpetrator was known to the police, the judicial authorities and the intelligence services.

Early detection of such attacks is very difficult and the financial trail of these terrorist acts is often non-existent or very limited. Analysis of perpetrators' profiles does show that there are potentially interesting warning signs that can be used in an investigation into financial transactions. Only by applying a very integrated approach and cooperation between national and international partners such developments can try to be stopped.

Apart from focus on Islamic terrorism, more focus is needed on growing extreme right-wing terrorism. On 19 February, ten people were killed following a shooting in a shisha bar in Hanau, Germany. The perpetrator had previously spread racist messages and incited to violence. This is not the first incident in Germany, which has seen a resurgence of extreme right-wing terrorism in recent years. Apart from this attack, another attack was foiled in Germany in 2020 and twelve people were arrested who were planning to commit large-scale attacks on Muslims in mosques. In 2019, extreme right-wing attacks were carried out in Christchurch (New Zealand), Poway (United States), El Paso (United States), Bærum (Norway) and Halle (Germany). It is striking that the perpetrators are always young people in their twenties.

The similarities between the most recent Islamic-inspired and extreme right-wing attacks are that both jihadi and extreme right-wing propaganda incite individuals to commit autonomous violence[40]. The perpetrators are often people in their twenties, who became radicalised and carried out an attack on their own initiative.

There have been several incidents in Belgium as well, confirming this unfortunate trend of potentially violent right-wing extremism.

Extreme right-wing groups, just like left-wing extremism, are mainly financed by contributions from their members and fundraising at events (parties, concerts). Some extreme right-wing groups explicitly request payments in Bitcoin of Ethereum when raising funds and praise the pseudo-anonymity of cryptopayments.

Over the past year, CTIF-CFI received more domestic and international disclosures related to extreme right-wing individuals or organisations. Only through integrated and close cooperation with the police, the Public Prosecutor's Offices and the intelligence services this issue can be tackled effectively. This way a well-founded assessment can be made of the potentially violent nature of individuals and organisations so specific suspicious financial transactions need to be considered to be terrorist financing. In a number of these files extensive cooperation with foreign FIUs was of great importance.

[40] https://beveiligingnieuws.nl/nieuws/zorgwekkende-stijging-extreemrechts-terrorisme

Typological case 14: Terrorist financing related to a foreign organisation

In 2020, CTIF-CFI received a disclosure regarding an organisation in Eastern Europe providing paramilitary training in which several Belgian nationals had taken part. One of them was known to OCAM-OCAD.

The organisation's website revealed that professional training was provided such as the use of firearms and manual combat techniques. The discourse is extreme right-wing, racist and identitarian. The training programme is presented as a preparation for acts of violence committed by migrants and considers governments failing to protect their citizens. Many people who take up this training support an identitarian or Neo-Nazi ideology.

Close cooperation with the FIU of the country involved enabled CTIF-CFI to analyse the accounts of this organisation providing military training. Between July 2016 and August 2020 the account received nearly EUR 400.000,00. Most of the funds originated from a personal account abroad of the organisation's founder, the remainder consisted of more than 200 smaller international transactions carried out by private individuals from Belgium, Switzerland, France as well as a smaller number of customers from the Netherlands, Estonia, Germany, Spain, Poland, Luxembourg, Great Britain and Italy. Most of the money received was converted into a different currency and used for the organisation's activities. Analysis showed that a number of the Belgian nationals who transferred money were known to the Belgian police for their extremist or racist ideology, discrimination offences or the possession of illegal firearms.

This information was shared with the intelligence service and OCAM-OCAD for further analysis.

V. ANNEX: Statistics 2020

TABLE OF CONTENTS

1. KEY FIGURES

1.1. Disclosures sent to CTIF-CFI

In 2020, CTIF-CFI received 31.605 disclosures from obliged entities.

	2018	2019	2020
Number of disclosures	33.445	25.991	31.605

22.823 disclosures were new money laundering or terrorist financing cases. 8.782 disclosures were additional reports related to existing files.

Section 2 below provides a detailed overview of these 31.605 disclosures.

The 22.823 disclosures received as new cases can be “subjective” disclosures or “objective” disclosures.

CTIF-CFI mainly receives “subjective” disclosures. These disclosures are based on a suspicion of money laundering or terrorist financing.

CTIF-CFI also receives “objective” disclosures, these are disclosures inter alia based on legal indicators or criteria.

“Objective” disclosures include disclosures from the Customs and Excise Administration (cross-border transportation of currency), notaries[41] and estate agents[42]. These disclosing entities are required to inform CTIF-CFI of facts, even if they do not have any suspicions. Some disclosures of payment institutions or currency exchange offices related to international transfers (money remittance) are generally also part of this category.

1.2. Newly opened files

A large number of disclosures relates to separate transactions related to the same case. Various disclosures from one single disclosing entity can relate to the same case. Furthermore, the same case can involve disclosures from various separate institutions.

CTIF-CFI groups disclosures of suspicious transactions that relate to one case into one file.

The disclosures received in 2020 were grouped into 21.805 files.

	2018	2019	2020
Number of new files opened because of ML or TF suspicions	15.670	13.796	21.805

In order to process disclosures effectively, CTIF-CFI classifies each disclosure upon receipt according to its importance (amount involved, nature of the transactions, politically exposed persons involved,…) and priority (urgent when funds can be frozen or seized or in case of an ongoing judicial investigation). These two criteria will determine the extent of research carried out and how quickly this research will have to be carried out. This selection process enables CTIF-CFI to balance any large variations in the number of disclosures or the number of files.

[41] In accordance with Article 66 of the Law of 18 September 2017.
[42] Ibid.

1.3. Files disseminated to the judicial authorities

In 2020, 1.228 new files or cases, for a total amount of EUR 1.636,49 million, were disseminated to the judicial authorities after CTIF-CFI's analysis revealed serious indications of money laundering or terrorist financing. The disseminated files refer to files opened in 2020 as well as in previous years.

In 2020, data or information from 2.765 disclosures, received in 2020 or in previous years, were disseminated to the judicial authorities after analysis. These 2.765 disclosures related to money laundering or terrorist financing transactions for a total amount of EUR 1.885,31 million.

	2018	2019	2020
Number of files disseminated to the judicial authorities	933	1.065	1.228
Amounts in the files disseminated to the judicial authorities(1)	1.432,73	1.158,66	1.636,49
Number of disclosures disseminated to the judicial authorities(2)	2.972	2.945	2.765
Amounts(1) in disclosures disseminated to the judicial authorities(2)	1.700,89	1.538,83	1.885,31

(1) Amounts in million EUR.
(2) CTIF-CFI does not disseminate any copies of disclosures, but only information on suspicious transactions mentioned in these disclosures, in addition to its analysis.

1.4. Number of freezing orders

In 2020, CTIF-CFI used its power to oppose execution of a transaction on 33 occasions. CTIF-CFI temporarily froze assets worth EUR 30,58 million.

	2018	2019	2020
Number of freezing orders	8	26	33
Total amount of freezing orders(1)	0,68	3,77	30,58

(1) Amounts in million EUR.

2. SOURCES OF DISCLOSURES SENT TO CTIF-CFI

2.1. Disclosures

	2018	2019	2020	% 2020
Credit institutions	9.980	11.237	17.678	55,93
Payment institutions	14.079	5.814	6.263	19,82
Notaries	1.270	1.239	1.177	3,72
Company under public law *bpost*	1.066	1.470	897	2,84
Life insurance companies	229	308	661	2,09
Institutions for electronic money	0	90	654	2,07
External accountants, external tax advisors, external licensed accountants, external licensed tax specialists-accountants	212	248	254	0,81
National Bank of Belgium	616	456	197	0,62
Mortgage credit institutions	26	83	166	0,53
Gaming establishments	1.103	396	157	0,50
Companies for consumer credit	22	132	151	0,48
Currency exchange offices	223	117	106	0,34
Branch offices of investment companies in the EEA	0	2	70	0,22
Company auditors	60	73	38	0,12
Estate agents	55	52	37	0,12
Stock broking firms	37	49	33	0,10
Company service providers	0	2	27	0,09
Bailiffs	69	44	24	0,08
Lease-financing companies	3	2	19	0,06
Lawyers	8	11	17	0,05
Branch offices of management companies of collective investment undertakings in the EEA	0	0	6	0,02
Insurance intermediaries	4	4	5	0,01
Dealers in diamonds	18	15	4	0,01
Intermediaries in banking and investment services	0	1	3	0,01
Portfolio management and investment advice companies	0	0	3	0,01
Branch offices in Belgium of life insurance companies in the EU	0	1	0	-
Central securities depositaries	-	0	0	-
Security firms	1	0	0	-
Market operators	0	0	0	-
Payment institutions issuing or managing credit cards	0	0	0	-
Collective investment undertakings	0	0	0	-
Independent financial planners	0	0	0	-

Alternative funding platforms	0	0	0	-
Debt investment firms	0	0	0	-
Mutual guarantee societies	0	0	0	-
Management companies of collective investment undertakings	0	0	0	-
Management companies of alternative investment funds	0	0	0	-
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0	-
Branch offices of investment companies outside the EEA	0	0	0	-
Settlement institutions	2	-	-	
Total	**29.083**	**21.846**	**28.649**	**90,64**

2.2. Requests for information received from FIU counterparts

	2018	2019	2020	% 2020
FIU counterparts	1.806	1.463	1.003	3,17

2.3. Notifications received from other competent authorities

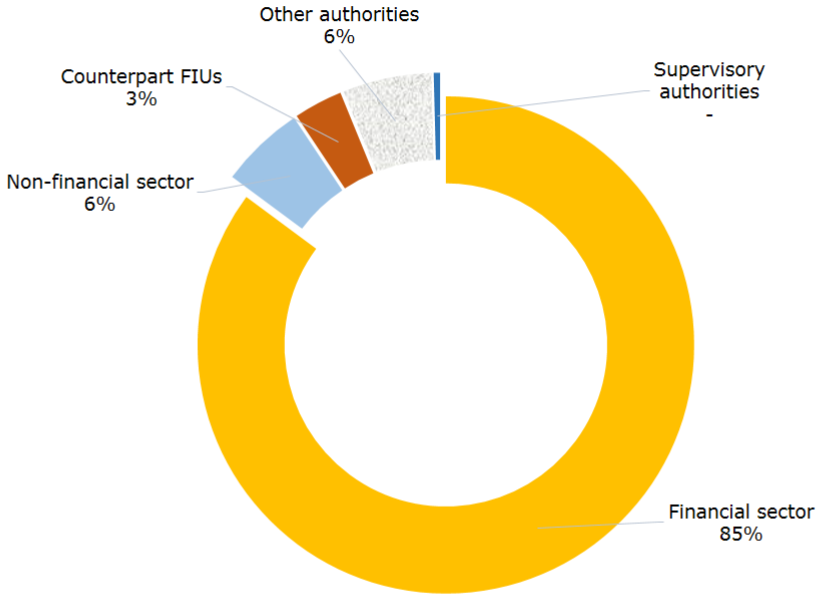
	2018	2019	2020	% 2020
Customs and Excise(1)	1.135	1.794	1.076	3,40
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	1.239	665	604	1,91
Federal Public Service Finance	11	29	50	0,16
Flemish tax authority [*Vlaamse belastingdienst*]	70	44	36	0,11
State Security Department [VSSE]	12	8	16	0,05
Federal Public Service Foreign Affairs	3	-	-	-
Federal Public Service Economy	18	68	26	0,08
(Federal and regional) social inspectorate	-	-	6	0,02
Trustees in a bankruptcy and temporary administrators	4	8	2	0,01
Coordinating Unit for Threat Analysis [OCAM-OCAD]	1	3	2	0,01
Information and advice centre on harmful sectarian organisations [*Centre d'Information et d'avis sur les organisations sectaires*]	-	1	2	0,01
General Intelligence and Security Service [SGRS-ADIV]	3	-	2	0,01
Federal Public Prosecutor's Office	28	12	1	-
Prisons	-	1	1	-
Public Prosecutor's Office Antwerp	1	-	-	-
Total	**2.520**	**2.633**	**1.824**	**5,79**

(1) In accordance with Directive (EC) no 1889/2005 of 26 October 2005 and the Royal Decree of 26 January 2014 on supervisory measures for the physical cross-border transportation of currency.

2.4. Notifications received from supervisory, regulatory or disciplinary authorities

	2018	2019	2020	% 2020
Financial Services and Markets Authority	7	28	114	0,36
National Bank of Belgium	-	1	1	-
Federal Public Service Economy Antwerp	24	17	12	0,04
Gaming Commission	-	1	1	-
Institute of Accountants and Tax Consultants [*Institut des Experts-comptables et des Conseils fiscaux*]	-	2	3	-
Total	**31**	**49**	**131**	**0,40**

GRAND TOTAL (2.1 - 2.4)	**33.445**	**25.991**	**31.605**	**100**



2.5. Number of entities having submitted disclosures

Financial professions	2018	2019	2020
Credit institutions	56	60	58
Currency exchange offices, payment institutions, and issuers and institutions for electronic money	36	37	32
Life insurance companies	20	16	17
Mortgage credit institutions	9	12	11
Companies for consumer credit	5	10	8
Stock broking firms	8	9	6
Insurance intermediaries	4	3	5
Branch offices of investment companies in the EEA	0	2	5
Lease-financing companies	2	2	5
Company service providers	0	2	4
Company under public law *bpost*	1	1	0
National Bank of Belgium	1	1	1
Intermediaries in banking and investment services	0	1	2
Payment institutions issuing or managing credit cards	0	0	0
Management companies of collective investment undertakings	0	0	0
Branch offices of investment companies in the EEA	0	0	1
Settlement institutions	2	-	0
Central securities depositories	-	0	0
Portfolio management and investment advice companies	0	0	1
Public Trustee Office	0	0	0
Portfolio management and investment advice companies	0	0	0
Market operators	0	0	0
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0
Collective investment undertakings	0	0	0
Mutual guarantee societies	0	0	0
Management companies of alternative investment funds	0	0	0
Debt investment firms	0	0	0
Alternative funding platforms	0	0	0
Independent financial planners	0	0	0
Total	**144**	**157**	**156**

Non-financial professions	2018	2019	2020
Notaries	290	345	307
Accounting and tax professions	136	142	156
Estate agents	25	29	19
Company auditors	21	27	20
Bailiffs	16	15	11
Lawyers	4	8	8
Gaming establishments	11	14	12
Trustees in a bankruptcy and the temporary administrators	3	6	2
Dealers in diamonds	2	3	1
Security companies	1	0	0
Total	**506**	**589**	**536**

3. FILES DISSEMINATED TO THE JUDICIAL AUTHORITIES

CTIF-CFI groups disclosures of suspicious transactions that relate to one case into one file. In case of serious indications of money laundering or terrorist financing, this file is disseminated to the competent Public Prosecutor or the Federal Public Prosecutor.

In 2020, CTIF-CFI disseminated 1.228 new files to the judicial authorities for a total amount of EUR 1.636,49 million.

If after disseminating a file to the judicial authorities CTIF-CFI receives new (additional) disclosures on transactions that relate to the same case and there are still indications of money laundering or terrorist financing, CTIF-CFI will disseminate these new suspicious transactions in an additional file.

In 2020, CTIF-CFI disseminated a total of 2.765 disclosures (new files and additional disseminated files) to the judicial authorities for a total amount of EUR 1.885,31 million.

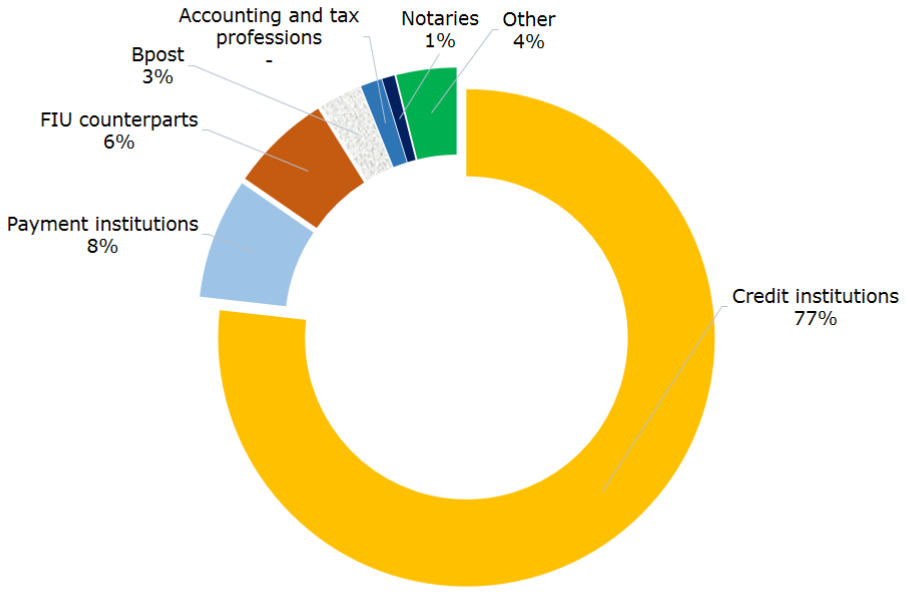
These disseminated files and disclosures are presented below by type of disclosing entity, type of transaction and predicate offence.

3.1. Files disseminated to the judicial authorities by category of disclosing entity

Number of files disseminated to the judicial authorities by category of disclosing entity – Evolution in the past 3 years

	2018	2019	2020	% 2020
Credit institutions	688	783	942	76,71
Payment institutions	108	102	96	7,82
FIU counterparts	43	68	80	6,51
Company under public law *bpost*	46	37	34	2,77
Accounting and tax professions	12	14	17	1,38
Notaries	7	4	10	0,81
Gaming establishments	8	1	6	0,49
Branch offices of investment companies in the EU	-	-	6	0,49
Federal Public Service Economy Antwerp	1	5	5	0,41
Institutions for electronic money	-	1	4	0,33
Federal Public Service Finance	1	6	4	0,33
Customs	-	3	4	0,33
Stock broking firms	2	2	3	0,24
State Security Department [VSSE]	1	2	3	0,24
Company auditors	1	1	2	0,16
Life insurance companies	-	-	2	0,16
Financial Services and Markets Authority	-	4	1	0,08
Currency exchange offices	3	2	1	0,08

Federal Public Prosecutor's Office	2	9	1	0,08
Mortgage credit institutions	-	3	1	0,08
Dealers in diamonds	1	3	1	0,08
Bailiffs	1	2	1	0,08
Coordinating Unit for Threat Analysis [OCAM-OCAD]	-	2	1	0,08
Prisons	-	-	1	0,08
Lawyers	-	1	1	0,08
Companies for consumer credit	-	-	1	0,08
National Bank of Belgium	5	6	-	-
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	-	2	-	-
Flemish tax authority [*Vlaamse belastingdienst*]	-	1	-	-
Estate agents	-	1	-	-
Federal Public Service Economy Other	2	-	-	
OLAF	1	-	-	-
Total	**933**	**1.065**	**1.228**	**100**



Amounts[1] *in the files disseminated to the judicial authorities – Evolution in the past 3 years*

	2018	2019	2020	% 2020
Credit institutions	1.245,84	807,77	1.122,09	68,57
FIU counterparts	48,34	85,70	206,15	12,60
Accounting and tax professions	15,78	15,50	113,22	6,92
Federal Public Service Economy Antwerp	87,04	218,16	91,65	5,60
Company auditors	0,10	1,02	29,38	1,80
Payment institutions	17,27	8,67	21,21	1,30
Federal Public Service Finance	0,09	4,43	14,72	0,90
Branch offices of investment companies in the EU	-	-	10,99	0,67
Notaries	5,22	3,03	7,25	0,44
Stock broking firms	2,73	0,83	5,55	0,34
Coordinating Unit for Threat Analysis [OCAM-OCAD]	-	0,38	3,75	0,23
Lawyers	-	0,21	2,67	0,16
Customs	-	0,74	1,86	0,11
Company under public law *bpost*	2,75	2,81	1,74	0,11
Life insurance companies	-	-	1,63	0,10
Gaming establishments	1,77	0,04	0,90	0,05
Financial Services and Markets Authority	-	1,75	0,82	0,05
Institutions for electronic money	-	0,04	0,53	0,03
Dealers in diamonds	0,06	0,78	0,21	0,02
State Security Department [VSSE]	0,05	-	0,08	-
Currency exchange offices	1,82	0,04	0,03	-
Bailiffs	2,20	1,28	0,03	-
Mortgage credit institutions	-	2,58	0,02	-
Companies for consumer credit	-	-	0,01	-
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	-	1,21	-	-
Flemish tax authority [*Vlaamse belastingdienst*]	-	0,86	-	-
Estate agents	-	0,65	-	-
National Bank of Belgium	1,09	0,15	-	-
Federal Public Prosecutor's Office	0,08	0,03	-	-
Federal Public Service Economy Other	0,38	-	-	-
European Anti-Fraud Office OLAF	0,12	-	-	-
General Intelligence and Security Service [SGRS-ADIV]	-	-	-	-
Total	**1.432,73**	**1.158,66**	**1.636,49**	**100**

(1) Amounts in million EUR.

Breakdown per category of disclosing institution for disclosures disseminated to the judicial authorities in 2018, 2019 and 2020

	2018		2019		2020	
	Number	Amount(1)	Number	Amount(1)	Number	Amount(1)
Credit institutions	1.625	1.430,77	1.829	1.075,52	1.998	1.323,51
FIU counterparts	122	70,93	139	119,86	153	221,73
Accounting and tax professions	42	16,56	34	16,24	39	114,00
Federal Public Service Economy Antwerp	4	87,04	15	218,16	14	94,97
Company auditors	3	0,10	6	1,84	4	29,39
Payment institutions	782	19,65	526	28,08	299	27,00
Federal Public Service Finance	3	0,10	8	5,84	8	16,11
Branch offices of investment companies in the EU	-	-	-	-	10	10,99
Life insurance companies	15	0,62	25	0,02	18	7,61
Notaries	25	5,78	30	4,29	40	7,45
Stock broking firms	4	36,47	4	0,83	3	5,55
Coordinating Unit for Threat Analysis [OCAM-OCAD]	-	-	2	0,38	1	3,75
Institutions for electronic money	-	-	1	1,01	9	2,40
Customs	7	0,10	18	0,81	27	2,12
Company under public law *bpost*	103	16,52	103	3,93	67	1,77
Gaming establishments	133	5,71	63	0,25	18	1,20
Financial Services and Markets Authority	2	-	5	1,77	3	0,81
Dealers in diamonds	1	0,06	9	0,78	2	0,21
State Security Department [VSSE]	2	0	6	0,01	5	0,10
National Bank of Belgium	32	1,64	23	1,62	6	0,07
Federal Public Service Economy Other	1	-	1	-	3	0,07
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	8	-	19	1,21	15	-
Federal Public Prosecutor's Office	6	0,10	14	0,04	2	-
Institute of Accountants and Tax Consultants [*Institut des Experts-comptables et des Conseils fiscaux*]	-	-	-	-	1	-
Currency exchange offices	37	3,09	44	50,73	1	-
Flemish tax authority [*Vlaamse belastingdienst*]	-	-	1	0,86	1	-
Federal Public Service Foreign Affairs	-	-	2	-	-	-
General Intelligence and Security Service [SGRS-ADIV]	-	-	-	-	-	-
Other	15	5,65	18	4,75	18	14,50
Total	**2.972**	**1.700,89**	**2.945**	**1.538,83**	**2.765**	**1.885,31**

(1) Amounts in million EUR.

The amounts above are the sum of actual money laundering transactions and potentially fictitious commercial transactions. With these transactions (including files related to VAT carousel fraud) it is very difficult to determine which part is laundered and which part consists of potentially fictitious commercial transactions.

3.2. Nature of the suspicious transactions

The table below specifies the nature of the suspicious transactions in files disseminated to the judicial authorities in 2020. A file disseminated to the judicial authorities may include various types of suspicious transactions.

Type of transactions	Number of files	% 2020
International transfers	420	25,07
Domestic transfers	396	23,64
Cash withdrawals from an account	258	15,40
Cash deposits into an account	215	12,84
Money remittance – Sent	110	6,57
Money remittance – Received	8	0,48
Purchase of real estate	12	0,72
E-money	5	0,30
Transport of cash	5	0,30
Consumer credit	3	0,18
Casino transactions	9	0,54
Fiscal regularisations	1	0,06
Mortgage credit	1	0,06
Life insurance	9	0,54
Cash payments	1	0,06
Use of cheques	2	0,12
Other	220	13,12
Total		**100**

3.3. Financial flows

The table below provides an overview of the financial flows outside of Belgium in the files that CTIF-CFI disseminated to the judicial authorities in 2020, including the main countries of origin and destination of the international transfers.

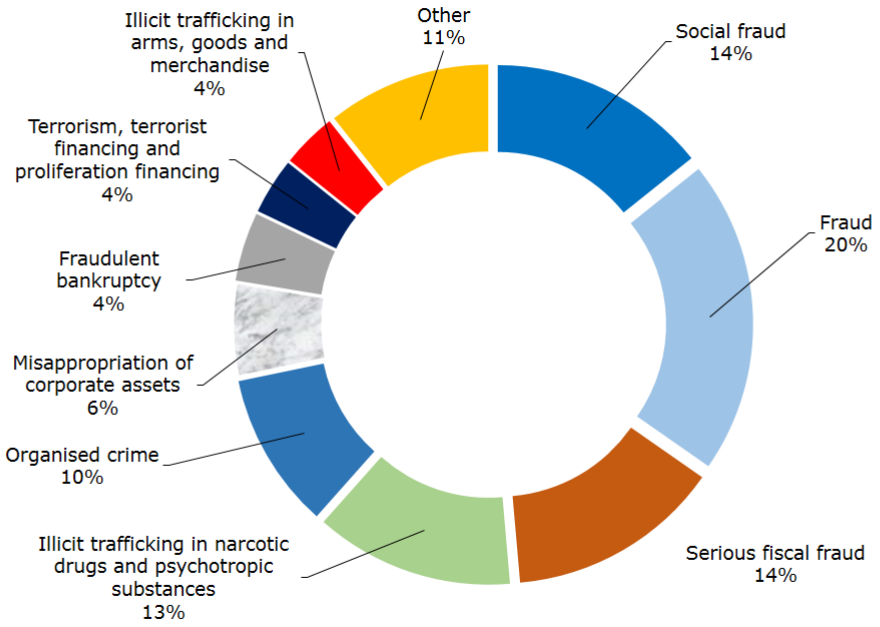
Origin of the funds	Amounts (million EUR)	%	Destination of the funds	Amounts (million EUR)	%
Luxembourg	162,78	32,70	United Arab Emirates	34,93	11,41
Switzerland	88,7	17,82	Portugal	30,43	9,94
Hong Kong	39,44	7,92	China	28,19	9,21
France	28,89	5,80	Monaco	27,13	8,86
Israel	23,41	4,70	Bangladesh	25,61	8,36
Netherlands	18,23	3,66	Germany	21,87	7,14
United Arab Emirates	17,31	3,48	Luxembourg	40,22	13,14
Portugal	12,94	2,60	Netherlands	17,32	5,66
Bahamas	12,02	2,41	Bulgaria	15,83	5,17
Monaco	10,33	2,08	Hong Kong	11,26	3,68
Democratic Republic of the Congo	10,27	2,06	Poland	8,73	2,85
Côte d'Ivoire	9,21	1,85	Turkey	7,36	2,40
Mauritius	7,15	1,44	Malta	5,28	1,72
Germany	5,07	1,02	France	5,09	1,66
Spain	5,04	1,01	Hungary	3,05	1,00
Liechtenstein	4,74	0,95	Switzerland	2,57	0,84
Guernsey	4,55	0,91	Romania	2,28	0,74
United Kingdom	4,32	0,88	Slovakia	1,82	0,59
Other	33,37	6,71	Other	17,22	5,63
	497,77	**100**		**306,19**	**100**

3.4. Files disseminated to the judicial authorities by main predicate offence

Number of files disseminated to the judicial authorities by main predicate offence

Predicate offence	2018	2019	2020	% 2020
Fraud	154	210	251	20,44
Social fraud(1)	137	197	175	14,25
Serious fiscal fraud	118	99	171	13,93
Illicit trafficking in narcotic drugs and psychotropic substances	119	119	159	12,95
Organised crime	75	103	125	10,18
Misappropriation of corporate assets	55	64	72	5,86
Fraudulent bankruptcy	63	57	55	4,48
Terrorism, terrorist financing and proliferation financing	48	57	45	3,66
Illicit trafficking in arms, goods and merchandise	40	46	44	3,58
Breach of trust	24	27	31	2,52
Trafficking in human beings²	20	17	27	2,20
Exploitation of prostitution	27	24	22	1,79
Smuggling of human beings	17	13	16	1,30
Embezzlement and corruption	15	10	11	0,90
Theft or extortion	9	12	10	0,81
Other	12	10	14	1,15
Total	**933**	**1.065**	**1.228**	**100**

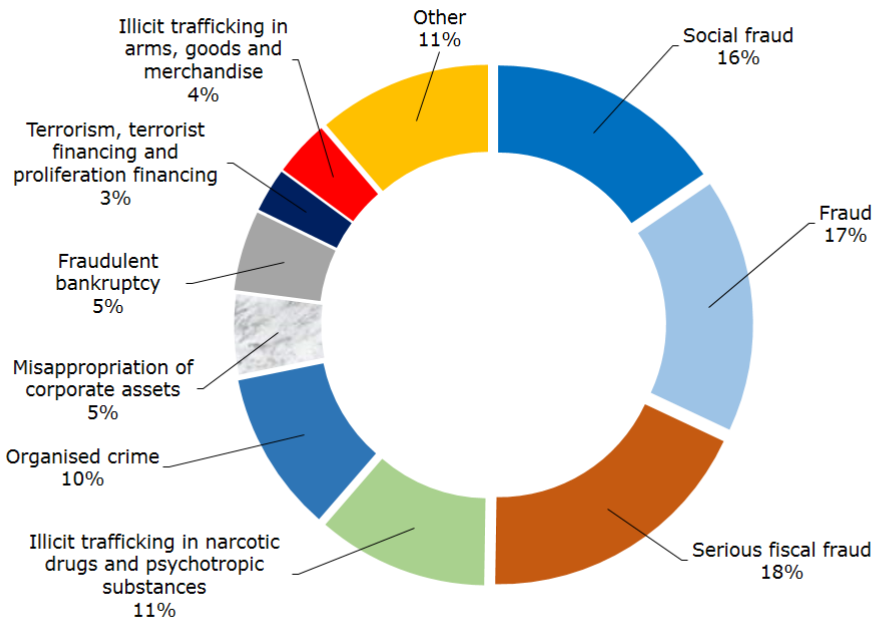
(1) Since the Law of 18 September 2017 entered into force.



Number of files disseminated by CTIF-CFI to the judicial authorities in 2020 according the main, second and third most important predicate offence

In one same file CTIF-CFI may have serious indications of money laundering related to one or more predicate offences. CTIF-CFI can also identify one main predicate offence and one or more other predicate offences.

Offence	Total 2020	Main offence	Second offence	Third offence
Social fraud	256	175	68	13
Fraud	273	251	19	3
Serious fiscal fraud	302	171	115	16
Illicit trafficking in narcotic drugs and psychotropic substances	184	159	22	3
Organised crime	173	125	42	6
Misappropriation of corporate assets	86	72	13	1
Fraudulent bankruptcy	86	55	23	8
Terrorism, terrorist financing and proliferation financing	47	45	2	0
Illicit trafficking in arms, goods and merchandise	60	44	11	5
Exploitation of prostitution	35	22	11	2
Breach of trust	40	31	8	1
Trafficking in human beings	33	27	5	1
Theft or extortion	17	10	7	0
Smuggling of human beings	23	16	7	0
Embezzlement and corruption	15	11	3	1
Other	24	14	9	1
Total	**1.654**	**1.228**	**365**	**61**



Amounts in files disseminated to the judicial authorities by main type of predicate offence (1)

Predicate offence	2018	2019	2020	% 2020
Serious fiscal fraud	573,41	311,87	704,10	43,03
Illicit trafficking in arms, goods and merchandise	180,97	299,71	148,23	9,06
Social fraud	169,17	228,42	219,85	13,43
Organised crime	112,23	151,09	226,21	13,82
Fraud	75,49	61,05	61,70	3,77
Misappropriation of corporate assets	22,30	30,49	16,33	1,00
Embezzlement and corruption	19,85	18,65	36,88	2,25
Fraudulent bankruptcy	24,94	16,98	34,14	2,09
Illicit trafficking in narcotic drugs and psychotropic substances	29,03	11,51	47,61	2,91
Breach of trust	16,46	7,77	33,73	2,06
Exploitation of prostitution	5,87	4,66	4,06	0,25
Terrorism, terrorist financing and proliferation financing	10,89	4,05	6,49	0,40
Trafficking in human beings	120,74	3,77	6,38	0,39
Smuggling of human beings	4,50	2,56	3,93	0,24
Theft or extortion	1,69	1,33	3,14	0,19
Other	65,19	4,75	83,71	5,11
Total	**1.432,73**	**1.158,66**	**1.636,49**	**100**

(1) Amounts in million EUR.

Disclosures in the files disseminated to the judicial authorities in 2018, 2019 and 2020 by predicate offence

	2018		2019		2020	
Predicate offence	**Number**	**Amount(1)**	**Number**	**Amount(1)**	**Number**	**Amount(1)**
Social fraud	335	184,52	520	305,71	464	291,73
Fraud	452	85,51	485	66,83	547	77,50
Organised crime	385	162,30	467	249,70	364	286,65
Serious fiscal fraud	309	694,84	260	386,74	364	746,99
Illicit trafficking in narcotic drugs and psychotropic substances	383	31,68	242	13,79	306	59,07
Terrorism, terrorist financing and proliferation financing	202	14,10	168	4,58	113	7,12
Illicit trafficking in arms, goods and merchandise	137	188,25	162	355,36	123	158,50
Fraudulent bankruptcy	145	33,96	141	22,34	107	36,42
Misappropriation of corporate assets	101	30,16	140	33,95	116	18,94
Trafficking in human beings	70	122,34	132	4,43	46	6,51
Breach of trust	74	21,82	57	9,79	63	37,21
Exploitation of prostitution	113	7,44	56	5,30	52	4,23
Embezzlement and corruption	98	20,55	36	30,96	30	37,98
Smuggling of human beings	43	3,52	23	2,57	24	4,52
Theft or extortion	14	1,82	18	7,09	12	3,14
Trafficking in illegal workers	82	32,47	11	4,03	-	-
Other	29	65,61	27	35,66	34	108,80
Total	**2.972**	**1.700,89**	**2.945**	**1.538,83**	**2.765**	**1.885,31**

(1) Amounts in million EUR.

3.5. Nationality of the main person involved in files disseminated to the judicial authorities

The table below provides the breakdown by nationality of the main person involved in the files disseminated to the judicial authorities in 2018, 2019 and 2020.

The lockdown from March onwards, the fact that the borders were closed for most of the year, the sharp drop in travel and the health crisis as a result of COVID-19 are clearly reflected in the nationalities of the main persons involved in the files disseminated to the judicial authorities.

In 2020, nearly 94% of the main individuals involved were Belgian nationals, compared to just 65% in 2019. Other nationalities that often featured in 2018 and 2019 were barely or no longer identified in 2020.

Nationality	2018	2019	2020	% 2020
Belgian	572	651	1.151	93,73
French	27	29	12	0,98
Dutch	48	26	6	0,49
German	3	2	5	0,41
Romanian	38	42	4	0,33
British	7	2	3	0,24
Congolese (Democratic Republic of the Congo)	8	5	3	0,24
Italian	11	20	3	0,24
Hungarian	5	3	2	0,16
Portuguese	22	59	2	0,16
Turkish	11	23	2	0,16
Albanian	9	10	1	0,08
Cameroonian	3	4	1	0,08
Ghanaian	-	2	1	0,08
Ivorian	-	-	1	0,08
Moroccan	11	9	1	0,08
Nigerian	5	7	1	0,08
Polish	7	3	1	0,08
Spanish	6	10	1	0,08
Thai		2	1	0,08
Afghan	-	1	-	-
Algerian	-	1	-	-
Angolan	-	1	-	-
Armenian	-	1	-	-
Austrian	-	1	-	-
Bosnian	-	1	-	-
Brazilian	15	16	-	-
Bulgarian	10	12	-	-
Chinese	-	2	-	-
Guinean	4	-	-	-
Indian		3	-	-
Iraqi	5	1	-	-
Israëli	-	7	-	-
Macedonian	-	2	-	-

Pakistani	4	4	-	-
Russian	8	3	-	-
Swedish	3	-	-	-
Syrian	-	9	-	-
Tunisian	-	2	-	-
Other	91	89	26	2,14
Total	**933**	**994**	**1.228**	**100**

3.6. Residence of the main person involved

The tables below provide the breakdown by place of residence of the main person involved in the files disseminated to the judicial authorities in 2020. These tables are intended to help disclosing entities apply the statutory compliance measures.

3.6.1. Residence in Belgium

The table below provides the breakdown for the 1.151 files disseminated to the judicial authorities in which the main person involved resided in Belgium.

	Number of files	%
Brussels	340	29,54
Antwerp	220	19,11
Oost-Vlaanderen	114	9,90
Hainaut	69	5,99
West-Vlaanderen	72	6,26
Limburg	70	6,08
Halle-Vilvoorde	99	8,60
Liège	60	5,21
Brabant wallon	26	2,26
Vlaams-Brabant	45	3,91
Namur	22	1,91
Luxembourg	14	1,23
Total	**1.151**	**100**

3.6.2. Residence abroad

The table below presents the breakdown for the 77 files disseminated to the judicial authorities in 2020 in which the main individual involved resided abroad.

Country of residence	2020	%
France	12	15,58
Netherlands	6	7,79
Luxembourg	6	7,79
Germany	5	6,49
Romania	4	5,19
Monaco	4	5,19
Italy	3	3,90
United Kingdom	3	3,90
Democratic Republic of the Congo	3	3,90
Turkey	2	2,60
Switzerland	2	2,60
Hungary	2	2,60
Portugal	2	2,60
Albania	1	1,30
Burkina Faso	1	1,30
China	1	1,30
Cyprus	1	1,30
Dominican Republic	1	1,30
Ghana	1	1,30
Gibraltar	1	1,30
Côte d'Ivoire	1	1,30
Cameroon	1	1,30
Lithuania	1	1,30
Morocco	1	1,30
Nigeria	1	1,30
Poland	1	1,30
Spain	1	1,30
Thailand	1	1,30
United States	1	1,30
Other	7	9,07
Total	**77**	**100**

4. INTERNATIONAL COOPERATION

As the statistics below indicate, this year CTIF-CFI again sent several requests abroad and also received numerous requests from counterpart FIUs in European or third countries. The statistics with regard to international cooperation are listed below.

The operational cooperation with foreign FIUs is usually based on written agreements between different FIUs (MOU or Memorandum of Understanding). Sometimes requests for information are sent to FIUs with which no MOU has been signed when this is useful for operational purposes and when the exchanged information is protected by strict confidentiality[43]. It should nevertheless be stressed that information is always exchanged in a secure way. The exchanged information may never be used without prior consent of the FIU providing the information and permission is only granted on the basis of reciprocity.

The figures below with regard to the number of requests received from and sent to foreign FIUs not only refer to normal requests but also to spontaneous requests for information exchange. Spontaneous information exchange takes place when CTIF-CFI informs foreign FIUs that a file was disseminated and links were identified with the country of this foreign FIU, even if CTIF-CFI did not query the FIU beforehand. Conversely, CTIF-CFI sometimes received information from foreign FIUs on individuals with an address in Belgium who fell prey to fraud in the country of that FIU or with warnings[44] for specific fraud schemes. CTIF-CFI also considers this exchange of information to be spontaneous information exchange.

In 2020, CTIF-CFI received and processed 1.003 requests for assistance from counterpart FIUs[45].

Africa (8)
Democratic Republic of the Congo (1), Gabon (1), Ghana (1), Madagascar (1), Niger (1), Nigeria (1), Republic of the Congo (1), South Africa (1)

Americas (229)
Argentina (2), Bahamas (3), Brazil (1), Canada (1), Costa Rica (1), Ecuador (1), Panama (1), Peru (1), United States (218)

Asia Pacific (10)
Australia (2), India (7), Japan (1)

Eurasia (7)
Kyrgyzstan (5), Russia (2)

Europe (731)
Albania (1), Andorra (1), Austria (42), Azerbaijan (2), Bosnia and Herzegovina (3), Bulgaria (1), Croatia (3), Cyprus (4), Czechia (4), Denmark (1), Estonia (7), Finland (13), France (79), Georgia (3), Germany (82), Gibraltar (1), Greece (3), Guernsey (5), Hungary (9), Ireland (4), Isle of Man (3), Israel (4), Italy (12), Jersey (16), Latvia (5), Liechtenstein (13), Lithuania (14), Luxembourg (194), Macedonia (3), Malta (45), Moldova (1), Monaco (1), Montenegro (2), Netherlands (71), Norway (1), Poland (7), Portugal (2), Romania (15), Slovakia (6), Slovenia (2), Spain (5), Sweden (1), Switzerland (4), Turkey (3), United Kingdom (30), Vatican City State (1),

Middle East and North Africa (12)
Algeria (1), Kuwait (1), Lebanon (1), Morocco (7), Syria (1), Tunisia (1)

[43] Article 125 of the Law of 18 September 2017

[44] Warnings or information on money laundering techniques are published on CTIF-CFI's website or in its annual report.

[45] Grouped on the basis of the regional groups of the Egmont Group and the FATF (FSRBs).

In 2020, CTIF-CFI sent 992 requests for information to counterpart FIUs[46].

Africa (27)
Angola (1), Burkina Faso (1), Cameroon (2), Chad (1), Cote d'Ivoire (1), Gabon (3), Ghana (1), Malawi (1), Mali (1), Mauritius (2), Namibia (1), Niger (2), Senegal (3), Seychelles (1), South Africa (3), Tanzania (1), Togo (1), Uganda (1)

Americas (55)
Anguilla (1), Antigua and Barbuda (1), Argentina (2), Aruba (1), Bahamas (1), Barbados (1), Belize (1), Bermuda (1), Bolivia (1), Brazil (3), British Virgin Islands (3), Canada (6), Chili (1), Colombia (3), Costa Rica (2), Cuba (1), Curaçao (1), Ecuador (1), El Salvador (1), Grenada (1), Guatemala (1), Honduras (1), Jamaica (2), Cayman Islands (1), Mexico (1), Panama (1), Paraguay (1), Peru (1), Saint Kitts and Nevis (1), Saint Lucia (1), Saint Vincent and the Grenadines (1), Sint-Maarten (1), Trinidad and Tobago (1), Turks and Caicos (1), United States (5), Uruguay (1), Venezuela (1)

Asia-Pacific (62)
Afghanistan (1), Australia (4), Bangladesh (1), Brunei Darussalam (1), Cambodia (1), China (8), Fiji (1), Hong Kong (15), India (5), Indonesia (3), Japan (2), Macao (1), Malaysia (1), Marshall Islands (1), Mongolia (1), Nepal (1), New Zealand (1), Philippines (1), Samoa (1), Singapore (5), South Korea (1), Sri Lanka (2), Taiwan (2), Thailand (2)

Eurasia (15)
Belarus (1), Kazakhstan (2), Kyrgyzstan (1), Russia (9), Tajikistan (1), Uzbekistan (1)

Europe (781)
Albania (2), Andorra (1), Armenia (2), Austria (5), Azerbaijan (1), Bosnia and Herzegovina (1), Bulgaria (21), Croatia (2), Cyprus (7), Czechia (7), Denmark (2), Estonia (6), Finland (4), France (185), Georgia (4), Germany (63), Gibraltar (5), Greece (5), Guernsey (4), Hungary (10), Iceland (1), Ireland (4), Isle of Man (2), Israel (7), Italy (28), Jersey (2), Kosovo (1), Latvia (6), Liechtenstein (2), Lithuania (11), Luxembourg (49), Macedonia (2), Malta (13), Moldova (1), Monaco (7), Montenegro (1), Netherlands (115), Norway (5), Poland (13), Portugal (10), Romania (10), San Marino (1), Serbia (3), Slovakia (2), Slovenia (4), Spain (26), Sweden (2), Switzerland (21), Turkey (25), Ukraine (7), United Kingdom (62), Vatican City State (1)

Middle East and North Africa (59)
Algeria (2), Bahrain (1), Egypt (1), Jordan (3), Kuwait (1), Lebanon (6), Morocco (6), Qatar (2), Saudi Arabia (3), Syria (1), Tunisia (2), United Arab Emirates (23)

[46] Ibid.

5. JUDICIAL FOLLOW-UP

5.1 Judgments

CTIF-CFI is informed of the follow-up of cases by the Public Prosecutor's Offices and the Federal Public Prosecutor's Office. When a judgment is pronounced in a disseminated case then the Public Prosecutor sends a copy of this judgment to CTIF-CFI. The table and graph below were drawn up based on the judgments reported by the Public Prosecutor to CTIF-CFI. The table and graph contain the judgements pronounced in the past ten years in CTIF-CFI's files disseminated to the judicial authorities as well as before. This statistical approach of judgments over a period of ten years takes into account the potential long period between the dissemination of a file to the Public Prosecutor, the investigation and the delivery of the judgment, especially when parties appeal a decision of the court of first instance.

The table below provides an overview per judicial district of the 533 judgments pronounced in the files disseminated by CTIF to the judicial authorities in the last ten years.

	Fraud	Fiscal fraud	Fraudulent bankruptcy	Trafficking in narcotic drugs	Illicit trafficking	Organised crime	Misappropriation of corporate assets	Trafficking in human beings	Breach of trust	Prostitution	Illegal workers	FT	Theft or extortion	Trafficking in hormonal substances	Improper public offering of securities	Other	**Grand total**
Brussels	31	40	13	10	8	14	7	14	6	3	4	1			1	1	**153**
Antwerp	13	9	8	10	8	4	8	1	6	3			1	1		1	**73**
Gent	8	2	9	4	2		4	2		1					1	1	**34**
Tongeren	4	4	3	8	4		1		1	2			1				**28**
Brugge		1	2	3	5	2	1	4	3	2				1	1		**25**
Liège	5	2	2	4	1	3				2			1		1	1	**22**
Turnhout	4	4	1	4	1		2		1		1					1	**20**
Charleroi	3	6			2	2				1	5						**19**
Federal Public Prosecutor's Office	3	1		1		1		1			1	10				1	**19**
Hasselt	2	3	2	2		1	3	1	1	2						1	**18**
Mons	3	1	3		2	4	1				1						**15**
Kortrijk	3	2	4	4												1	**14**
Leuven		1	4	3		1	2	1									**12**
Dendermonde	3		2	2		1							2			1	**11**
Tournai	4	1	1	1				2			1						**10**
Mechelen	1	1	2	2					2				1				**9**
Namur	1	1	2		3				1								**8**
Neufchâteau	4			1	1	1											**7**
Nivelles	1		1		2		1		1				1				**7**
Verviers	2			1			1	1			1						**6**
Ieper				1				1	2							1	**5**
Oudenaarde		2					2							1			**5**
Huy	1		1		1												**3**
Marche-en-Famenne					2		1										**3**
Veurne			2		1												**3**
Dinant					1									1			**2**
Halle-Vilvoorde	1												1				**2**
Grand total	**97**	**81**	**62**	**61**	**44**	**34**	**34**	**28**	**24**	**16**	**14**	**11**	**8**	**4**	**4**	**11**	**533**

5.2. Judicial follow-up – fines and confiscations

The table[47] below provides an overview of the fines and confiscations imposed by courts and tribunals, (amounts in EUR) in files disseminated to the judicial authorities in the past ten years (2011 to 2020) and of which CTIF-CFI was informed. When examining these figures it should be noted that for a large number of files securing evidence may take longer than ten years. This is the case for files related to economic and financial crime, which account for more than 50% of the files disseminated by CTIF-CFI. Moreover, for some decisions an appeal was lodged.

	Fines 2011 to 2020	Confiscations 2011 to 2020	Total
Brussels	€ 7.752.435	€ 80.211.021	€ 87.963.456
Antwerpen	€ 23.987.777	€ 73.550.343	€ 97.538.120
Antwerpen	€ 1.601.931	€ 63.030.460	€ 64.632.391
Turnhout	€ 569.953	€ 10.519.883	€ 11.089.836
Mechelen	€ 0	€ 0	€ 0
Hainaut	€ 1.580.705	€ 120.738.500	€ 122.319.205
Mons	€ 653.180	€ 116.745.440	€ 117.398.620
Tournai	€ 25.750	€ 374.932	€ 400.682
Charleroi	€ 901.775	€ 3.618.128	€ 4.519.903
Oost-Vlaanderen	€ 995.678	€ 36.584.348	€ 37.580.026
Gent	€ 438.365	€ 9.135.416	€ 9.573.781
Dendermonde	€ 493.163	€ 27.439.504	€ 27.932.667
Oudenaarde	€ 64.150	€ 9.428	€ 73.578
West-Vlaanderen	€ 522.213	€ 6.255.210	€ 6.777.423
Brugge	€ 500.763	€ 3.637.949	€ 4.138.712
Veurne	€ 15.950	€ 2.363.310	€ 2.379.260
Ieper	€ 5.500	€ 253.951	€ 259.451
Kortrijk	€ 0	€ 0	€ 0
Limburg	€ 261.262	€ 5.087.589	€ 5.348.851
Hasselt	€ 188.656	€ 4.748.841	€ 4.937.497
Tongeren	€ 72.606	€ 338.748	€ 411.354
Liège	€ 38.500	€ 2.863.233	€ 2.901.733
Liège	€ 5.500	€ 2.862.571	€ 2.868.071
Huy	€ 33.000	€ 0	€ 33.000
Verviers	€ 0	€ 662	€ 662

[47] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 31 January 2021 and that were spontaneously sent to CTIF-CFI in accordance with Article 82 § 3.

Namur	€ 172.771	€ 3.006.508	€ 3.179.279
Namur	€ 25.275	€ 2.741.653	€ 2.766.928
Dinant	€ 147.496	€ 264.855	€ 412.351
Brabant Wallon	€ 17.750	€ 228.062	€ 245.812
Leuven	€ 4.957	€ 160.508	€ 165.465
Eupen	€ 0	€ 0	€ 0
Luxembourg	€ 0	€ 0	€ 0
Neufchâteau	€ 0	€ 0	€ 0
Arlon	€ 0	€ 0	€ 0
Marche-en-Famenne	€ 0	€ 0	€ 0
Total	**€ 35.334.048**	**€ 328.685.322**	**€ 364.019.370**

BELGIAN FINANCIAL INTELLIGENCE PROCESSING UNIT

Gulden Vlieslaan 55, bus 1 – 1060 Brussel – Belgium
Avenue de la Toison d'Or 55, boîte 1 – 1060 Bruxelles – Belgium

Phone: +32 (0)2 533 72 11 – Fax: + 32 (0)2 533 72 00

Email: info@ctif-cfi.be – http://www.ctif-cfi.be/

Published by
Philippe de KOSTER
Gulden Vlieslaan 55, bus 1 – 1060 Brussel – Belgium
Avenue de la Toison d'Or 55, boîte 1 – 1060 Bruxelles – Belgium

Additional information on this report and statistics can be obtained by sending a written request to info@ctif-cfi.be.