ctif cfi

ANNUAL REPORT

Belgian Financial Intelligence Processing Unit

2021

TABLE OF CONTENTS

I. PREFACE

PREFACE BY THE DIRECTOR OF THE FINANCIAL PROCESSING UNIT CTIF-CFI

Mr Philippe de KOSTER

After having been affected for two years and a half by the COVID-19 health crisis, we are now facing a war on Europe's doorstep. The very least we can say is that we are living in a world that is becoming increasingly uncertain.

Despite all of this, the mechanisms for the prevention of money laundering and terrorist financing have worked and the results presented in this annual report 2021 prove this.

Upon the publication of this report I would again like to thank all members of staff, the liaison officers and all our preferential partners (judicial authorities, federal police, FPS Economy,…) for the work they did in 2021, often in difficult circumstances including working from home orders and minimal presence at the office. Especially since the number of disclosures continued to rise sharply in 2021. CTIF-CFI received a record number of 46.330 disclosures, which is an increase of almost 50 % compared to 2020.

Several British payment institutions set up a company in Belgium in order to operate under the freedom to provide services, which may explain a large part of this increase. Awareness of the financial sector and "lookback" operations requested by the National Bank definitely also provide an explanation for this rise.

Given that CTIF-CFI receives such disclosures, it must constantly find a balance between "looking back at the past" and finding a more effective way of approaching money laundering aimed at the future and new money laundering risks such as those linked to the use of cryptocurrencies.

Tools for prioritising and orientating disclosures, which have been used by CTIF-CFI for a number of years and are constantly being improved, have enabled us to deal with this massive surge in new disclosures, without having to secure additional financial resources at present.

1.241 new files were disseminated to the Belgian judicial authorities. A thousand notifications of useful information were sent to administrative authorities of the State (the unit Antifraud Coordination CAF, the Social Intelligence and Investigation Service SIRS-SIOD, FPS Economy, etc.) and to the supervisory authorities in accordance with Articles 83 and 121 of the Law of 18 September 2017.

The IT tools developed by FIU.Net and by CTIF-CFI have also made it possible to disseminate 8.021 XBR (Cross-Border Reports) and 613 XBD (Cross-Border Dissemination Reports) regarding transactions involving another European Member State (cf. Section V.4.).

In accordance with the fourth AML/CFT Directive, when CTIF-CFI receives a disclosure regarding another country, it shall send for analysis, all relevant information in the disclosure to the Financial Intelligence Unit (FIU) of the country in question. These notifications do not replace the current procedure of information exchange upon request or spontaneous exchange, however, which is usually carried out during or at the end of the analysis of a file, but completes this procedure.

Generally speaking some 15.000 items of intelligence received by CTIF-CFI from reporting entities are disseminated to external parties in one way or another, either to the judicial authorities, administrative services of the State, intelligence services (including OCAM-OCAD), AML/CFT supervisory authorities and counterpart FIUs. The information that cannot be disseminated to external parties forms an essential base, which can be used for the purposes of strategic analysis, but also for a potential dissemination in the future if any serious indications of money laundering or terrorist financing would subsequently be identified.

Although there is little change in criminal phenomena and money laundering and terrorist financing techniques, there is growing evidence that the laundered funds are the proceeds of polycriminal activities. Over the past year, a large number of cases have shown how social fraud, serious fiscal fraud and organised crime increasingly feature as interrelated issues.

CTIF-CFI has also identified an increased professionalization of money laundering as such and works tirelessly to raise awareness of this issue among its partners as well as the risks of such an evolution for the rule of law and society as a whole.

Extremely well-structured organisations that operate internationally provide their “money laundering services” to various other high-level criminal organisations involved in various illegal activities (drug trafficking, gangsters, human traffickers, international fraudsters, etc.) that generate huge profits (mainly in cash). Alarmingly, CTIF-CFI has found that these money laundering networks have anchored part of their activities in Belgium, by using a very large number of bank accounts, front companies and front men.

Finally, I would like to stress the efforts made and the significant resources put in place in 2021 by the European Commission (DG FISMA) to ensure the transfer of the secure communication system for European FIUs, FIU.Net, from Europol to the European Commission’s infrastructure, while maintaining the decentralised nature of the system as was the case in the past. This transfer was the start of the development of a modernised FIU.Net, in order to increase the effectiveness of the tools for the prevention of money laundering and terrorist financing and to adapt them to new threats.

The new “AML package” was announced by DG FISMA in June 2021 and subsequently discussed at Council level and this package is now starting to take shape. The main aim is to improve the fight against money laundering and terrorist financing through preventive measures applicable in a uniform manner in all Member States. It will include the creation of an Anti-money Laundering Authority (AMLA), which will of course involve European FIUs.

The AML Package will undoubtedly have a significant impact on the preventive AML/CFT framework, but also on the organisation and future architecture of the system for the prevention of money laundering and terrorist financing in Belgium.

That is why I have asked the Director-General of DG FISMA, Mr John Berrigan, to contribute to CTIF-CFI’s annual report of 2021. I thank him for accepting this request.

I hope you enjoy reading the report.

Philippe de KOSTER
Director

FOREWORD OF THE DIRECTOR-GENERAL OF THE EUROPEAN COMMISSION'S DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION

Mr. John BERRIGAN

The past two years have brought a series of challenges to the European Union (EU). The COVID-19 pandemic forced us to change our ways of living, with an increased reliance on digitalisation in our daily lives. Russia's military aggression against Ukraine is a reminder that we should take nothing, including international peace, for granted. In this context, the fight against 'dirty money' becomes all the more important.

Money laundering and terrorist financing pose a clear and present threat not just to the financial system, but to society as a whole. The scale of the problem cannot be underestimated and we must do our utmost to close the loopholes that criminals can exploit. We have made huge strides in recent years and our EU rules on anti-money laundering and countering the financing of terrorism (AML/CFT) are among the toughest in the world. However, the rules must be applied consistently and closely supervised to have the necessary impact on malicious actors, such as criminals and terrorists, who are trying to abuse the financial system.

In July 2021, the European Commission proposed an ambitious policy package, which revamps the EU's AML/CFT framework. The package consists of four legislative proposals:

- A proposal for a Regulation establishing a new EU AML/CFT authority (AMLA) which will transform AML/CFT supervision in the EU and enhance cooperation among Financial Intelligence Units (FIUs). AMLA will enable FIUs to improve their analytical capacity around illicit financial flows and turn financial intelligence into a key source for law enforcement agencies;
- A proposal for a 6th Anti-money Laundering Directive (AMLD6), replacing the existing Directive and containing rules on national supervisors and FIUs;
- A proposal for an AML/CFT Regulation, containing directly applicable rules, including in the areas of customer due diligence and beneficial ownership;
- A revision of the 2015 Regulation on Transfers of Funds to trace transfers of crypto-assets.

The package significantly strengthens our efforts to stop the laundering of dirty money through the financial system. Essentially, the new framework that we propose will enable CTIF-CFI and its counterparts from other EU Member States to analyse information on suspicious transactions and activities more effectively, conduct joint analysis of cross-border suspicious activities more efficiently and exchange information more swiftly.

When speaking of the swift and effective exchange of information, I have to mention the FIU.net system. In addition to proposing an ambitious legislative package, last year we also managed to successfully transfer the FIU.net system from Europol to the Commission, thereby ensuring that FIUs have the communication channel to exchange information and cross-match data. The FIU.net advisory group, chaired by CTIF-CFI, played an indispensable role in this exercise and this transfer would have not been possible without the great level of cooperation between the Commission and the advisory group, led by CTIF-CFI.

On behalf of all colleagues from the Commission, I would like to wish CTIF-CFI another very successful year in the fight against money laundering, its predicate offences and terrorist financing. I sincerely hope that we will continue to work together as effectively as we did in 2021.

John BERRIGAN
Director-General

II. COMPOSITION OF CTIF-CFI

From 2 February 2022 onwards

Director:	Mr	Philippe de KOSTER
Vice-President:	Mr	Fons BORGINON
Deputy Directors:	Mr	Christophe REINESON
	Mr	Bart VAN HULST
Members:	Ms	Chantal DE CAT
	Mr	Jean-François VANDERMEULEN
	Mr	Philippe GARZANITI
	Mr	Benoit WOLTER
Secretary-General:	Mr	Kris MESKENS

Until 2 February 2022

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

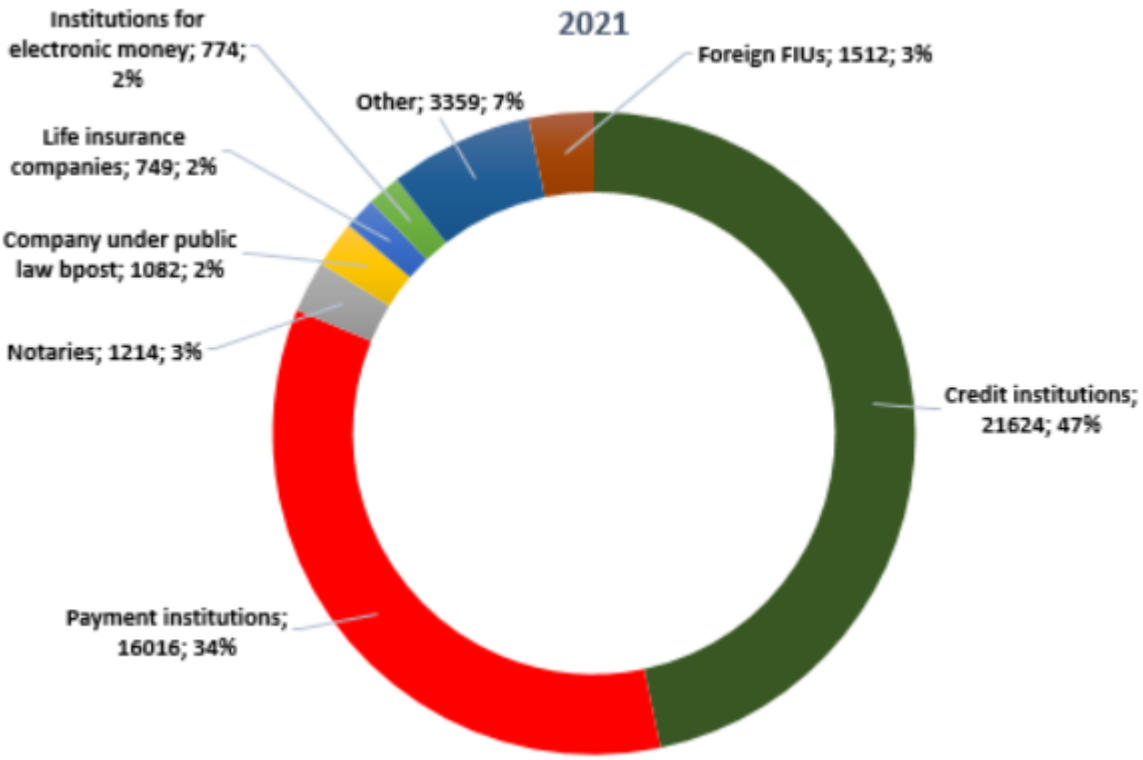
III. KEY FIGURES 2021

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[1], from foreign FIUs as part of international cooperation and from other services of the State, as referred to in the Law.

In 2021, CTIF-CFI received a total of 46.330 notifications of information (disclosures of suspicious transactions, information from foreign counterparts and services of the State), which were grouped into 35.605 new cases and 10.725 additional notifications of information in cases that had previously been opened.

	2021	%
Total number	46.330	100
New cases	35.605	76
Additional information	10.725	24

Most of the disclosures originate from credit institutions, from payment institutions, from the company under public law bpost, from institutions for electronic money, from notaries and from life insurance companies.



Since 2021 the contents of a large part of the disclosures (22%), mainly received from payment institutions approved to operate in Belgium under the freedom to provide services in the European Union has been externalised to counterpart FIUs (automatic exchange, spontaneous exchange and exchange upon request).

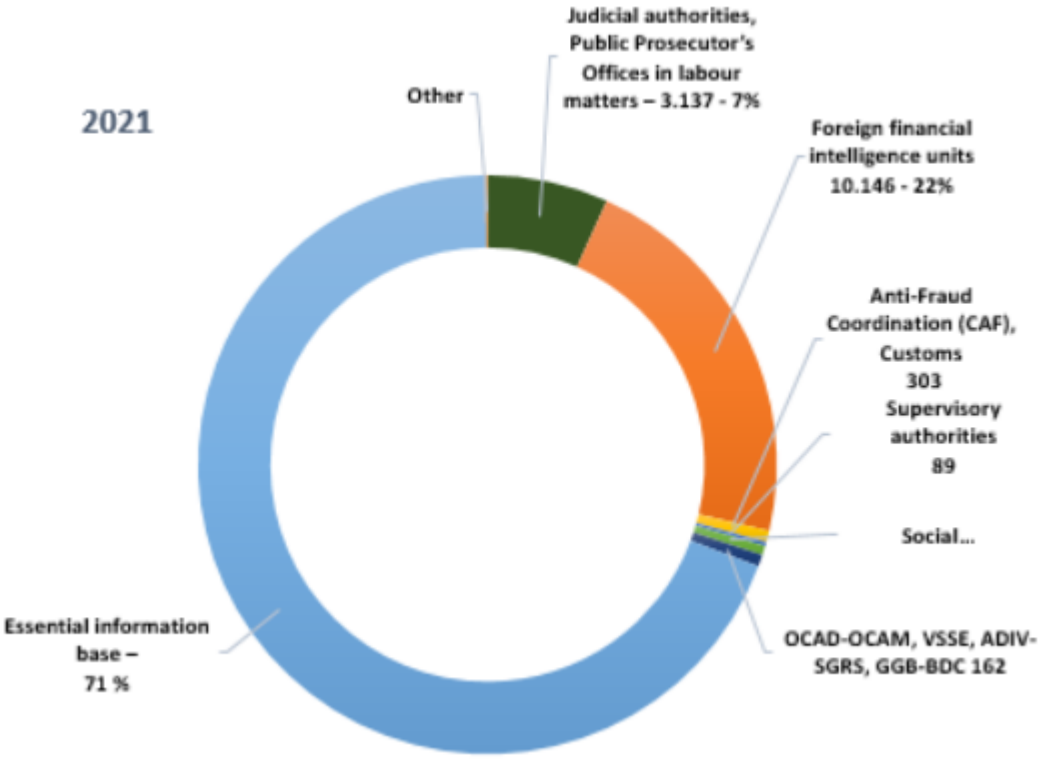
[1] Hereinafter referred to as the Law of 18 September 2017. Belgian Official Gazette of 6 October 2017 – Chamber of Representatives (www.lachambre.be) Documents: 54-2566.

The remaining disclosures and information received are analysed and enriched and in case of serious indications of money laundering or terrorist financing or financing of proliferation, CTIF-CFI disseminates the result of its analysis to the judicial authorities (7%).

CTIF-CFI is also obliged to share information with other competent authorities in Belgium, with the civil and military intelligence services, with the Coordination Unit for Threat Analysis OCAM-OCAD and with the supervisory authorities of the obliged entities[2].

Moreover, CTIF-CFI always informs the Central Office for Seizure and Confiscation (OCSC-COIV) when assets of significant value, of any nature, are available for potential judicial seizure.

The information received that cannot be externalised by CTIF-CFI, is not lost however, this information is an essential information base, available for purposes of strategic analysis, as well as future analysis by the operational department when new relevant information (police information, new judicial information, etc.) would make it possible to subsequently to establish a link to money laundering or terrorist financing.



A detailed overview of the statistics of 2021 is included in part V.

[2] The unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance when the dissemination 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; the Customs and Excise Administration when the dissemination to the Public Prosecutor contains information regarding laundering the proceeds of offences for which the Customs and Excise Administration conducts criminal proceedings; the supervisory authorities of obliged entities and the FSMA and the Federal Public Service Economy when the dissemination to the Public Prosecutor contains information regarding laundering the proceeds of an offence for which these authorities have investigative and/or supervisory powers; the Social Intelligence and Investigation Service (SIRS-SIOD) when the dissemination 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 dissemination to the Public Prosecutor contains information regarding laundering the proceeds of smuggling of human beings or trafficking in human beings.

IV. MONEY LAUNDERING AND TERRORIST FINANCING TRENDS

Money laundering trends

1. Main threats

1.1. Trafficking in narcotic drugs

Trends identified

In 2021, as in previous years, a record amount of drugs was seized in Belgium. In the port of Antwerp alone, more than 89 tonnes of cocaine were intercepted, a sharp rise compared to 2020 (65 tonnes), which was also a record year. Significantly larger amounts of cocaine, cannabis, synthetic drugs and heroin were seized in 2021 in the rest of Belgium.

This spectacular increase in seizures of drugs is partly the result of the information brought to light in the investigation into Sky ECC, the Canadian provider of an encrypted communication network. Based on messages from Sky ECC, dozens of news drug investigations were started all over Belgium or ongoing investigations were able to be relaunched.

The total street value of the drugs seized in 2021 alone easily reaches more than EUR 10 billion. Even if we assume that thanks to cracking the secured communication within the criminal organisations a larger part of the total trade was intercepted, the criminal flows of money from drug trafficking in Belgium worth billions of EUR are enormous.

The fact that these enormous amounts are at least partly laundered via Belgium, has made laundering the proceeds of trafficking in narcotic drugs one of CTIF-CFI's most important operational and strategic priorities, as it has been for years. Trafficking in narcotic drugs is often linked to other money laundering predicate offences such as corruption, fiscal and social fraud and organised crime. So figures regarding the dissemination of files to the Public Prosecutor's Office related to laundering the proceeds of trafficking in narcotic drugs –which have remained stable in 2021 compared to 2020- only provide a partial view of the issue. The main files related to trafficking in narcotic drugs were disseminated to the judicial authorities for "organised crime" because criminal organisations involved in drug trafficking use professional money laundering networks. The number of files and related amounts in which serious indications of laundering the proceeds of organised crime were identified has risen compared to 2020.

Files related to intermediary trade

In general CTIF-CFI has identified two types of files in which proceeds of drug trafficking are laundered. Firstly, the files related to intermediary trade or direct trade in Belgium. These individuals reside in Belgium and launder their proceeds of drug trafficking through local activities. Amounts up to EUR 500.000 a year can be identified in these files, these proceeds are deposited in cash on accounts.

In smaller cases natural persons carry out cash deposits that cannot be explained by official sources of income. In a number of files money was transferred to online gaming sites, winnings were subsequently paid out to accounts with other financial institutions, in order to provide an explanation for their origin.

Usually companies in cash-intensive industries are used, so income from professional activities can be mixed with proceeds of drug trafficking. The (second-hand) car industry is a sector that is often identified. The value of second-hand cars is not easy to determine objectively. In Germany cars can still be purchased in cash, even for large amounts.

The hospitality industry is another sector targeted by criminals involved in drug trafficking. The large wave of bankruptcies and potential sell-out to criminals, which was feared as a result of the COVID-19 crisis has not materialised based on CTIF-CFI's experience.

Various types of businesses are also used to launder the proceeds of drug trafficking. The cash deposits on the company's accounts are not proportionate to the assumed turnover. Despite extensive action taken in the past, night shops are still often involved in money laundering operations. Apart from the involvement in drug trafficking, social fraud and fiscal are also identified.

Finally, several files were disseminated to the judicial authorities in 2021 that featured real estate transactions and the funds for these transactions were linked to cannabis plantations in houses. Either a property was purchased in order to house a plantation, or the income from the plantation was used to invest in real estate. In both cases irregularities regarding the purchase transaction and the profile of the individuals involved resulted in the initial disclosure.

Files related to professional money laundering networks

A second type of file is of much larger magnitude and is part of the most important money laundering trend in recent years, i.e. professional money laundering networks operating on an international scale. These money laundering networks offer their financial services for various criminal activities such as the exploitation of undeclared workers, fraud, fiscal fraud but especially drug trafficking. They use corporate structures in several countries that are ready to receive the cash, originating from drug trafficking for instance, but can also supply cash using the offsetting technique, to pay undeclared workers for instance. Initially these networks were mainly aimed at social fraud involving Brazilian or Portuguese entities, hence why the name "Brazilian networks" is still often used. By now the networks have evolved and although front men -who manage these companies- are still often Portuguese or Brazilian nationals, the activities are no longer limited to laundering the proceeds of undeclared work in the construction industry.

CTIF-CFI had a strong suspicion in recent years that these networks were used to process drug money, given the enormous amounts transferred between the companies' accounts. Information from the investigation into Sky ECC and the similar system Encrochat that had been cracked previously confirmed this suspicion. Messages were intercepted in which the account numbers of companies in the money laundering network were exchanged between key figures of the drug trafficking. This link between the trafficking on the one hand and money laundering on the other was difficult to establish, given that front men were always used for the companies and the organisers of the money laundering system were never directly involved in the drug operations themselves.

The amounts in the files related to laundering the proceeds of drug trafficking through professional money laundering networks add up to tens of millions EUR.

The large quantities of cash are partly used directly to pay undeclared workers. Using fake invoices the money is then transferred to accounts of the network of companies. Yet the amount of money that has to be laundered is too large for the offsetting technique alone, so part of the money is also deposited in cash on the different accounts of the numerous companies involved. Subsequently the funds are transferred between the companies and fake invoices are used as a justification for the financial flows. Some companies do carry out actual activities in the construction industry, services or (international) trade. In the last phase the money is invested to the benefit of the ordering party. This could involve luxury consumer goods such as cars, watches or boats but also real estate or commercial goods. To further conceal the origin of the money for these investments and their total amount in the invoices are paid by multiple companies in the network. In one file a car was purchased in Germany by three companies conducting a range of activities who each paid part of the 80.000 EUR purchasing price, and made reference to the same chassis number and invoice number.

Challenges

The main challenges to detect these money laundering networks, which are able to almost completely eliminate the link between the criminal activities and their proceeds, are the complexity and the international nature of the operations. Hundreds of companies are involved in a large number of countries, combining legal and illegal activities. Trade-based money laundering and fiscal fraud are used to make criminal money even more profitable.

International cooperation is absolutely essential to be able to combat these professional money laundering networks effectively. Many vulnerabilities regarding questionable incoming financial flows have been identified in certain countries. The FATF recently listed the United Arab Emirates on the list of countries requiring enhanced due diligence. CTIF-CFI's experience shows that not only drug traffickers find refuge in the United Arab Emirates but that some organisers of professional money laundering networks are established there, especially in Dubai.

Finally, the evolution regarding virtual assets will be monitored closely in the future in the context of tackling the proceeds of drug trafficking. Although this is not yet apparent in the cases, there are indications that criminal organisations involved in drug trafficking in the Netherlands and Belgium focus on cryptocurrencies to launder part of their proceeds. In Europe providers of cryptocurrencies are subject to the preventive anti-money laundering system, but this is not the case everywhere, or the rules are not applied consistently. It is therefore not unlikely that criminal organisations would use crypto-assets to carry out payments to countries from where the cocaine originated and launder the proceeds of this drug trafficking.

Action taken

Apart from international cooperation CTIF-CFI also focusses on cooperation with the police to analyse and prosecute the financial aspects of drug trafficking in Belgium. This involves operational as well as strategic cooperation, and information is exchanged in specific cases and as part of projects aimed at tackling drug trafficking.

In 2021 the exchange of information between CTIF-CFI and the police was strengthened in the framework of the investigation into SkyECC. The police's input is of great importance to CTIF-CFI because the investigations provide an insight into the key players involved in organised crime and drug trafficking in Belgium. By linking financial data from disclosures to the main individuals involved CTIF-CFI can help reveal the financial aspect of the criminal organisations and make a valuable contribution to the investigation through its financial expertise.

1.2. Organised crime, social fraud and serious fiscal fraud

Trends identified

Interaction between different criminal networks

The various types of criminal activities that criminals are involved in are part of the elements that make up the concept of organised crime. Organised crime has many aspects that are revealed through polycriminal activities.

Many criminal groups have become increasingly opportunistic and use other offences consecutively to obtain an operational benefit or make more profit. According to the 2021 SOCTA report published by Europol[3], the ability of criminal networks to adapt is one of their main characteristics. This became clear during the COVID-19 pandemic, criminals adapted their methods very quickly to this unprecedented situation.

Analysis of the files related to organised crime that CTIF-CFI disseminated to the judicial authorities reveals that the laundered money originates from polycriminal activities. The past year many files showed that serious fiscal fraud, social fraud and organised crime increasingly feature as interrelated issues.

Several files involve well-organised (inter)national networks with links to organised crime. This is very alarming and CTIF-CFI increasingly finds that the number of front companies and front men is on the rise and the schemes used are becoming more complex. There is a clear interaction between these networks

[3] Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

and the networks of drug traffickers, large VAT carousels or large-scale fraud. Corruption and involvement of professions that are obliged to report have also been identified.

Involvement of professional money laundering networks

In the past year several professional money laundering networks featured in files that were disseminated to the judicial authorities. These networks are becoming ever larger and more complex.

In terms of scale we find that the individuals involved persist and continue to set up or take over many legal persons. Sometimes the initial commercial name is hardly modified at all. This phenomenon occurs all over Belgium in different forms. An increasingly common phenomenon is that one account is used to carry out several payments to the Belgian Official Gazette when taking over companies, the addresses are moved to several judicial districts and front men are subsequently appointed, so there is no apparent link between these entities.

With regard to complexity it should be noted that the individuals involved can direct several other people or that they can teach these people various modi operandi (sometimes people who are in charge of a complex structure with intermediate levels so the organisation can remain operational in case a link is lost), from one location individuals can take over the management of a large number of bank accounts registered in the name of other people or companies that are actually listed in the name of other persons or companies. Several professional money laundering networks can also work together and make the financial flow even more complex using fake invoices. There is the international aspect as well, with various counterparties abroad that are, at least partly, led by the same professional money laundering networks.

The organisations, from different criminal circles, sometimes produce fake identities or fake documents themselves that can be used to open bank accounts and launder the proceeds of different crimes. By using various branches of the organisation simultaneously, detection becomes more difficult and the volume they can process in a short space of time becomes larger. Several branches are suspected of VAT (carousel) fraud and are being investigated by the Federal Public Service Finance.

The illicit money is invested in second-hand cars, drinks and tobacco. Given that these goods are trafficked illegally, there is also a suspicion of excise fraud. In this context it should be noted that in several files disseminated by CTIF-CFI to the judicial authorities links with night shops were identified, which leads to suspect that these criminal organisations have interests in these businesses.

It should be noted these investments have recently become increasingly diverse and goods such as yachts, real estate, speedboats and even parrots are purchased. Where all of these products end up and knowing who the clients of the money laundering network are, is not always clear however, as the links between them become more vague. These accounts can also be used to carry out payments for the import or export for these goods, such as customs duties.

Despite the fact that branches have been dismantled, money laundering networks remain operational and the phenomenon seems to have been thoroughly anchored in society.

Sharp rise in the number of disclosures with a fiscal aspect as a result of the circular of the National Bank of Belgium (NBB)

The past year CTIF-CFI received a considerable larger number of disclosures with a fiscal aspect. A number of disclosures referred to the circular of the National Bank of Belgium (NBB).

On 8 June 2021, the NBB published the circular “Due diligence obligations regarding the repatriation of funds from abroad and taking into account the tax regularisation procedures when applying the Anti-Money Laundering Law”. This circular aims to promote equal treatment of all Belgian financial institutions, to ensure adequate management of risks by these institutions and to increase the predictability of the NBB’s further actions with regard to financial institutions that have followed the required procedure.

Financial institutions comply with the circular and conduct an internal audit, a so-called look back analysis. If there is no reasonable proof for the legitimate origin of the funds and their correct fiscal processing the

institution is required to report this information to CTIF-CFI. It should be noted that the collection of information and its analysis should be conducted with the necessary care. The deadline for finalising the internal audit is 30 June 2022.

Raising awareness of police services and the judicial authorities regarding polycriminal money laundering platforms

Immediately after last year CTIF-CFI continued the awareness-raising process of the police and the judicial authorities regarding the networks identified in the main channels aimed at emphasising the organised nature of the criminal networks operating as polycriminal laundering platforms.

Various initiatives were launched to strengthen the cooperation between CTIF-CFI, the police and the judicial authorities, for the operational processing of files as well as for strategic analysis of the methods identified.

In cooperation with CTIF-CFI and the central departments of the judicial police, the Federal Public Prosecutor's Office coordinates the criminal proceedings and intelligence management of the polycriminal phenomenon of "Brazilian networks".

More spontaneous information with a fiscal aspect exchanged

CTIF-CFI also received more spontaneous information with a fiscal aspect from foreign counterparts. The information provides an interesting insight into foreign financial products, unusual fiscal behaviour and investments over time enabling CTIF-CFI to conduct targeted analyses. These analyses could lead to disseminations to the competent Public Prosecutor's Office, as well as disseminating relevant information to the Federal Public Service Finance.

More information exchanged with the Federal Public Service Finance

The rise in disclosures with a fiscal aspect lead to more disseminations, which in turn lead to more relevant information being exchanged with the Federal Public Service Finance, via the unit "Anti-fraud Coordination (CAF)". In 2021, no fewer than 268 documents were exchanged[4]. CTIF-CFI received feedback showing that this information leads to good results.

Relevant information is swiftly disseminated to the Federal Public Service Finance if this is the result of a disseminated report linked to "Brazilian networks" and in which a decision was taken to block the balance of the assets.

Action plan to combat fraud: automatically checking fiscal information

In June 2021, the Minister of Finance Mr Vincent Van Peteghem, as Chair of the Board for combating fiscal and social fraud [*Collège pour la lutte contre la fraude fiscale et sociale*] launched a 29-point action plan. The action plan was developed quickly after the board was relaunched. Several projects were developed that strengthen the government's coordinated policy against fraud. These projects involve several departments.

One of these projects deals with digitalizing the procedure when CTIF-CFI requests additional information from administrative departments. CTIF-CFI has the power (pursuant to Article 81 of the Law of 18 September 2017) to obtain any additional information it deems useful to accomplish CTIF-CFI's task from departments such as the Federal Public Service Finance, including the right to ask whether an individual involved in a money laundering case is (unfavourably) known to the tax authorities. Checking fiscal records of an individual is currently done manually.

[4] For more information please refer to the section on statistics, the fiscal statistics on relevant information disseminated by CTIF-CFI to the unit "Anti-fraud Coordination (CAF)" pursuant to Article 83, 2, fifth subparagraph of the AML Law of 18 September 2017.

CTIF-CFI's project aims to look into how and to which extent this check could be automated (checking the Federal Public Service Finance's database automatically). The aim of the two entities taking part in this project is to quickly achieve improved mutual information exchange. The legal framework enabling CTIF-CFI to request information from the Federal Public Service Finance and enabling the Federal Public Service Finance to respond is already in place and does not need to be amended. The IT tools are also available.

Since July 2021 CTIF-CFI has been using lists of individuals and these lists have been enhanced by the Federal Public Service Finance. Automating the exchange will enable both parties to work more efficiently and combat money laundering and serious fiscal fraud more efficiently.

1.3. Corruption

Trends identified

In 2021, CTIF-CFI disseminated twelve new files to the Public Prosecutor's Office in which corruption or embezzlement by public officials was identified as the main predicate money laundering offences. This number is similar to the one of 2020. The origin of the disclosures included in these files (categories of reporting entities) is virtually the same. Once again credit institutions had the largest share.

Analysis of the money laundering files[5] has shown that these files featured key figures from the world of politics, diplomacy, finance and business. Several files featured individuals who were politically exposed persons (PEPs) in Belgium or abroad or were the partner of a PEP[6]. In other files the main figures were individuals closely linked to long-term rulers in Africa.

In addition nearly all individuals involved featured in a current international investigation by journalists with regard to suspected large-scale embezzlement of government funds or were linked to corruption, embezzlement and political and financial scandals in media reports.

The suspicious transactions in these files consisted of multiple transactions, especially international transfers, including from high-risk countries with regard to corruption. It should be mentioned that the total suspicious transactions per file were generally in excess of EUR 1 million. In half of the transnational files much larger amounts were laundered, but these transactions were sometimes carried out over a longer period (5 years and more). It should also be noted that the suspicious transactions or activities took place in a pre-election period (parliamentary and/or presidential elections).

The money laundering techniques used varied in complexity, but were clearly more advanced in files with an international dimension. Analysis showed that corrupt foreign PEPs used companies and accounts in their own country and abroad to move public funds out of their country and to conceal the origin and the destination of these flows and used third parties (family members and close associates[7]) to launder funds that had been obtained unlawfully. It was also found that a foreign national had set up an international structure to conceal he was the ultimate beneficiary of a suspicious contract worth millions with a foreign public authority and that the third-party account of a legal service provider was used as a conduit.

The funds or advantages obtained illegally or advantages resulting from corrupt practices in strategic business sectors were in many cases partly laundered through real estate in Belgium. The methods used were: opaque ownership of commercial real estate, purchasing residential luxury real estate, financing renovations and refurbishments and mortgage payments.

Purchases of other high-value goods (such as jewellery) and other expenditure (purchasing luxury products, payment by credit cards,…) were also identified.

---

5 Two out of twelve files were attempted laundering of proceeds of corruption.

6 The list of functions considered to be prominent public functions by Belgium can be found in annex IV of the Law of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash.

7 Both terms are defined in Article 4, 29° of the anti-money laundering law.

As usual for the analysis of files CTIF-CFI requested information from the police, judicial authorities and obliged entities and consulted databases to which CTIF-CFI has direct access, including the Central register of beneficial owners (UBO register) and the Central Point of Contact (CPC) for accounts and financial contracts.

In some cases CTIF-CFI contacted FIUs from the Egmont Group[8] to identify the beneficial owners of foreign legal persons or to get an insight into the origin of funds transferred to Belgium. In a case involving an individual who conducted business activities in a country with an FIU that is not yet a member of the Egmont Group CTIF-CFI obtained relevant information on this individual through the Belgian civil intelligence and security service.

Finally, it should be noted that CTIF-CFI used its power to oppose execution of a transaction on several occasions.

Global context

Corruption has been a priority issue within CTIF-CFI's activities for a number of years now. The focus on the topic not only becomes clear through CTIF-CFI's operational policy (processing disclosures and exchanging information with other FIUs), but also through some of the FIU's strategic choices.

In 2021 CTIF-CFI contributed to a project by the Egmont Group on FIUs' role in the fight against money laundering of corruption proceeds within the context of the COVID-19 pandemic. The report of the project, which is not yet publicly available[9], provides an overview of corruption-related risks identified in the first year of the pandemic in jurisdictions of the Egmont Group of FIUs, efforts that FIUs made to tackle challenges resulting from this emergency situation and a number of effective practices for tackling corruption-related crimes.

CTIF-CFI had several meetings with the European Prosecutor and the European Delegated Prosecutors for Belgium to discuss possible synergies and effective forms of cooperation between CTIF-CFI and the European Public Prosecutor's Office (EPPO)[10]. The results of these discussions will be integrated into CTIF-CFI's work processes.

As part of the Belgian delegation CTIF-CFI also attended the regular meetings of the OCDE working group on bribery and the followed the discussions on the revision of the anti-bribery Recommendation. The text of the revised Recommendation[11], which was adopted by the OECD at the end of November 2021, is the result of consensus. Nevertheless, CTIF-CFI welcomes the fact that FIUs are now explicitly mentioned as partners in the fight against foreign bribery[12].

The importance of international cooperation and enhanced cooperation between competent authorities (including FIUs) in the fight against corruption was also recognised in the political declaration on combating corruption adopted in June 2021 during a special session of the General Assembly of the United Nations.

---

8 These were FIUs in the regions of Europe, Africa and the Middle East.

9 The Role of FIU in Combating the Laundering of Corruption Proceeds (within the COVID-19 Context).

10 As a reminder, the European Public Prosecutor's Office (EPPO) is an independent body of the European Union responsible for investigating and prosecuting crimes against the financial interests of the EU, including public procurement fraud, embezzlement by public officials of the European Union, corruption and money laundering, and commenced its operational activities in June 2021.

11 2021 OECD Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions. The Recommendation complements the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Anti-Bribery Convention), obliging parties to the Convention to hold individuals and companies responsible for bribery of foreign public officials in international business transactions.

12 The Recommendation stimulates a comprehensive approach to combating foreign bribery through new measures to improve awareness and detection by key government bodies (including FIUs). The Recommendation also encourages the exchange of financial intelligence between FIUs as an additional form of international information exchange. As CTIF-CFI keeps emphasizing, FIUs play an essential role in the procedure for asset recovery and asset tracing, freezing and seizing.

This political declaration guided the anti-corruption action plan 2022-2024 that was adopted by the G20 a few months later[13]. The plan and the overarching principles on corruption related to organised crime[14], tackling corruption in sport[15] and preventing and combating corruption in emergencies[16] contain new anti-money laundering commitments, including on issues such as the role of gatekeepers, audit and compliance, and transparency on the ultimate beneficiaries of legal persons and legal arrangements.

The G20 Anti-Corruption Working Group has also stated that the cooperation with the Egmont Group will be intensified. Time will tell how this will be applied in practice.

1.4. Fraud

Trends identified

Multiplication of different types of fraud and new money laundering channels

Fraud has been the predicate offence most commonly identified by CFI-CFI in files for many years. Although the aim remains unchanged, these fraudsters innovate, look for new opportunities and use various types of fraudulent practices. Over the years simple types of fraud have been replaced by more complex types of fraud: fraud with fraudulent transfers, CEO fraud, fraud with unregulated trading sites, offers to invest in diamonds, platforms for trading cryptocurrencies, etc.

The great surge of this issue, which is largely linked to the increasing digitalization of society, has also been identified by other entities that are competent to combat fraud, such as the FPS Economy, the police and the Public Prosecutor's Office. The FSMA has also identified this: in 2021, 40% of reports to the FSMA related to fraudulent online trading platforms trading in binary options, CFDs, forex products as well as cryptocurrencies. This is a 53% increase compared to 2020[17].

Networks also thrive thanks to new professions related to cybercrime linked to the concept "Cybercrime as a Service", such as selling on personal information or various kinds of malware such as ransomware and professional networks recruiting money mules. All these services are elements that, when connected, facilitate quite complex but very lucrative forms of fraud.

For money laundering purposes the system is often based on the role that money mules play, with the aim of adding a multitude of steps to the money laundering process enabling fraudsters, usually located abroad, to remain in the background of transactions. The money is withdrawn in cash from accounts of money mules (and subsequently sent abroad using money remittance), or transferred abroad directly.

Given that financial institutions are now more alert with regard to fraud, fraudsters are actively looking for alternative money laundering channels. They use crypto-assets and payments on accounts with payment service providers or neobanks.

In general our analysis shows that organised networks are not only involved in carrying out the fraud but also in subsequent money laundering transactions. Fraud cases feature increasingly large amounts and money laundering transactions increasingly feature professional money laundering networks that operate on an international scale. These networks use money laundering schemes with compensation and channelling accounts in the name of front companies.

[13] G20 Anti-Corruption Plan 2022-2024.
[14] G20 High-Level Principles on Corruption related to Organized Crime.
[15] G20 High-Level Principles on Tackling Corruption in Sport.
[16] G20 High-Level Principles on Preventing and Combating Corruption in Emergencies.
[17] https://www.fsma.be/en/news/fraudulent-online-trading-platforms-53-cent-increase-reports.

Challenges

The evolution of international payments in recent years, which provides many advantages for consumers, has also made it more difficult for investigative services to follow the money of predicate money laundering offences such as fraud. The international, virtual nature and the speed with which accounts are opened and transactions can be carried out are often to criminals' advantage. For FIUs and other financial investigative services it is becoming increasingly difficult to quickly locate assets or accounts geographically.

A recent example of this issue is the increased use of virtual bank accounts or Virtual IBANs (vIBANs). Virtual IBANs are linked to a "traditional" bank account (International Bank Account Number or IBAN) but can be issued by financial institutions – usually Payment Service Providers – that do not have a banking licence. One IBAN with a bank can be used as a "parent account" for numerous vIBANs with Payment Service Providers, who in turn provide these accounts to their customers.

Virtual IBANs are often used for the international management of receivables as payments can be received by geographical zone or currency. As they can be issued quickly and because of their international nature they are also attractive to criminals. The cascade system when they are issued make it more difficult for investigative services to determine who the beneficial owner of an account is and where this account is "physically" located. Enhanced international cooperation and a clear legal framework are needed to avoid that that the rapid evolution of international payments present opportunities to criminal organisations.

Cooperation with the "Fraud Team" with regard to fraud

To combat different types of crime, including as a result of cybercrime, more effectively CTIF-CFI works with the "Fraud Team". This specialised unit was created at the initiative of the Public Prosecutor's Office in Brussels and consists of CTIF-CFI as well as the federal judicial police, the local police, banks, the FSMA and Febelfin. In this regard a discussion was held on money mules to actively tackle this issue.

2. Evolution of techniques

2.1. Virtual assets

CTIF-CFI has been monitoring the topic of virtual currencies and the risk of them being used from money laundering and terrorist financing purposes for many years.

The Law of 20 July 2020[18] ensures that service providers for the exchange of virtual currency and fiat currency and custodian wallet providers established in Belgium fall within the scope of the Law of 18 September 2017.

In addition all ATMs installed in Belgium that enable the exchange between virtual currencies and fiat currencies have been subject to the AML/CFT Law since the Law of 1 February 2022[19]. Furthermore, providers governed by the law of a country outside of the European Economic Area are not allowed to provide services related to virtual assets in Belgium, unless they establish a subsidiary in Belgium or in another Member State of the European Union.

The rules and conditions for registration / supervision by the FSMA of these various entities in the crypto industry that are subject to the Law of 18 September 2017 were laid down this year[20].

[18] In accordance with Article 5, § 1, 14°/1 and 14°/2.

[19] Law amending the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash to introduce provisions on the status and the supervision of providers of exchange services between virtual currencies and fiat currencies and custodian wallet providers.

[20] Royal Decree of 8 February 2022 on the status and the supervision of service providers for the exchange of virtual currency and fiat currency and custodian wallet providers.

Thanks to this legal framework CTIF-CFI will be able to receive disclosures from these entities from 1 May 2022 onwards, be able to ask questions and receive additional information for its analysis.

An innovative sector

Because of the technical evolutions of virtual currencies and the increasing technical possibilities of various criminal and terrorist organisations it is vital to understand how the use of virtual currencies can lead to misuse so government bodies can respond appropriately.

CTIF-CFI's AML/CFT experience related to virtual currencies is currently based on disclosures received from other obliged entities such as credit institutions. The disclosures received contain suspicious transactions for which virtual currencies are used. As part of the spontaneous information exchange from foreign FIUs CTIF-CFI also receives information as a result of disclosures by foreign exchange platforms.

Given the specific characteristics of the sector of virtual currencies and the continuous development of the sector, in particular with regard to Non-Fungible Tokens (NFTs) and decentralised financing (DeFi), CTIF-CFI keeps expanding its expertise and remains particularly vigilant to ML/TF risks linked to virtual assets. A dialogue with new players in the world of finance is therefore essential. It is also important to acknowledge that an innovative sector involved in virtual assets has developed in Belgium.

Furthermore, CTIF-CFI will strengthen its cooperation with the FSMA, which has been designated as the supervisory authority of these entities that will be subject to the AML/CFT law in the future, as well as with other partners to keep up with the challenges linked to the world of cryptocurrencies. Meetings with the public and the private sector are organised through the AML-platform[21]. Information and expertise can be shared through this platform on developments, trends, new risks, mechanisms and typologies related to combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction identified at national, European and international level and that are useful in order to carry out their tasks effectively and correctly.

A world without borders

Given the international and cross-border nature of virtual currencies combating their use for money laundering and terrorist financing purposes cannot be done at national level. A coordinated approach at international level is needed. There has been significant progress internationally in recent years to regulate the sector of virtual currencies. There was global consensus on the need to regulate the sector of virtual currencies to combat money laundering and terrorist financing.

There is increasing supervision on the financial flows related to virtual assets in the European Union. In June 2019, a first important step with regard to regulation was taken by updating the FATF Recommendations on processing global crypto exchanges comparable to transactions of traditional financial institutions. With the fifth AML Directive the European Union, at least partially, followed the FATF Recommendations. Following the transposition of this Directive, Belgium and the other member states are well under way of preventing the anonymous use of virtual currencies. The technology behind virtual currencies evolves very quickly and it would be an illusion to think that the current European rules, focussed on the exchange between so-called fiat currencies and virtual currencies provide an adequate response. Regulators will have to continue to monitor the different technological evolutions of the sector of virtual currencies. Important differences remain between the traditional banking sector and the sector of virtual currencies. In order to be effective specific rules for this industry must be introduced.

[21] The platform, which was created in 2021 to combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction is a public-private partnership between the General Administration of the Treasury, the Belgian Financial Intelligence Processing Unit CTIF-CFI, the National Bank of Belgium, the Financial Services and Markets Authority, the Belgian federation of the financial sector and the Professional Association of Insurance Companies. In addition, representatives of other public or private institutions or specific experts can also be invited to take part in meetings, give presentations or contribute to ongoing discussions.

To avoid regulatory arbitrage between member states the European Commission adopted a comprehensive package of legislative proposals in September 2020. The Commission put forward new European legislation on cryptocurrencies: Markets in Crypto-Assets Regulation[22]. This new legislation is a regulation and will not only apply to entities issuing virtual currencies but also to companies providing services related to these crypto-assets such as companies issuing digital wallets and exchanging virtual currencies. The European Commission aims for MiCA to come into force in 2024[23].

Risks related to money laundering / terrorist financing

Thanks to their joint expertise the financial intelligence units of Austria, Denmark, France, the Netherlands, Luxembourg and Belgium were able to identify several cases in which crypto-assets were used as a means for money laundering and terrorist financing.

The cooperation between these financial intelligence units and the national law enforcement agencies revealed several offences such as terrorist financing, fiscal fraud, online fraud, fraudulent investments, fraud committed in organised groups, fraudulent access to a computer system or trade in illegal products or content.

2.2. Professional money launderers

Because of the extension of the scope of money laundering, the extent of amounts involved and increased supervision on the legal financial system an increasing number of criminal organisations outsource money laundering to specialised professionals, resulting in a professionalization of money launderers.

It has become an activity in itself, professional money launderers operate as service providers for third parties. The money to be laundered originates from multiple and various criminal activities. Professionals with various and complementary specialties provide their services to criminal groups.

Analysis of these files shows that some of the professional money launderers are financial or non-financial professionals and shows how these professionals provide their services and advice to criminals, in order for them to have companies at their disposal to carry out their illegal activities and/or launder proceeds of these activities. On several occasions during the past year CTIF-CFI informed the relevant supervisory authorities for the purpose of applying potential sanctions when entities registered with these authorities featured as entities in files disseminated by CTIF-CFI to the judicial authorities.

A growing number of files shows that professional money laundering networks are involved. In exchange for commissions these networks ensure that the dirty money is collected, transported and they move the money of front companies to offshore accounts, they move it using the offsetting technique via polycriminal money laundering platforms, making each chain of the money laundering chain more obscure. Each additional chain is meant as a cover so it becomes virtually impossible to determine the criminal origin of the money. In case of a complex criminal economy this method is used to avoid that proceeds of crime can be detected.

Professional money launderers are not members of the groups responsible for predicate offences and do not take part in these offences. It is therefore a particular challenge to identify them.

Several files show that these professional money launderers set up companies that operate as money laundering platforms. These companies act as intermediaries, they provide cash to criminals in need of cash and provide the money through the banking system to criminals wanting to dispose of their cash.

[22] Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937, Brussels, September 2020.

[23] The European parliament voted on 14 March 2022 on the most recent version of the text of the European MiCA regulation.

These money laundering companies enable the simultaneous laundering of proceeds of different illegal predicate offences[24].

Professional money launders are not only used to conceal the origin of the money but also to carry out the money laundering transactions from start to finish, until the last phase of the money laundering process, integration. They subsequently invest in real estate and in other legal assets such as cars.

Typological case: professional money launderers and integrating money in real estate

1. The Belgian company A operates in the construction industry. Large amounts are sent to the company's bank account from various companies with an account in Belgium and in a neighbouring country.

   Company A's manager led several companies that have gone bankrupt in recent years. Company A, that he recently started to manage, seems to be a front company: apart from the fact that the company's bank account is used as a channelling account, this company also does not fulfil all of its fiscal requirements.

2. This money is subsequently used for transfers to many counterparties (mainly companies) with an account in numerous European countries.

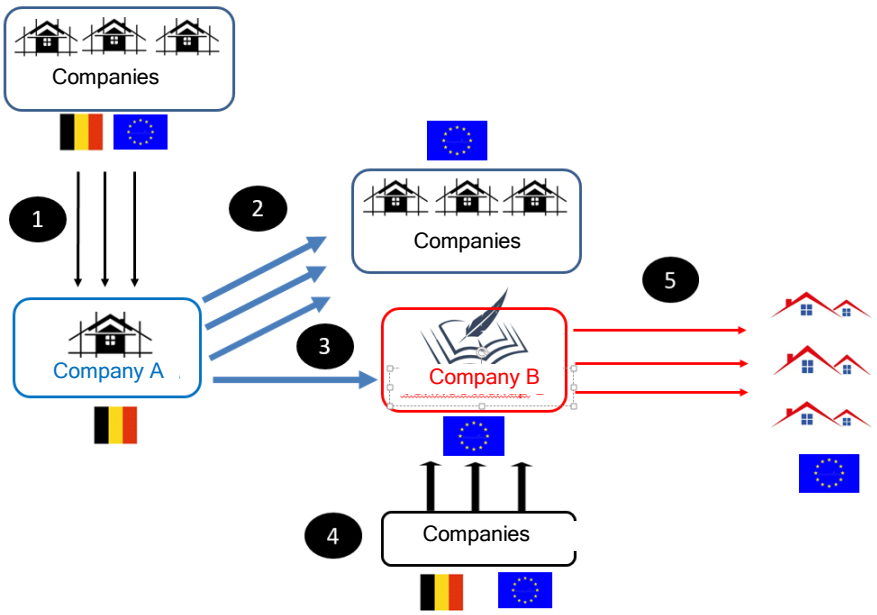
3. Company B stands out as a counterparty because of the large amounts transferred to this company (in excess of a million EUR) in a country in Southern Europe.

   According to information received from a foreign counterpart company B is a law firm in the real estate sector in Southern Europe operating as an intermediary for purchasing real estate abroad for third parties. This company is unfavourably known in files related to real estate transactions involving money laundering.

4. CTIF-CFI also finds that this law firm is a counterparty in several files that were disseminated to the judicial authorities in recent months because of several type of offences (mainly social fraud and serious fiscal fraud in the construction and cleaning industry).

5. Company A and the law firm are used as part of a money laundering scheme using the offsetting technique in which suspicious transactions are carried out from accounts of companies in the building industry. Company A and the manger operate as professional money launderers, they centralise the proceeds of various types of illegal activities and subsequently move this money abroad, mainly to the law firm. The law firm then enables the ordering parties of the transactions to purchase real estate in Southern Europe.

[24] Transfers by these money laundering platforms are often carried out to wholesalers in consumer goods or import or export companies. This money can be used to pay for a range of goods, for criminals who had initially handed over cash money. These goods can subsequently be sold using trade-based money laundering (TBML) techniques. This technique misuses the possibilities and legitimacy of (international) trade to conceal and move illegal funds by using commercial transactions. In addition to flows to Asia, CTIF-CFI also identified links to the United Arab Emirates, especially Dubai.



All of these elements point to the laundering of the proceeds of various criminal activities by collecting money through the account of a front company, facilitating the purchase of real estate abroad through a law firm taking part in the money laundering scheme.

Several criminals carrying out illegal activities in Belgium and a neighbouring country used this professional money laundering structure to purchase real estate. The file reveals the complexity and scope of the system set up by the individuals involved: money laundering on an international scale, use of professional money launderers, the laundered money is invested by purchasing real estate for third parties, large amounts of money are laundered and a significant number of Belgian and foreign companies use this system.

CTIF-CFI disseminated the file to the judicial authorities due to serious indications of laundering the proceeds of organised crime and/or illegal trafficking in narcotic drugs and/or illicit trafficking in goods and merchandise. Given that part of the laundering identified in this file took place by purchasing real estate abroad there were possibilities for the judicial authorities to potentially seize these goods.

2.3. Misuse of corporate structures

CTIF-CFI found that companies play a key role as vehicles for money laundering in a growing number of files disseminated to the judicial authorities. In files related to so-called Brazilian networks a series of companies is set up, with the aim of committing social fraud and serious fiscal fraud and they are used as shell companies for money laundering purposes. Several files with links to organised crime show that companies operate as polycriminal money laundering platforms. Each file often involves millions of EUR.

Several national and international sources confirm this trend. Europol recently stated in the SOCTA 2021[25] report that the use of corporate structures is a key element of organised crime in Europe. Corporate structures such as companies are used to facilitate nearly all types of criminal activities, which affects the EU. Criminals directly exercise control or infiltrate in legitimate corporate structures to facilitate their criminal activities.

[25] Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.
"More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level."

The past year CTIF-CFI conducted a strategic analysis on the misuse of corporate structures for money laundering purposes. This analysis shows that companies mainly feature in transactions related to social fraud (Brazilian networks, secondment fraud,…), serious fiscal fraud (VAT carousel fraud and other serious fiscal fraud), organised crime (polycriminal networks) and fraud. With regard to high-risk sectors CTIF-CFI's experience shows that companies with a lot of cash resources are often used to move illegal proceeds, as well as companies in other sectors known to be susceptible to money laundering such as the construction industry, the industrial cleaning industry, the transport industry and the hospitality industry.

Files disseminated to the judicial authorities reveal that several money laundering techniques are used, these can be simple or rather complex: cash-intensive businesses are used as a cover, companies feature as money mules, the beneficial owner is concealed, the use of money laundering schemes featuring the offsetting technique or business transactions, the involvement of polycriminal money laundering platforms and the use of professional money launderers.

These techniques are often combined with each other and are not mutually exclusive. In this respect shell companies often play an important role as a money laundering vehicle in many files. These companies are usually used for a limited time only, the time needed to carry out fraudulent transactions. These companies are left with fiscal and social debts and eventually go bankrupt. They are subsequently replaced by new structures to perpetuate the system.

To ensure that these fraud systems are detected early, the analysis of account statements can reveal certain suspicious elements that stand out. Analysis of the account statements of corporate accounts point to payments to the offices of notaries or to the Belgian Official Gazette. These payments refer to company numbers of companies being set up or companies that had been taken over. These companies could be part of the same money laundering network or be used for illegal purposes in the near future.

Financial institutions should pay more attention to payments to the Belgian Official Gazette or notaries when they are carried out for a new companies using accounts of third companies, without any official link to these companies or accounts or third-party natural persons, who are the actual managers of shell companies.

Notaries, given their involvement in setting up companies, as well as company service providers play a key role in detecting the creation or the use of companies for the purposes of criminal activities and/or laundering the proceeds of criminal activities.

3. International trends

The adaptability of criminals should not be underestimated. Their methods evolve constantly and the trends identified at international level should be taken into account in order to tackle these issues at a national level.

In this respect CTIF-CFI actively takes part in the activities of the Financial Action Task Force (FATF) and the Egmont Group to identify and analyse trends, methods and risks related to money laundering and terrorist financing.

Environmental crime and smuggling of migrants are two topics that have recently been studied by the FATF and the Egmont Group.

3.1. Environmental crime

Environmental crime refers to different types of offences, ranging from extraction and illegal trade of forestry and minerals to illegal logging and trade in waste.

As mentioned by the FATF in the report published in 2021[26] environmental crime is a very lucrative activity, generating huge amounts of proceeds of crime. The "low-risk, high-reward" nature of environmental offences ensures a safe and lucrative source of income for criminals. These offences also facilitate corruption and are combined with numerous other serious and organised offences such as serious fiscal fraud or trafficking in narcotic drugs.

This report builds on the conclusions of the FATF's 2020 report on financial flows from the illegal wildlife trade[27] and shows that criminals generate huge profits by using front companies to combine -licit and illicit- goods and payments at the start of the delivery chain of resources.

Environmental crime is a topic beyond national interests. The FATF's work, to which CTIF-CFI contributed, shows that criminals hide the profits of these crimes all over the world, also in countries without natural resources.

In this regard, the private sector has an important role to play in detecting financial flows originating from environmental crime. The FATF's study mentions best practices and risk indicators to help financial and non-financial sector detect potential cases.

In recent files of the police and CTIF-CFI the link between drug trafficking and gold was repeatedly identified. The police found cash and often also gold bullion during house searches linked to drugs. CTIF-CFI has found that gold features in files in which the offsetting technique is used to launder money, and criminal organisations involved in drug smuggling receive gold in return for their cash.

The issue of laundering through the gold trade was also identified in other current typological analyses of CTIF-CFI. The analysis of the role of Dubai in international money laundering systems revealed the role gold can play to move assets internationally via TBML. As revealed in the recent FinCEN files, gold was linked to large-scale fiscal fraud in cases of correspondent banking.

Moreover, the FATF also stated in its report on illegal wildlife trade that gold is used by criminal organisations that focus on this type of smuggling. The proceeds of illegal gold mining in these areas of conflict are often a source of armed clashes and increase the power of criminal or extremist organisations.

As the gold trade currently seems to be a cross-cutting element in various money laundering issues that CTIF-CFI encounters, CTIF-CFI will analyse this issue in order to check a number of hypotheses mentioned above.

Following a number of high-profile criminal cases in the gold and diamond trade in Antwerp interdisciplinary cooperation was started early 2021 with regard to illicit retail trade in jewellery and diamonds. This initiative - called *Midas* - coordinates the efforts of the police and the social inspection services. CTIF-CFI is also part of this initiative.

3.2. Smuggling of migrants

As a result of several migrant crises smuggling of migrants is one of the offences whose profitability has increased greatly in recent years. Usually smugglers organise the smuggling of human beings in exchange for large amounts of money.

Human smuggling networks are sometimes simple (with a small number of individuals involved) but can also be very complex (so sophisticated and organised they can be considered to be genuine criminal organisations). Depending on the degree of complexity of the networks different money laundering methods are used to inject, move or invest money in the legitimate economy.

---

[26] FATF, Money Laundering from Environmental Crime, 2021.
The FATF report mentions methods used by criminals to launder the proceeds of environmental crime as well as the resources that governments and the private sector can use to stop these activities. When they are applied correctly the FATF Recommendations are effective tools to combat these illicit financial flows.

[27] FATF, Money Laundering and the Illegal Wildlife Trade, 2020.

The transactions identified in files disseminated to the judicial authorities by CTIF-CFI are generally money remittance transactions, often to and from regions known to be areas on migration routes that migrants cross to reach Western Europe.

In other cases we find that legitimate companies led by smugglers or their associates (such as retail or wholesale businesses, food shops, travel agencies, transport companies, internet access points or night shops) are used during the entire journey to support the facilitating activities of the networks, in particular logistical support. They can also be used to launder the proceeds of crime and make their income appear legitimate. These files also show that individuals often use their commercial activities as a cover for illegal activities related to illegal immigration networks. Although the nature of the commercial activities of these businesses can provide an explanation for cash deposits it is probable that, given the police information, the transactions are, at least partially, proceeds of migrant smuggling.

The generated profits are invested in real estate, high-value goods and in legitimate companies, in the countries of origin as well as in the countries of destination[28].

Criminal networks thrive thanks to the great demand for the services of smugglers and the low risk of detection. Smuggling of migrants is a topic of international concern. The FATF has, as part of its work on trends, conducted a typological study[29] on this topic, to which CTIF-CFI contributed. The results are aimed at providing an international insight into the issue, provide typologies on the money laundering methods used and raise awareness among the private sector[30].

Detecting financial flows from migrant smuggling remains difficult. The frequent use of cash money, the avoidance of the formal banking system and the use of unofficial methods outside of the banking system such as hawala are impediments. According to the FATF report there are other difficulties such as the use of crypto-assets and of professional money laundering networks.

Europol[31] emphasises that one of the main changes in the way smugglers work is the extensive use of digital services and resources, such as social media and mobile applications for recruitment, (encrypted) communication, sharing photos and videos of (fake) documents and for money remittance.

Terrorist financing trends

Trends identified

The downward trend of recent years of the number of files disseminated to the judicial authorities due to serious indications of terrorist financing continued in 2021. The amounts in the files disseminated to the judicial authorities are also limited. Despite these relatively low figures, analysis of these files does reveal some prominent common elements. These elements relate to the way in which money is transferred or to the techniques used to conceal financial flows, as well as themes that feature in multiple files.

New payment systems

One finding is that –as is the case with money laundering- “new” payment methods provided by “neobanks”, Payment Service Providers (PSPs) or Virtual Asset Service Providers (VASPs) are increasingly used for terrorist financing purposes. The international nature and the speed at which accounts can be opened and transactions carried out present new challenges to FIUs. This is especially the case with regard to terrorist financing, given that the amounts are smaller than in money laundering cases. Terrorist financing can result in a very significant impact, even when smaller amounts are involved. The “risk-based approach” of

[28] Europol (2021), European Migrant Smuggling Centre – 5th Annual Report Publications Office of the European Union, Luxembourg.
[29] FATF, ML/TF Risks Arising from Migrant Smuggling, 2022.
[30] FATF, Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling: The role of the private sector in detection and prevention, March 2022.
[31] Europol (2021), European Migrant Smuggling Centre - 5th Annual Report, Publications Office of the European Union, Luxembourg.

neobanks and PSPs in general is based on absolute amounts and, even more than is the case with money laundering, is under even more pressure when tackling potential terrorist financing.

The transition to online payment systems is partially also the result of some “de-risking” policy of traditional banks. Large and small entities in this sector are becoming less willing to take risks. As a result, accounts of high-risk customers are simply closed. This not only complicates the work of FIUs and intelligence services, but also leads these individuals to online neobanks, which are often established abroad. As a result the financial trail in Belgium ends and becomes more difficult to follow.

Right-wing extremism

A second finding in the files that CTIF-CFI processed in 2021 is the link with right-wing extremism. There already was an increase in the number of files related to this issue in 2020, and this trend continued in 2021. Right-wing extremism is gaining in importance and visibility in Belgium as well as in Europe. These are individuals and groups who, simply stated, base themselves on racism, nationalism and totalitarianism. With the Alt-right movements in the United States, the identitarian discourse of an increasing number of political and ultraconservative, political or not, movements in Russia and the Middle East, right-wing extremism in Belgium and Western Europe is becoming ever more difficult to describe, analyse and combat compared to twenty years ago. Financial investigation into right-wing extremism is becoming progressively more difficult because of the increased use of crypto-assets, crypto exchange platforms, Payment Service Providers and neobanks that operate online and often internationally.

It was repeatedly identified in files that some extreme right-wing organisations were financially linked to foreign counterparts. It also became clear that organisations with modern methods and a very good understanding of social media received more financing in recent years. The financial analysis of natural persons with extreme right-wing views regularly revealed purchases from foreign web shops exclusively aimed at individuals with such views. Depending on the age of the individual this ranges from traditional Nazi symbols and items referring to Norse mythology to very modern-looking clothing and gadgets.

Challenges

The common element between the issue described above and the cases in question is that FIUs should keep up with swift technological developments in the world of finance and need to adapt their methods in order to respond appropriately. It has become much easier to open accounts with neobanks abroad and carry out international transactions quickly, which was not possible a few years ago. Financial flows are increasingly made up of crypto-assets that are more difficult to trace and are regularly moved to crypto-exchange platforms located abroad. Only by regulating these new players, and by quickly exchanging this type of information with the country of origin or residence and the availability of appropriate analytical tools a comprehensive picture of the individual can be established and an adequate conclusion is possible. Financial borders are fading more than ever before and the success of combating money laundering and terrorist financing will depend on an integrated and overarching approach.

To tackle the issue of right-wing extremism close and integrated cooperation is required with the Public Prosecutor’s Office, the police and the intelligence services. This way an informed assessment of potentially violent nature of individuals and organisations can be made, in which case some suspicious transactions should be considered to be terrorist financing.

In a number of these files extensive cooperation with foreign FIUs was also of great importance. When foreign neobanks or crypto exchange platforms are involved FIUs fully depend on good mutual cooperation. Often this involves “financing of extremism” rather than terrorist financing. This distinction between extremism/radicalism and terrorism requires FIUs and other partners to adopt a different approach.

Action taken

Only by following up and approaching individuals and persons with extreme right-wing ideas can we try to avoid that some of them move towards violent right-wing extremism or extreme right-wing terrorism. In

Belgium it is possible to share information with the intelligence services and the Coordination Unit for Threat Analysis OCAM-OCAD within the framework of the fight against the radicalisation process, terrorism, terrorist financing and related money laundering transactions, pursuant to Article 83, §2, first subparagraph, 4°. The Belgian legislator did not include radicalism and extremism as a predicate offence on the basis of which CTIF-CFI can disseminate a file to the judicial authorities, but CTIF-CFI does have the possibility to share all information in this regard with the intelligence services State Security Department (VSSE), the General Intelligence and Security Service (SGRS-ADIV) and the Coordination Unit for Threat Analysis OCAM-OCAD. This possibility was used extensively by CTIF-CFI this past year and emphasises its preventive value. In 2021 CTIF-CFI sent 18 information reports regarding right-wing extremism to the intelligence services and OCAM-OCAD.

This cooperation results in more targeted analyses and a more direct communication flow. This way the transactions of certain individuals, who were able to remain undetected from the police and CTIF-CFI, can then be linked to the financing of right-wing extremism.

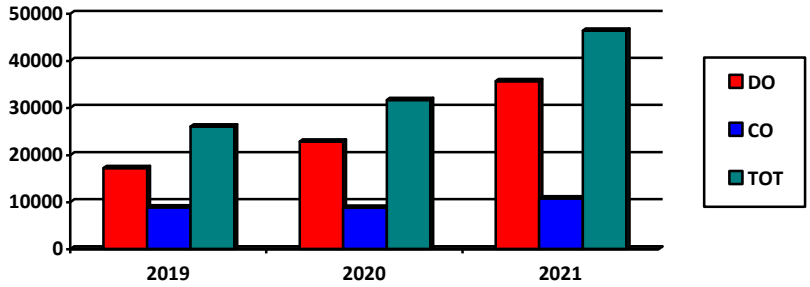
V. INFORMATION SYSTEM

1. KEY FIGURES

1.1. Disclosures sent to CTIF-CFI and newly opened files

In 2021, CTIF-CFI received a total of 46.330 disclosures or notifications of information that were grouped in 35.605 new cases and 10.725 additional notifications of information in cases that had been opened previously.

	2019	2020	2021
Total number (TOT)	25.991	31.605	46.330
New cases (DO)	17.166	22.823	35.605
Additional information (CO)	8.825	8.782	10.725



These disclosures are listed by category of obliged entity in section 2 below.

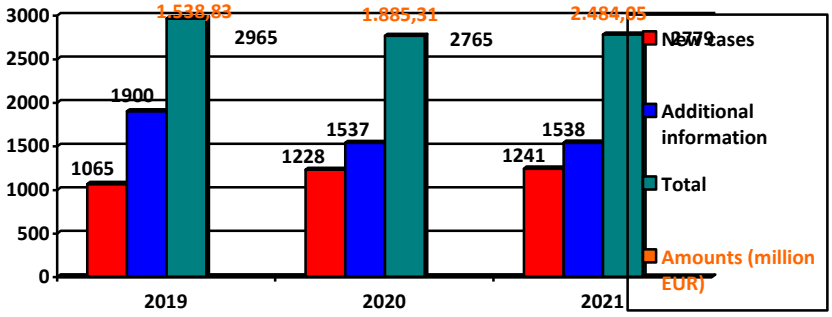
1.2. Files disseminated to the judicial authorities

If CTIF-CFI has serious indications of money laundering, terrorist financing or proliferation financing CTIF-CFI shall disseminate the results of its analysis to the Public Prosecutor or the Federal Public Prosecutor. If subsequently additional information (regarding new transactions) is reported to CTIF-CFI, CTIF-CFI shall inform the Public Prosecutor of the Federal Public Prosecutor accordingly.

CTIF-CFI must also send a copy of its report to the Prosecutor at a labour tribunal when the dissemination to the Public Prosecutor or Federal Public Prosecutor contains information regarding laundering the proceeds of trafficking in human beings, smuggling of human beings or social fraud[32].

	2019	2020	2021
Public Prosecutor or Federal Public Prosecutor - New cases (number) - Amounts communicated - Additional information (number) - Communicated additional information (Amounts in million EUR)	 1.065 1.158,66 1.900 380,17	 1.228 1.636,49 1.537 248,82	 1.241 2.336,95 1.538 147,10
Number of copies to Prosecutors at a labour tribunal	227	137	358

[32] Article 83 of the Law of 18 September 2017



When a file is disseminated to the judicial authorities CTIF-CFI must in a number of cases also send relevant information from its files disseminated to the judicial authorities to a number of administrative authorities listed in Article 83 of the Law of 18 September 2017 (cf. 4.2.).

1.3. Freezing orders by CTIF-CFI

The Law of 18 September 2017 (Article 80) enables CTIF-CFI, when it receives a report of a suspicion or information in accordance with Article 79 (so also within the framework of a request for assistance from a foreign FIU), to freeze the execution of any transaction announced by the reporting entity, as well as the execution of any related transaction. CTIF-CFI determines to which transactions and accounts this freezing order refers.

In 2021, CTIF-CFI used its power to oppose execution of a transaction on 44 occasions. CTIF-CFI temporarily froze assets worth EUR 7,04 million.

	2019	2020	2021
Number of freezing orders	26	33	44
Total amount of freezing orders(1)	3,77	30,58	7,04

(1) Amounts in million EUR.

As a reminder, CTIF-CFI also informs the Central Office for Seizure and Confiscation (OCSC-COIV) when in a file disseminated to the judicial authorities amounts or assets of significant value are available for potential judicial seizure (cf. 4.2.). CTIF-CFI does not necessarily freeze or block these amounts. It only does so if there are indications of avoidance of potential seizure and court cases.

2. DISCLOSURE ACTIVITY

2.1. Disclosures

	2019	2020	2021	% 2021
Credit institutions	11.237	17.678	21.624	46,67
Payment institutions	5.814	6.263	16.016	34,57
Notaries	1.239	1.177	1.214	2,62
Company under public law *bpost*	1.470	897	1.082	2,34
Institutions for electronic money	90	654	774	1,67
Life insurance companies	308	661	749	1,61
Mortgage credit institutions	83	166	671	1,45
External accountants, external tax advisors, external licensed accountants, external licensed tax specialists-accountants	248	254	314	0,68
National Bank of Belgium	456	197	273	0,59
Gaming establishments	396	157	191	0,41
Companies for consumer credit	132	151	119	0,26
Company auditors	73	38	86	0,19
Estate agents	52	37	48	0,10
Stock broking firms	49	33	39	0,08
Bailiffs	44	24	27	0,06
Currency exchange offices	117	106	23	0,05
Company service providers	2	27	19	0,04
Lease-financing companies	2	19	20	0,04
Branch offices of investment companies in the EEA	2	70	10	0,02
Royal Belgian Football Association	-	-	10	0,02
Lawyers	11	17	8	0,02
Branch offices of management companies of collective investment undertakings in the EEA	0	6	9	0,02
Insurance intermediaries	4	5	6	0,02
Portfolio management and investment advice companies	0	3	7	0,02
Football clubs	-	-	4	0,01
Dealers in diamonds	15	4	5	0,01
Intermediaries in banking and investment services	1	3	0	-
Branch offices in Belgium of life insurance companies in the EU	1	0	0	-
Central securities depositaries	0	0	0	-
Security firms	0	0	2	-
Market operators	0	0	0	-
Payment institutions managing credit cards	0	0	0	-
Collective investment undertakings	0	0	0	-

Independent financial planners	0	0	1	-
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	-
Total	**21.846**	**28.649**	**43.351**	**93,61**

2.2. Requests for information received from FIU counterparts

	2019	2020	2021	% 2021
FIU counterparts	1.463	1.003	1.512	3,23

2.3. Notifications received from other competent authorities

	2019	2020	2021	% 2021
Customs and Excise(1)	1.794	1.076	632	1,46
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*] (2)	665	604	489	1,13
Federal Public Service Finance	29	50	37	0,09
Flemish tax authority [*Vlaamse belastingdienst*] (2)	44	36	32	0,07
Federal Public Service Economy	68	26	19	0,04
State Security Department [VSSE]	8	16	9	0,02
General Intelligence and Security Service [SGRS-ADIV]	-	2	4	0,01
Trustees in a bankruptcy and temporary administrators	8	2	2	-
Information and advice centre on harmful sectarian organisations [*Centre d'Information et d'avis sur les organisations sectaires*]	1	2	1	-
(Federal and regional) social inspectorate	-	6	-	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	3	2	-	-
Federal Public Prosecutor's Office	12	1	-	-
Prisons	1	1	-	-
Total	**2.633**	**1.824**	**1.225**	**2,64**

(1) Includes the declarations of cross-border transportation of currency in accordance with Directive (EC) no 1889/2005 of 26 October 2005 and from 2 June 2021 onwards with Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 and the Royal Decree of 26 January 2014 on supervisory measures for the physical cross-border transportation of currency.

(2) Includes the fiscal regularisation certificates that these departments sent to CTIF-CFI.

In 2021, the European Commission developed a computer application enabling the customs authorities to communicate declarations of cross-border transportation of currency through a joint database that FIUs can access. So the decrease in the number of reports by Customs and Excise in 2021 is merely due to a technical matter.

2.4. Notifications received from supervisory, regulatory or disciplinary authorities

	2019	2020	2021	% 2021
Financial Services and Markets Authority (FSMA)	28	114	179	0,39
Institute for Tax Advisors and Accountants (ITAA)[33]	-	-	57	0,13
FPS Economy (dealers in diamonds)	17	12	5	-
National Chamber of Notaries			1	-
National Bank of Belgium (NBB)	1	1	-	-
Gaming Commission	1	1	-	-
Institute of Accountants and Tax Consultants (IAB-IEC)	2	3	-	-
Total	**49**	**131**	**242**	**0,52**
GRAND TOTAL (2.1 – 2.4)	**25.991**	**31.605**	**46.330**	**100**

[33] A result of the merger of the two institutes of accountants and tax consultants (IAB-IEC and BIBF-IPCF).

3. INTERNATIONAL COOPERATION

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 exchange of information is always carried out securely. 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.

CTIF-CFI attaches great importance to protecting the data it sends to counterpart financial intelligence units.

Three year ago CTIF-CFI became obliged to, when it receives a disclosure relating to another EU country, to externalise the data of this disclosure in an automated and standardised way to the counterpart FIU in question. Section 4.4. below contains more detailed information on this externalisation method.

The figures below with regard to the number of requests received from (1.512) and sent to (717) 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 receives information from foreign FIUs on individuals with an address in Belgium who fell victim to fraud in the country of that FIU or with warnings[34] for specific fraud schemes. CTIF-CFI also considers this exchange of information to be spontaneous information exchange.

	Incoming international cooperation (requests and notifications received by CTIF-CFI)			Outgoing international cooperation (requests and notifications sent by CTIF-CFI)		
Region	**Requests for information**	**Spontaneous notifications**	**Total**	**Requests for information**	**Spontaneous notifications**	**Total**
Africa	23	-	**23**	5	8	**13**
Americas	18	350	**368**	14	12	**26**
Asia Pacific	8	3	**11**	12	19	**31**
Eurasia	7	2	**9**	1	8	**9**
Europe	531	549	**1.080**	287	321	**608**
Middle East and North Africa	14	7	**21**	19	11	**30**
Total	**601**	**911**	**1.512**	**338**	**379**	**717**

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

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

4. DISSEMINATION OF INFORMATION

4.1. Files disseminated to the judicial authorities

In 2021, CTIF-CFI disseminated 1.241 new files to the judicial authorities for a total amount of EUR 2.336,95 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 2021, CTIF-CFI disseminated a total of 2.779 disclosures (new files and additional disseminated files)[35] to the judicial authorities for a total amount of EUR 2.483,98 (2.336,95+147,03) million.

In 358 cases a copy of CTIF-CFI's report was simultaneously sent to the Prosecutor at a labour tribunal in accordance with Article 83 of the Law of 18 September 2017.

	2019	2020	2021
- New cases (number)	1.065	1.228	1.241
- Amounts in files disseminated to the judicial authorities	1.158,66	1.636,49	2.336,95
- Additional information (number)	1.900	1.537	1.538
- Additional amounts in files disseminated to the judicial authorities	380,17	248,82	147,03
(Amounts in million EUR)			
Copies to the Prosecutors at a labour tribunal (number)	227	137	358

Moreover, CTIF-CFI is required to share information with various administrative departments (cf. 4.2.).

If there are no serious indications of money laundering or terrorist financing, CTIF-CFI does not disseminate anything to the judicial authorities, although the information from disclosures is never lost.

Even if a file is not disseminated to the judicial authorities CTIF-CFI can disseminate the information from this file to the intelligence services and OCAM-OCAD within the framework of the fight against the radicalisation process, terrorism, terrorist financing and related money laundering transactions (cf. 4.2.).

CTIF-CFI also disseminates a lot of information to its foreign counterparts, in particular when disclosures originate from obliged entities operating in Belgium under the freedom to provide services (cf. 4.4).

The information that is not externalised forms an essential base and remains available in case new relevant information would make it possible to link this information with money laundering or terrorist financing. This information is also used for strategic analysis purposes.

[35] The Law of 18 September 2017 prohibits CTIF-CFI from disseminating disclosures to the judicial authorities, as well as to third parties.

4.2. Dissemination to judicial authorities

The members of CTIF-CFI and the staff of CTIF-CFI are subject to strict professional secrecy. Yet this professional secrecy is lifted in a number of cases listed exhaustively in Article 83 of the Law of 18 September 2017.

This enables CTIF-CFI to exchange information with the departments below and share relevant information.

Article 83 of the Law of 18 September 2017 – number of notifications	2019	2020	2021
Anti-fraud Coordination (CAF) Unit FPS Finance Customs and Excise	276 -	271 10	268 35
Social Intelligence and Investigation Service (SIRS-SIOD)	394	251	242
Federal Public Service Economy	-	24	17
Financial Services and Markets Authority (FSMA)	4	-	-
Central Office for Seizure and Confiscation (OCSC-COIV)	34	39	50
Coordinating Unit for Threat Analysis (OCAM-OCAD)	162	142	97
State Security Department (VSSE)	162	142	97
General Intelligence and Security Service (SGRS-ADIV)	162	142	97
Joint Database [*Banque de Données Commune*].	102	31	8

4.3. Exchange with supervisory authorities and reporting entities

In accordance with Article 121 of the Law of 18 September 2017, CTIF-CFI strengthened its cooperation with supervisory authorities of reporting entities subject to the AML/CFT framework.

This enhanced cooperation is to enable the different competent authorities to carry out the tasks they have been given pursuant to the Law of 18 September 2017 as well as possible.

In general this cooperation take place by exchanging information, spontaneously or upon request, between CTIF-CFI and the supervisory authorities and sharing expertise, in accordance with the applicable legal provisions on professional secrecy.

Notifications from CTIF-CFI to the supervisory authorities relate to feedback on the reporting activity of obliged entities under their supervision (quantitative and qualitative assessment) or infringements of the AML/CFT obligations by these entities and identified by CTIF-CFI when carrying out its tasks.

These notifications make it possible to assess the reporting activity individually or by sector and improve the number and quality of disclosures. This also enables supervisory authorities to fine-tune their risk-based due diligence obligations and impose sanctions where applicable in case infringements are identified.

The notifications with feedback on reporting activity were regularly exchanged between CTIF-CFI and the supervisory authorities of financial professions given that they usually send the largest number of disclosures to CTIF-CFI (NBB, FSMA and the FPS Finance Treasury) and occasionally between CTIF-CFI and the supervisory authorities of non-financial professions.

In 2021, CTIF-CFI sent a total number of 89 notifications to the supervisory authorities.

In accordance with Article 78 of the Law of 18 September 2017 as amended by the Law of 20 July 2020 (and previously on the basis of the recommendations to Member States on the supranational risk assessment) CTIF-CFI provides specific feedback on the quality and relevance of disclosures to obliged entities (mainly to credit institutions and payment institutions) to help them improve their disclosures. In

general the feedback is based on an analysis examining whether the disclosure is complete, clear and precise, the grounds of the suspicion are also carefully examined. It is also reviewed whether disclosures and responses to additional requests are submitted within a reasonable period of time.

CTIF-CFI recently published a list on its website aimed at reporting entities with the main criteria that CTIF-CFI uses to assess the general quality of a disclosure. Obliged entities should pay particular attention to this list when drawing up their disclosures.

CTIF-CFI's website also features a list with ML/FT indicators that may be helpful to reporting entities. It is a non-exhaustive list of elements that could be suspicious. These criteria are examples that each reporting entity should assess to determine whether there are suspicions of ML/TF.

4.4. Dissemination to other financial intelligence units

Article 53.1 of the fourth European AML/CFT Directive obliges Member States to cooperate immediately with counterpart FIUs in the EU: "When an FIU receives an STR which concerns another Member State, it shall promptly forward it to the FIU of that Member State."

This provision was transposed in Article 124 of the Law of 18 September 2017, which stipulates: When CTIF-CFI receives a suspicious transaction report, drawn up by an obliged entity in accordance with Article 47 or 54, regarding another country, it shall send for analysis, all relevant information in the report to the FIU of the country in question that has access to the FIU.Net, as soon as possible.

There are different types of cross-border cooperation, including XBD and XBR.

XBR "Cross-border reporting": receipt of a disclosure submitted by a reporting entity whose main activity is operating under the freedom to provide services in the European Union from Belgium, and is therefore subject to the AML/CFT law but the vast majority of disclosures is not related to or does not have any direct link to our country. In this case CTIF-CFI sends the entire contents of the disclosure to the FIU(s) in question to enable this/these FIU(s) to analyse this disclosure themselves.

XBD "Cross-border dissemination": receipt of a "traditional" disclosure that may be relevant to one or more European Financial Intelligence Units. The transfer of information to the FIU(s) in question takes place using "metadata" and "promptly", so immediately upon receipt of the disclosure, prior to any analysis.

The XBD procedure does not replace the current procedure of spontaneous exchange, which takes place during or after the analysis of the file. The two procedures are complementary in this respect, an initial XBD (or lack of an XBD) does not exclude a subsequent spontaneous exchange.

CTIF-CFI also responds to requests for information from foreign financial intelligence units and sends them information it already holds or requests and receives from obliged entities, police services and other administrative authorities in Belgium.

Number	2019	2020	2021
- XBR - XBD - Spontaneous exchange - Exchange upon request	38 47 - 1.463	893 114 - 1.003	8.021 613 601 911

VI. FIGURES AND ADDITIONAL CLARIFICATIONS

Reporting activity

1. Number of entities having submitted disclosures

Financial professions	2019	2020	2021
Credit institutions	60	58	57
Currency exchange offices, payment institutions and institutions for electronic money	37	32	32
Life insurance companies	16	17	22
Mortgage credit institutions	12	11	15
Companies for consumer credit	10	8	9
Stock broking firms	9	6	6
Insurance intermediaries	3	5	6
Branch offices of investment companies in the EEA	2	5	0
Lease-financing companies	2	5	3
Company service providers	2	4	4
Company under public law *bpost*	1	1	1
National Bank of Belgium	1	1	1
Intermediaries in banking and investment services	1	2	0
Payment institutions issuing or managing credit cards	0	0	0
Management companies of collective investment undertakings	0	0	0
Branch offices of management companies of collective investment undertakings in the EEA	0	1	0
Settlement institutions	-	0	0
Central securities depositories	0	0	0
Portfolio management and investment advice companies	0	1	4
Public Trustee Office	0	0	0
Branch offices of investment companies outside the EEA	0	0	2
Market operators	0	0	0
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	1
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	1
Total	**157**	**156**	**164**

Non-financial professions	2019	2020	2021
Notaries	345	307	298
Accounting and tax professions	142	156	148
Estate agents	29	19	23
Company auditors	27	20	28
Bailiffs	15	11	12
Lawyers	8	8	4
Gaming establishments	14	12	11
Trustees in a bankruptcy and the temporary administrators	6	2	1
Dealers in diamonds	3	1	2
Security companies	0	0	2
High-level professional football clubs	-	-	3
Royal Belgian Football Association	-	-	1
Total	**589**	**536**	**533**

Analysis of disseminations

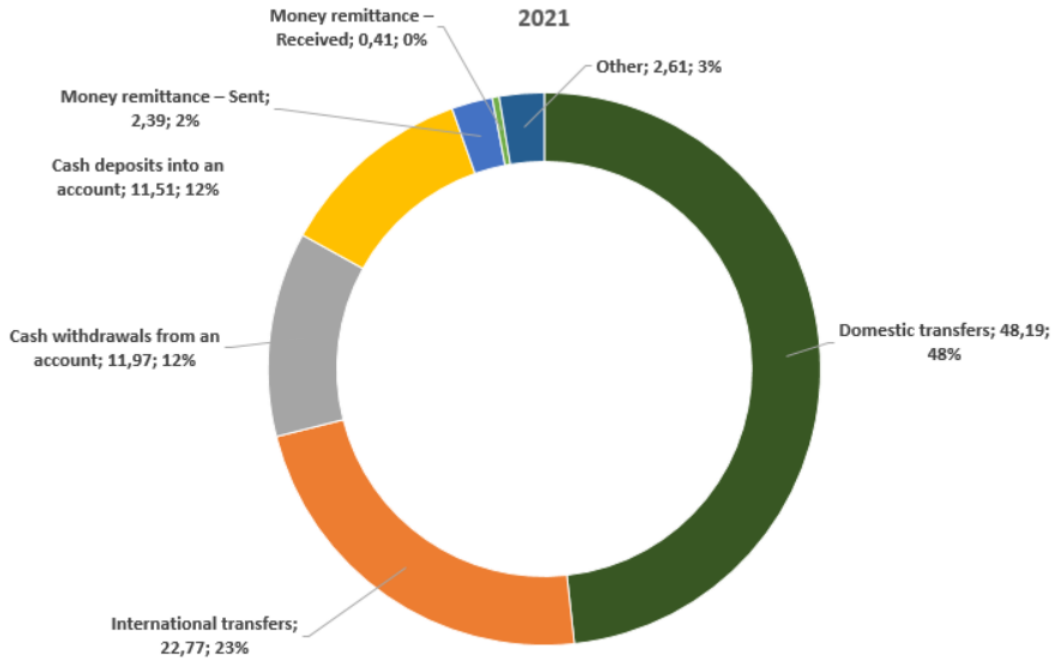
2. Disseminations by type of reporting entity

	2019	2020	2021	% 2021
Credit institutions	783	942	990	79,77
Payment institutions	102	96	97	7,82
FIU counterparts	68	80	67	5,40
Company under public law *bpost*	37	34	30	2,42
Notaries	4	10	13	1,05
Gaming establishments	1	6	7	0,56
Institutions for electronic money	1	4	7	0,56
Accounting and tax professions	14	17	6	0,48
Mortgage credit institutions	3	1	6	0,48
Customs	3	4	3	0,25
Company auditors	1	2	3	0,25
Federal Public Service Economy (dealers in diamonds)	5	5	2	0,16
Life insurance companies	-	2	2	0,16
Financial Services and Markets Authority	4	1	2	0,16
National Bank of Belgium	6	-	2	0,16
Branch offices of investment companies in the EU	-	6	1	0,08
Life insurance intermediaries	-	-	1	0,08
Federal Public Prosecutor's Office	9	1	1	0,08
Royal Belgian Football Association	-	-	1	0,08
Federal Public Service Finance	6	4	-	-
Stock broking firms	2	3	-	-
State Security Department [VSSE]	2	3	-	-
Currency exchange offices	2	1	-	-
Dealers in diamonds	3	1	-	-
Bailiffs	2	1	-	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	2	1	-	-
Prisons	-	1	-	-
Lawyers	1	1	-	-
Companies for consumer credit	-	1	-	-
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	-	-	-	-
European Anti-Fraud Office OLAF	-	-	-	-
Total	**1.065**	**1.228**	**1.241**	**100**

3. Nature of the suspicious transactions

The table below specifies the nature of the suspicious transactions in files disseminated to the judicial authorities in 2021. A file disseminated to the judicial authorities may include various types of suspicious transactions.

Type of transactions	% 2021
Domestic transfers	48,19
International transfers	22,77
Cash withdrawals from an account	11,97
Cash deposits into an account	11,51
Money remittance - Sent	2,39
Money remittance - Received	0,41
Casino transactions	0,36
E-money	0,31
Life insurance	0,25
Payments in cash	0,25
Purchase of real estate	0,15
Transport of cash	0,10
Consumer credit	0,10
Mortgage credit	0,10
Fiscal regularisations	0,05
Other	1,09
Total	**100**

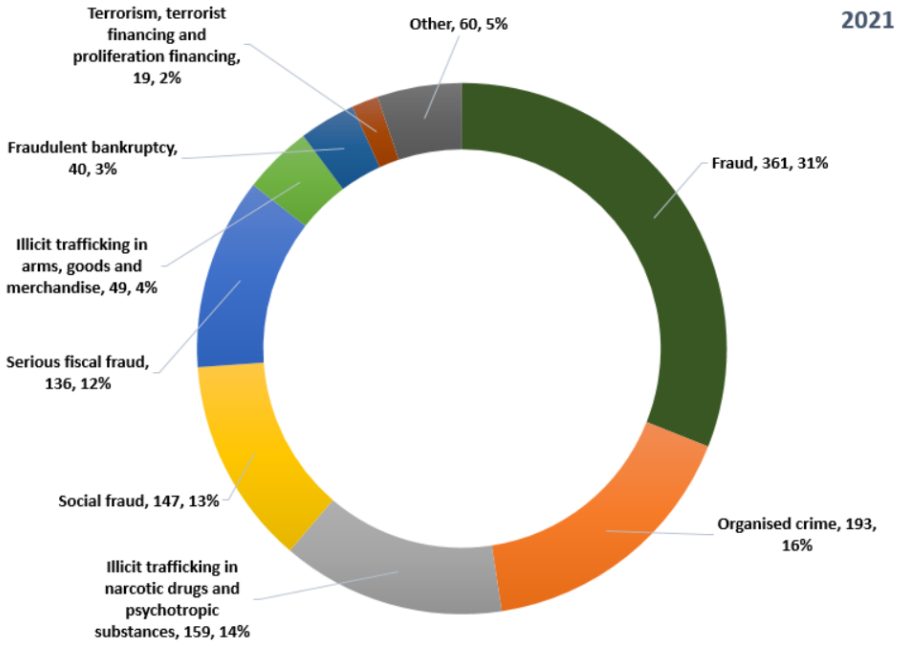


4. Financial flows (origin and destination of international transfers)

Origin of the money	%	Destination of the money	%
Luxembourg	43,57	Luxembourg	34,40
Switzerland	17,40	United Kingdom	12,90
Rwanda	7,40	Switzerland	5,55
France	6,64	United Arab Emirates	4,83
Netherlands	4,31	Netherlands	4,76
Germany	2,56	Germany	4,51
Liechtenstein	1,51	China	4,37
Italy	1,46	Liechtenstein	3,76
Cyprus	1,43	Poland	3,28
Other	13,72	Other	21,64
Total	**100**	**Total**	**100**

5. Predicate offences

Predicate offence	2019	Amount[36]	2020	Amount	2021	Amount
Fraud	210	61,05	251	61,70	361	628,15
Organised crime	103	151,09	125	226,21	193	549,07
Illicit trafficking in narcotic drugs and psychotropic substances	119	11,51	159	47,61	159	46,36
Social fraud	197	228,42	175	219,85	147	149,09
Serious fiscal fraud	99	311,87	171	704,10	136	486,50
Illicit trafficking in arms, goods and merchandise	46	299,71	44	148,23	49	382,61
Fraudulent bankruptcy	57	16,98	55	34,14	40	16,07
Misappropriation of corporate assets	64	30,49	72	16,33	38	24,17
Breach of trust	27	7,77	31	33,73	27	5,34
Terrorism, terrorist financing and proliferation financing	57	4,05	45	6,49	19	3,64
Exploitation of prostitution	24	4,66	22	4,06	12	1,44
Embezzlement and corruption	10	18,65	11	36,88	12	24,76
Theft or extortion	12	1,33	10	3,14	12	0,62
Trafficking in human beings	17	3,77	27	6,38	11	8,02
Smuggling of human beings	13	2,56	16	3,93	7	0,95
Other	10	4,75	14	83,71	18	10,16
Total	**1.065**	**1.158,66**	**1.228**	**1.636,49**	**1.241**	**2.336,95**



[36] Amount in million EUR. The amounts above are the sum of actual money laundering transactions and potentially fictitious commercial transactions. In these files (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.

The sharp increase in amounts identified for the predicate offence “fraud” is the result of the dissemination of a file with regard to the purchase/sale of masks in which the announced credit transaction of several million EUR was in reality never carried out.

In one and the same file CTIF-CFI may on the basis of its analysis conclude that there are serious indications of money laundering related to one or more predicate offences. It should be noted that CTIF-CFI does not have the same investigative powers as the judicial authorities and the police and works on the basis of indications and not yet of evidence.

CTIF-CFI can also identify one potential predicate offence (see table below) or multiple additional predicate offences.

The table below provides an overview of the main and additional predicate offences combined.

Predicate offences	Total number of files 2021
Fraud	401
Serious fiscal fraud	314
Social fraud	249
Organised crime	239
Illicit trafficking in narcotic drugs and psychotropic substances	191
Illicit trafficking in arms, goods and merchandise	80
Misappropriation of corporate assets	54
Fraudulent bankruptcy	54
Breach of trust	37
Theft or extortion	22
Terrorism, terrorist financing and proliferation financing	20
Trafficking in human beings	19
Embezzlement and corruption	19
Exploitation of prostitution	18
Smuggling of human beings	13
Other	27
Total	**1.757**

6. Individuals 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 2021. These tables are intended to help reporting entities apply the statutory due diligence measures.

6.1. Residence

The lockdown, 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 2021, without being able to claim that solely these factors explain this ranking.

In 88,6 % of the files disseminated to the judicial authorities the individuals involved resided in Belgium, mainly in Brussels and Antwerp.

Country 2021	%	Breakdown Belgium	%
Belgium	88,66 ➔	Brussels	45,88
		Antwerp	15,02
		Oost-Vlaanderen	7,43
		Hainaut	5,38
		West-Vlaanderen	3,18
		Limburg	4,65
		Halle-Vilvoorde	8,08
		Liège	3,76
		Brabant Wallon	2,12
		Vlaams-Brabant	2,86
		Namur	0,73
		Luxembourg	0,66
		Eupen	0,25
France	1,63		
Germany	1,14		
Luxembourg	0,97		
Democratic Republic Congo	0,80		
Netherlands	0,69		
Portugal	0,62		
Spain	0,41		
Other	5,08		

6.2 Nationality

In 2021, 52 % of the main individuals involved were Belgian nationals, compared to 94 % in 2020 and 65% in 2019.

Nationality	%
Belgian	51,91
Romanian	8,04
Portuguese	6,65
Brazilian	4,64
Dutch	3,22
French	2,74
Italian	1,98
Turkish	1,98
Bulgarian	1,32
Moroccan	1,32
Albanian	1,11
Cameroonian	1,11
German	1,11
Other	12,87
Total	**100**

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.