FINANCIAL INTELLIGENCE GROUP

2017

FROM SUSPICION TO ACTION

Converting financial intelligence into greater operational impact

EUROPOL

Printed by the Publications Office in Luxembourg

Luxembourg: Publications Office of the European Union, 2017

Photo credits: Shutterstock, German Customs (p.21), Europol (p.37)

Print	ISBN 978-92-95200-82-1	doi:10.2813/568228	QL-01-17-932-EN-C
PDF	ISBN 978-92-95200-81-4	doi:10.2813/308061	QL-01-17-932-EN-N

CONTENTS

1 FOREWORD FROM THE DIRECTOR

Money laundering is one of the key 'engines of crime' sustaining global criminal business worth billions of dollars ([1]). The task of combating it has become more difficult, due to the increasingly global and virtual nature of financial services and the emergence of technology-enabled factors such as crypto currencies and anonymisation tools that frustrate the identification of beneficial owners. Controlling much of this mega-illicit activity are global money laundering syndicates, who offer their services at scale to criminal networks, and are highly adept at exploiting gaps in the financial system. These are the challenging conditions within which anti-money laundering (AML) arrangements currently operate that set a very high bar for success in curtailing the international flows of illicit funds.

The widespread acknowledgement of the importance of tackling criminal finances has led to the development of a global anti-money laundering framework. One of its cornerstones is the reporting of suspected criminal financial flows (known as STRs) from the private sector, acting as gatekeepers to the financial system and legal economy, to Financial Intelligence Units (FIUs). At EU level, this regime generates millions of suspicious transaction reports annually, however, in Europol's experience just a fraction of these (around 10%) lead to further investigation by competent authorities. Further down the line, the picture remains bleak, and Europol estimates that barely 1% of criminal proceeds in the European Union are ultimately confiscated by relevant authorities ([2]).

These stark findings make it impossible not to question why the success rate of the system is so poor and what can be done about it. Nobody doubts the importance of bringing order to systemic attempts to prevent the criminal misuse of the financial system, and efforts invested in the EU anti-money laundering regime have created a valuable framework. However, this framework needs better exploitation to make a more meaningful contribution to the fight against serious crime and to achieve real outcomes in combating the misuse of the financial system for money laundering, terrorist financing and other criminal activities.

Europol is uniquely positioned to see how financial intelligence, in particular relating to cross border criminal activity, assists investigators across Europe in dismantling organised criminal groups. From this vantage point, Europol also has a clear picture of the shortcomings of the current framework. The anti-money laundering regime still operates at a domestic level, and has not yet fully adjusted to the reality of a problem that is defined by its international nature. While structures exist to facilitate cross-border cooperation between national units, significant barriers in international cooperation and information exchange remain, revealing the urgent need for supranational overview in increasingly global markets.

Emerging threats also require that the regime adapts. Current efforts are ineffective to tackle burgeoning cyber-enabled crime and online frauds. These offences rely on the rapid transfer of funds across borders and out of the financial system before detection and, once moved, there is little hope of recovering them. The time taken to cooperate between the private sector, FIUs and law enforcement means that the speed of response is simply too slow to stem the flow of funds which move globally almost instantly.

Clearly there is no lack of activity, and a great deal of time and resources is put into sending, receiving and handling millions of reports each year. However, the fact that very few are either the result of a police-directed effort or the subject of any significant feedback indicates that resources may be misdirected. In law enforcement and intelligence communities an 'intelligence-led' approach of using enhanced knowledge of the threat to direct operational resources into the highest priority areas is at the heart of all counter-terrorist and other major security programmes. That these conceptual principles have not fully translated in to the anti-money laundering regime partly reflects poor outcomes.

New 'intelligence-led' approaches to tackle financial crime are needed to achieve better outcomes. Some green shoots of positive change are emerging, including initiatives under the 4th EU AML Directive designed to improve the standard and practice of financial intelligence sharing, and proposals to establish centralised bank registers and an EU Financial Intelligence Unit. By placing emphasis on cultivating better data-sharing practices and an outcomes-focused, rather than process-driven regime, there is enormous scope to deliver real change.

Rob Wainwright
Executive Director of Europol

([1]) Europol Serious and Organised Crime Threat Assessment 2017 (SOCTA 2017): https://www.europol.europa.eu/socta/2017/

([2]) Europol reports *'Does crime still pay? Criminal Asset Recovery in the EU - Survey of Statistical Information'* https://www.europol.europa.eu/newsroom/news/does-crime-still-pay and *'Why is cash still king: a strategic report on the use of cash by criminal groups as a facilitator for money laundering'* https://www.europol.europa.eu/content/why-cash-still-king-strategic-report-use-cash-criminal-groups-facilitator-money-laundering

2 KEY FINDINGS

- The structure of Financial Intelligence Units (FIUs), their activities, working practices, and methods of recording and analysing information vary considerably across the EU. There is limited harmonisation among EU Member States (MS) beyond the obligation to establish an FIU. This makes any comparison of the implementation and effectiveness of the EU anti-money laundering directives and the effectiveness of suspicious transaction reporting difficult, if not impossible.
- Just 10% of suspicious transaction reports (STRs) are further investigated after collection, a figure that is unchanged since 2006.
- Over 65% of reports are received by just two Member States - the UK and the Netherlands.
- The overall number of reports sent by the regulated sector continues to increase. In 2014, the EU FIUs received almost 1 million reports. Volumes are likely only to increase, in particular as virtual currency providers come into regulatory scope and services using distributed ledger technology (DLT) enter the mainstream.
- Between 0.7-1.28% of annual EU GDP is detected as being involved in suspect financial activity.
- Together banks and MSBs are the source of the majority of STRs sent to the FIUs. Certain sectors are noted for their low levels of reporting, in particular high value goods dealers and bureaux de change.
- Reporting on terrorist financing accounted for less than 1% of reports received by FIUs in 2013-14.
- The use of cash is the primary reason triggering reporting entities to report suspicion, however in Luxembourg, where cash issuance is almost double its GDP, the use of cash is not a common reason for reporting.
- The 'symmetrical' exchange of information between FIUs may prevent crucial information contained in STRs reaching authorities tasked with criminal investigations. Europol could assist in overcoming this barrier through acting as a pan-European hub for STRs enabling integration with other sources of information stemming from multiple agencies across Europe and beyond.
- New technology presents challenges to the current anti-money laundering framework. The increasing digitalisation of financial services results in growing volumes of transactions and extremely large data sets requiring computational analysis to reveal patterns, trends, and associations. The use of analytics is therefore becoming essential for both reporting entities and FIUs to cope with information and fully exploit its potential.
- The growing demand for online services and related internet payment systems poses considerable challenges to the EU policies concerning money laundering and terrorist financing. The development of borderless virtual environments call for reflection on how to adapt policies which are meant to be supervised only at national level, while the underlying business is already transnational and globalised in its own nature: there is an urgent need for a supranational overview.
- The embedment of the FIU.net project at Europol presents an opportunity for greater operational cooperation between FIUs and law enforcement.

3 ACKNOWLEDGEMENTS

Europol would like to extend sincere thanks to all the Financial Intelligence Units who contributed to the production of this report. Of course, our thanks also go to the reporting entities that are the ultimate source of information, which can be of such high value in effectively combating organised crime groups and terrorist organisations.

4 INTRODUCTION

Almost all organised criminal groups (OCGs) carry out their activities for one reason: profit. Criminal finances encompass both the crimes that generate vast sums and the methods used to launder these in order that they can be enjoyed and reinvested.

The widespread acknowledgement of the importance of tackling money laundering and criminal proceeds has led to a greater emphasis on conducting financial investigations and gathering financial intelligence. In response, a global anti-money laundering framework has developed over time, and one of its cornerstones is the reporting of suspected criminal financial flows (known as STRs) from the private sector, acting as gatekeepers to the financial system and legal economy, to Financial Intelligence Units (FIUs).

The reports sent by the private sector contain valuable information that can enhance ongoing investigations and often trigger entirely new ones. A number of cases have demonstrated the importance of this system: it would not be possible to effectively combat OCGs operating in the EU or affecting the EU from abroad without pursuing their finances, both for intelligence purposes and as a target.

4.1 AIMS AND OBJECTIVES

While most FIUs publish annual reports that provide a domestic picture of STR reporting, there is no overview at EU level. Europol's Financial Intelligence Group regularly monitors and prepares reports on the extent of suspicious transaction reporting (STRs) in the European Union, with a view to providing this pan-European perspective. This report seeks to provide insight into the extent of suspicious transaction reporting in the EU and highlight noteworthy trends and developments.

Europol is uniquely positioned to see how STRs, in particular relating to cross-border criminal activity, assist investigators across Europe in dismantling OCGs. This report provides a law enforcement perspective on the benefits and shortcomings of the current framework regarding the use of STRs to combat organised crime and terrorism.

As the STR regime in the EU is in place to combat the misuse of the financial system for money laundering, terrorist financing and other criminal activities, the findings of the report also focus on recommendations to improve the regime's effectiveness in achieving this goal.

In addition, the report contains a number of case examples that show the benefit that can be derived from STRs – not only limited to the investigation of money laundering, but also demonstrating the value of financial intelligence to all investigators more generally.

Europol's Financial Intelligence Group and Analysis Project Sustrans

Europol's Financial Intelligence Group, established in 2012, incorporates three distinct areas with a view to strengthening Europol's capacity to combat organised crime and terrorism through financial intelligence and investigations: Analysis Project (AP) Sustrans, dealing with money laundering; AP Asset Recovery, dedicated to tracing and recovering criminal proceeds, and FIU.net, focusing on cooperation and information exchange among EU FIUs.

As Europol's project dedicated to money laundering, AP Sustrans is an operational platform to support Member States' on-going cases in the area of money laundering. It was established in 2001 in compliance with the Amsterdam Treaty in view of providing EU Member States with a pan-European platform to integrate and analyse dedicated financial data. AP Sustrans provides a platform through whi ch operational data pertaining to Suspicious Transaction Reports filed by FIUs, reports on cash detections (usually from Customs authorities) and on-going money laundering investigations from all relevant agencies (including but not limited to Customs, Tax and Police services) across the EU and beyond are analysed and developed. This assists in developing the picture of criminal activity across Europe, for example through revealing links with your case to STRs in the Netherlands, cash seizures in France or on-going investigations in Poland. The Analysis Project plays a role in the timely dissemination of STR data to investigators across Europe in support of their on-going investigations.

5 WHAT ARE STRs?

There is no single name for, or definition of, a suspicious transaction report ((STR), often known as a suspicious activity report (SAR)). However, it is generally understood to mean a report compiled by the regulated private sector (most commonly banks and financial institutions, but also non-financial designated professions) about financial flows they have detected that could be related to money laundering or terrorist financing ([3]).

In 1989 the Financial Action Task Force (FATF) - an inter-governmental body - was created. Since then it has set international standards in the fight against money laundering, and their recommendations form a blueprint for the EU's anti-money laundering framework. FATF's recommendations and the need for a more unified approach to anti-money laundering across the EU led to the First European anti-money laundering Directive in 1991. The Directive (updated three times in 2001, 2005 and most recently in 2015) underpins the EU anti-money laundering framework in place today, through minimum requirements to be implemented by the EU Member States. The Directive created the master design for the current EU anti-money laundering architecture. A cornerstone of this framework is the designation of entities obliged to report suspicious transactions to a central authority, known as a Financial Intelligence Unit (FIU).

It is one of the areas in which bodies set up to counter organised crime and terrorism rely heavily on the efforts of the private sector: the anti-money laundering framework entrusts them with significant responsibility for policing the financial markets.

The STR regime exists to prevent and detect the abuse of the financial system by criminal groups seeking to launder the profits of illegal activities. The system ultimately aims at maintaining the integrity of the financial markets, with relevant reports reaching those tasked with investigations, while balancing the need to protect the privacy of innocent citizens.

These reports can bring significant operational benefit. The reports Europol receives from only a handful of FIUs generate thousands of links with ongoing cross-border investigations providing crucial leads and evidence for investigators.

([3]) Please see definitions section for a more detailed explanation of STRs.

Why are STRs useful?

In 2014 the Tax and Customs Authority in one MS conducted a key anti-money laundering operation that culminated in the provisional arrest of the former Prime Minister.

The case was an investigation related to tax fraud, corruption and money laundering, involving sums in excess of 20 million euros.

The role of STRs in the case was pivotal: the entire investigation was initiated because of a set of STRs filed by banking entities, informing that EUR 600 000 had been deposited by way of structuring into the bank account of a former Prime Minister. Sums were transferred from his mother's bank account, justified by way of the sale of an apartment (which was over invoiced) to the former politician's close friend.

On-going investigations indicated that this close friend was in fact a front man, used to manage an amount of EUR 20 million belonging to the former Prime Minister – sums incompatible with his declared income and corruption seen as the probable source of funds.

The reporting behind the case revealed the use of several money laundering methods including: the use of front men to manage bank accounts; fake and over-invoiced purchases to justify the integration and use of funds; false employment and service contracts; the use of cash couriers to transport money between the front men and the beneficial owner.

6 HOW MANY REPORTS ARE SENT?

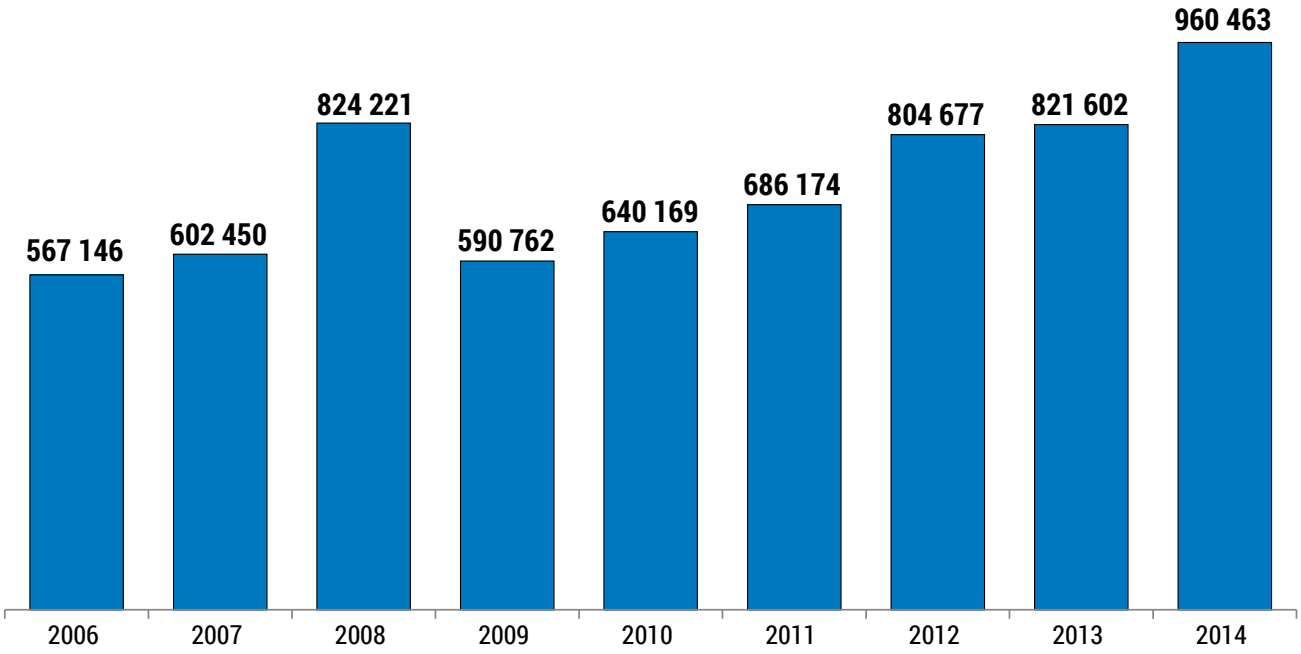
Across the board, the regulated sector is sending almost 70% more reports than in 2006. In 2014, the private sector filed almost 1 million reports across the 28 EU Member States, almost double the number received in 2006.

The ever-increasing reports sent indicate that certain reporting entities take their obligation very seriously and have invested significant resources to improve reporting. This has resulted in a steady increase in reporting volumes from obliged entities since the introduction of the First EU anti-Money Laundering Directive.

Chart 1 shows the total number of reports filed by the regulated sector from 2006 – 2014. There has been a continuous rise in the total volume of STR reports filed throughout this period ([4]).

([4]) The sharp increase in 2008 is due to figures reported by the Dutch FIU, which received over 175 000 outstanding reports retrospectively filed in 2008.

Chart 1([5]) — Total annual reports across all Member States (2006 - 2014)



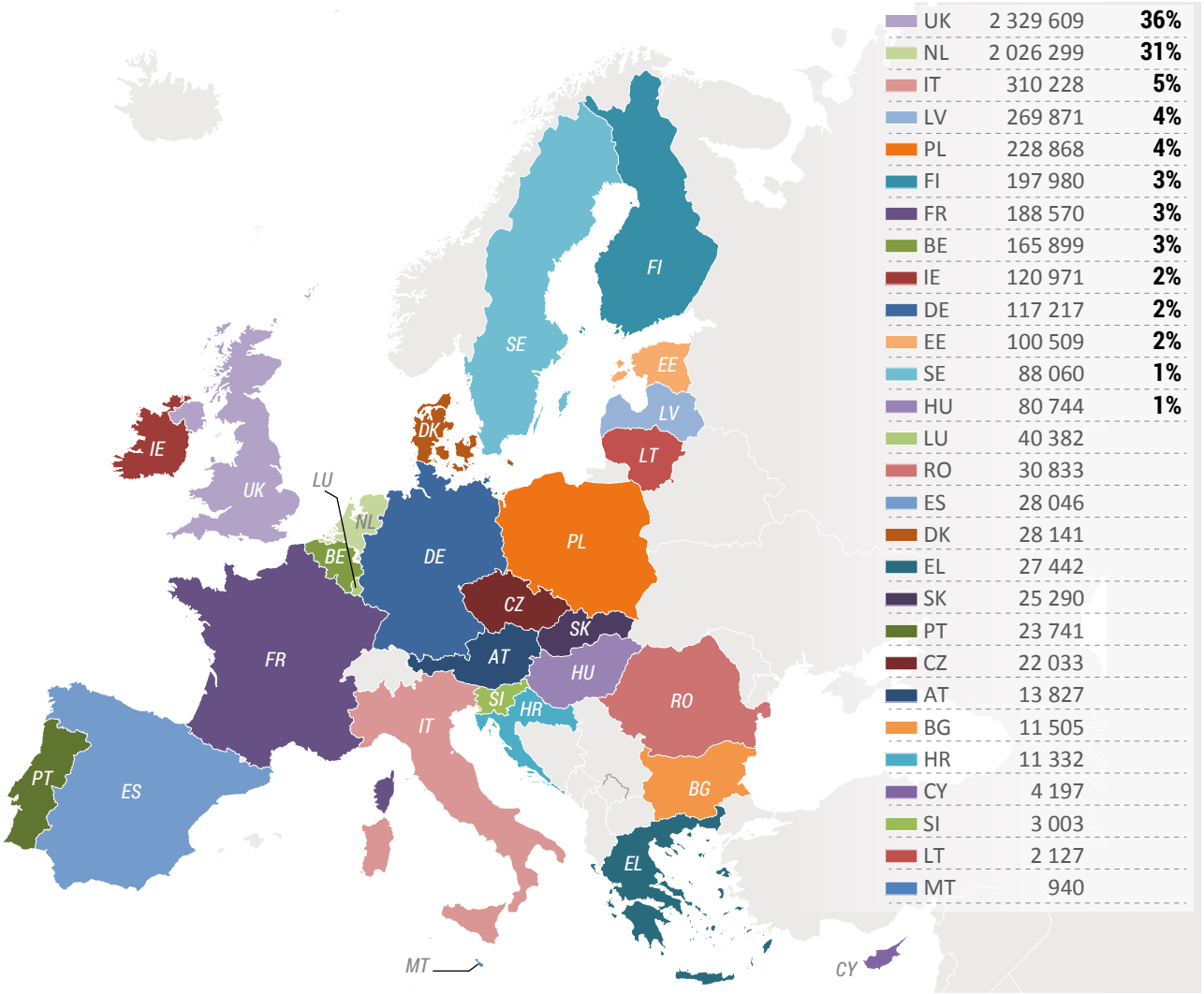
([5]) Chart shows total number of reports received by an FIU, regardless of whether these relate to activity, transactions, or the degree of suspicion required in order to submit a report (which varies across the EU).

Reporting entities are expected to report domestically to their home authority (the country in which they are registered). As such, the size of the financial market in a country, as well as differences in reporting thresholds, the interpretation of suspicion, and the quality of awareness and supervision by FIUs and supervisory authorities means that there are significant differences between the volumes of reports sent from one country to another.

In fact, two countries alone account for 67% of all reports filed in the EU: the UK and the Netherlands ([6]), as shown in Chart 2.

([6]) The Netherlands operates an unusual transaction reporting regime, based on objective indicators with little analysis conducted by entities, hence the high numbers. It should be stressed that it is only incumbent on the FIU to declare a report as suspicious.

Chart 2 — Total reports across all Member States (2006 - 2014)



The number of reports filed across the EU has steadily increased since 2006; however, over 65% of all reporting in the EU is accounted for by just two Member States, the Netherlands and the UK

It is of course understandable that the UK would generate one of the highest reporting volumes in the EU: not only is it home to one of the largest financial markets in Europe, but in addition, it operates a Suspicious Activity Regime (SAR), which broadens the types of reports it can receive. Nonetheless, the figures are extremely high in comparison to other countries, which may also be a result of defensive or over reporting([7]).

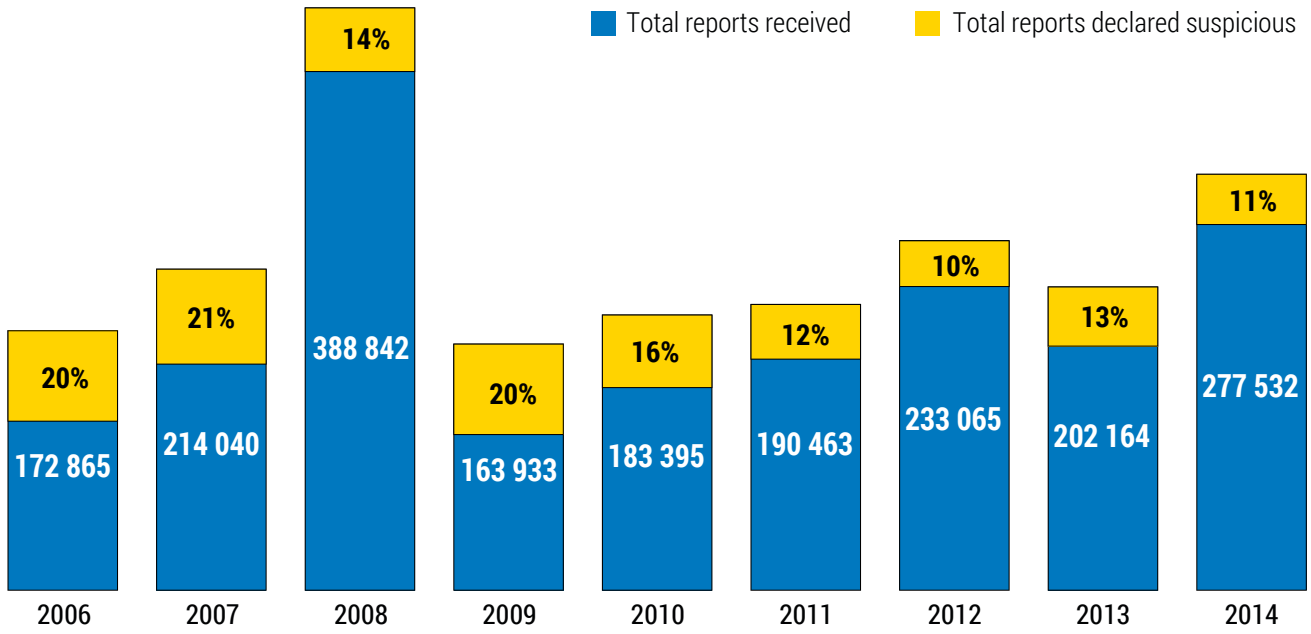
Reporting volumes in the Netherlands, given the size of its territory, population and financial sector, are anomalous. The very high number of reports received by the Dutch FIU can be explained by way of the fact that they do not receive STRs, but rather Unusual Transaction Reports (UTRs) from reporting institutions. The vast majority of these reports stem from money transfer offices that are obliged to report all transactions in excess of EUR 2000 ([8]). After investigation by the FIU, an unusual transaction may be declared suspicious and all STRs are forwarded to investigation services. Only a small proportion of the reports received by the Dutch FIU are declared suspicious (on average around 15%), meaning that much of the reporting is rarely utilised for investigative purposes ([9]).

([7]) Although reporting guidance from the FCA, JSMLG and NCA is quite comprehensive on obligations and the UK FIU analysis of reports suggests that the majority of the financial institutions that submit SARs conduct at least a basic level of research and analysis prior to submission, and in some cases undertake quite substantial pre-submission examination.

([8]) https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5276-fiu_jaaroverzicht_2014-engelsweb2.pdf

([9]) Nonetheless, UTRs are continuously assessed and the Dutch FIU does use UTRs to inform supervisory bodies of the AML/CFT framework, produce strategic analyses and detect new developments and trends.

Chart 3 — Proportion of reports received by Dutch FIU categorised as suspicious



Certainly, it seems disproportionate that over two thirds of all reports are filed with just two FIUs in the EU.

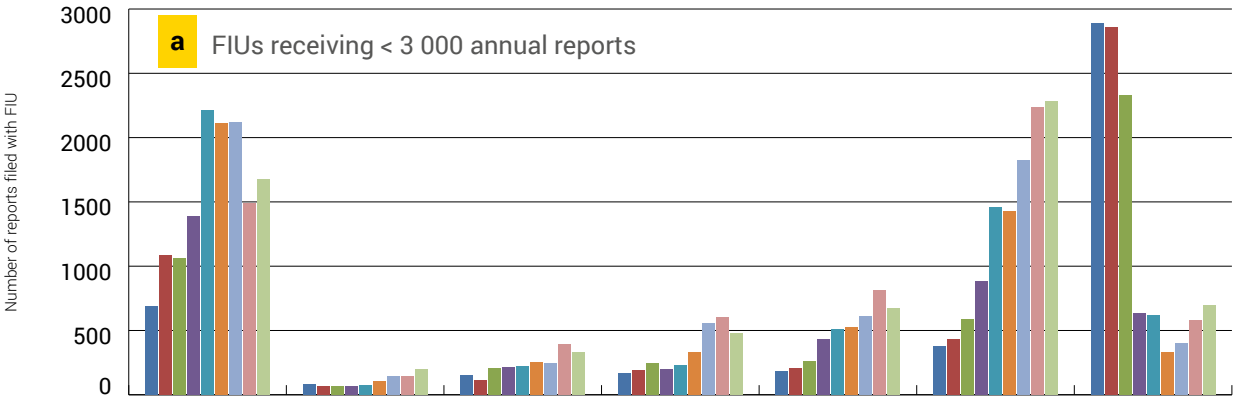
Even disregarding the UK and the Netherlands, we see that reporting figures across the EU are not always in line with what one might expect to see, given the extent of the regulated sector in particular jurisdictions. While volumes reported in Italy and France appear to reflect the size of those countries' regulated sectors, certain other jurisdictions, notably Cyprus and Malta, receive very few reports given the size of their banking sectors and the significance of these jurisdictions in offshore financial services. At first glance, reporting volumes in Luxembourg do not seem unusual, however the vast majority of reports stem from electronic bank/payment service providers, in spite of the fact that other sectors, such as private banking and offshore financial services, offer significant scope for money laundering activities and tax crimes.

In contrast to the general trend of a steady increase in reporting volumes, a number of countries have registered decreases in the volumes of reports received in recent years (2013/2014) by comparison to 2006 (notably the Czech Republic, Hungary, Latvia, Luxembourg and Poland). This matter is largely accounted for by changes to reporting entities' automatic monitoring systems to fine-tune the quality of reporting. For example, Luxembourg, who receives the majority of its reports from one single electronic bank, saw a dramatic drop in the number of reports filed in 2013/14 (resulting in a decrease of almost 50% for 2013 as compared to 2012) due to changes made to the monitoring systems of that reporting entity. However, it remains that by comparison with reporting volumes in 2006, the number of reports received by the Luxembourg FIU have dramatically increased. This is again, largely as a result of the policy of the same reporting entity, an electronic bank, which accounts for the majority of all reports received by the FIU.

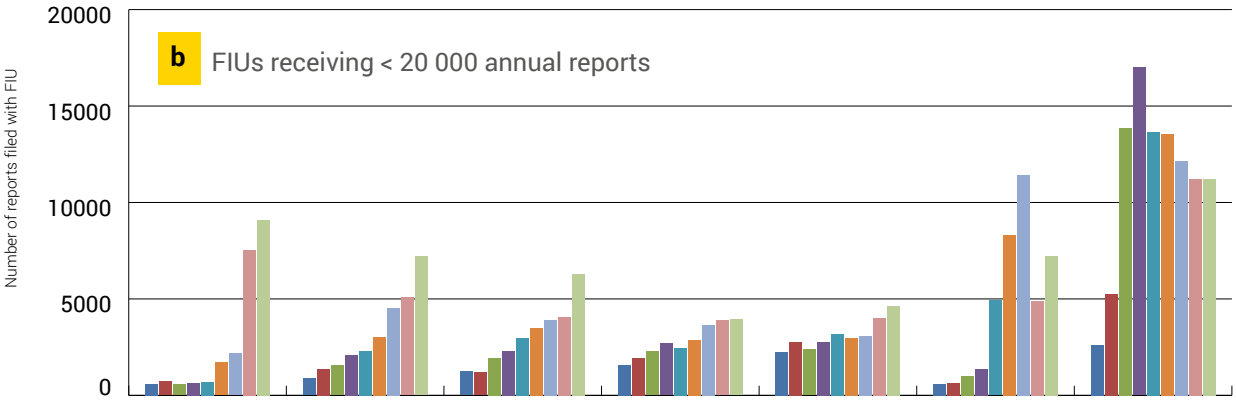
While on the face of it increased reporting is an indication of the improvement of the STR regime, demonstrating great engagement and commitment from the private sector, consideration also needs to be given to the quality of these reports and FIUs' capacity to handle these ever increasing streams of data. These aspects are addressed in more detail in further sections of this report.

Charts 4 (a, b, c, d and e) show the number of reports filed annually in each Member State, from 2006 – 2014, including figures. These have been grouped by annual volumes received in order that trends in increases and decreases by country can be observed.

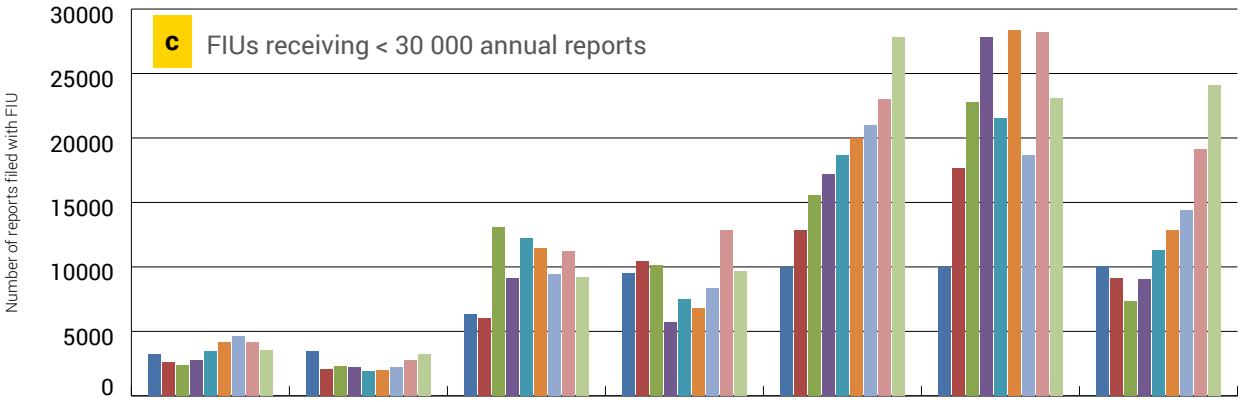
Charts 4 (a, b, c, d and e) — STR Reporting per Member State - 2006 - 2014



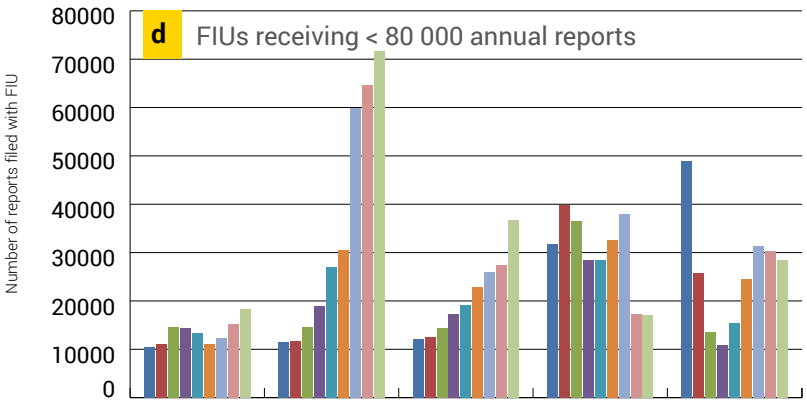
	AT	MT	LT	SI	CY	BG	HR
2006	691	78	153	165	179	374	2 891
2007	1 085	63	115	192	204	431	2 858
2008	1 059	69	203	248	258	591	2 327
2009	1 385	63	213	199	428	883	635
2010	2 211	73	222	233	510	1 460	615
2011	2 115	107	255	327	526	1 428	334
2012	2 118	142	245	559	610	1 821	397
2013	1 490	143	393	600	809	2 233	577
2014	1 673	202	328	480	673	2 284	698



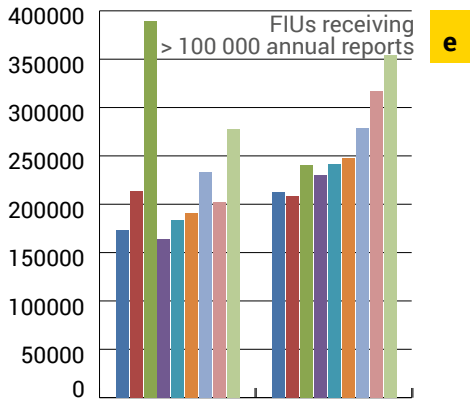
	PT	DK	GR	SK	ES	LU	EE
2006	584	876	1 236	1 571	2 251	574	2 601
2007	724	1 349	1 179	1 943	2 783	646	5 272
2008	568	1 553	1 952	2 274	2 380	1 008	13 861
2009	634	2 095	2 304	2 686	2 764	1 368	16 999
2010	703	2 316	2 982	2 470	3 172	4 915	13 655
2011	1 699	3 020	3 507	2 882	2 975	8 306	13 536
2012	2 168	4 511	3 923	3 650	3 059	11 436	12 157
2013	7 554	5 080	4 071	3 886	4 025	4 891	11 224
2014	9 107	7 199	6 288	3 928	4 637	7 238	11 204



	RO	CZ	SE	HU	BE	FI	DE
2006	3 196	3 480	6 353	9 475	9 938	9 975	10 051
2007	2 574	2 048	6 040	10 456	12 830	17 658	9 080
2008	2 338	2 320	13 048	10 091	15 554	22 752	7 349
2009	2 771	2 224	9 137	5 683	17 170	27 836	9 046
2010	3 477	1 887	12 218	7 486	18 673	21 490	11 313
2011	4 116	1 970	11 461	6 776	20 001	28 373	12 868
2012	4 637	2 191	9 436	8 304	21 000	18 677	14 361
2013	4 170	2 721	11 185	12 855	22 966	28 157	19 095
2014	3 554	3 192	9 182	9 618	27 767	23 062	24 054



	IE	IT	FR	LV	PL
2006	10 403	11 451	12 047	31 840	48 848
2007	11 145	11 724	12 481	39 877	25 653
2008	14 505	14 602	14 465	36 418	13 586
2009	14 400	18 822	17 310	28 492	10 904
2010	13 416	26 961	19 208	28 499	15 357
2011	11 168	30 447	22 856	32 649	24 408
2012	12 390	59 862	26 011	37 887	31 395
2013	15 242	64 601	27 477	17 168	30 212
2014	18 302	71 758	36 715	17 041	28 505



	NL	UK
2006	172 865	213 000
2007	214 040	208 000
2008	388 842	240 000
2009	163 933	230 378
2010	183 395	241 252
2011	190 463	247 601
2012	233 065	278 665
2013	202 164	316 527
2014	277 532	354 186

7 WHO SENDS THEM?

7.1 REPORTING ENTITIES

All EU FIUs report that credit institutions and banks are the primary source of the STRs they receive

The Fourth anti-Money Laundering Directive sets out those sectors, both financial and non-financial, which have obligations to file reports around suspicious transactions or activities with their national FIUs ([10]). Some countries may also implement further categories of obliged entities through domestic legislation (for example, Spain includes NGOs and security and cash transport companies).

Credit institutions and banks remain overwhelmingly the most significant reporting sector. Money transfer services, such as money remitters and money service businesses, also account for a significant proportion of reports filed within the EU. All EU FIUs report that credit institutions and banks are the primary source of the STRs they receive, while 80% cite money remitters as the second most significant category of reporting entity.

As regards the designated non-financial sector ([11]), three categories of obliged entities report most frequently to the FIUs – the gambling industry, public notaries and accountants. However, professional gatekeepers, who play a pivotal role in preventing the misuse of the financial system, do not perform the same function across every country in Europe. In some countries, such as France, a public notary is an official of integrity appointed by the state, officially required for the signing of documents where they play a crucial role in all matters relating to property sales. In other countries this is not the case, where this role falls instead other members of the legal profession, such as solicitors, who report far less.

The gambling industry, given that casinos are by nature cash-intensive businesses, is of course very attractive to criminals who want to launder ill-gotten proceeds. While the scope of the Third anti-Money Laundering Directive only covered physical casinos, the Fourth Directive extends the scope to the gambling sector more generally, including both online and bricks-and-mortar casinos and gambling services providers. As such it is highly likely that there will be an increase in reports from the gambling sector in the near future, which may affect particular European Member States who have a significant online gambling sector, for example Malta.

([10]) Article 2: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L0849&from=en/

([11]) FAFT Recommendation 22 encompasses the following designated non-financial businesses and professions: casinos; real-estate agents; dealers in precious metals and dealers in precious stones; lawyers, notaries, other independent legal professions and accountants; trust and company service providers. However each country can designate additional non-financial businesses and professions, as deemed relevant.

Case example: Operation Gambling

A recent case reported across open sources deals with the Italian Operation Gambling in which Italian authorities arrested 41 persons and seized assets worth EUR 2 billion in a massive illegal gambling and money laundering operation ([12]).

Italian authorities took down a huge network of companies involved in online betting, headquartered in Malta and controlled by the 'Ndrangheta, the notorious Calabrian criminal organisation. Police believe the firms, including the six that were operating out of Malta, were used to launder vast sums of illicit cash.

The case has raised some concerns around the online gambling market and the potential for its abuse by criminal organisations. The implementation of the Fourth anti-Money Laundering Directive which extends scope beyond physical casinos to the gaming sector more generally, may have a significant effect on Malta given the size of its online gambling industry (with over 400 licences granted).

([12]) http://www.timesofmalta.com/articles/view/20150722/local/companies-in-malta-have-assets-seized-licences-suspended-over-alleged.577658 http://calvinayre.com/2015/09/14/business/italys-operation-gambling-yields-e25m-in-asset-freeze/

Chart 5 ([13]) — Most Frequent Reporting Entities in 2013/2014 (Financial Sector)

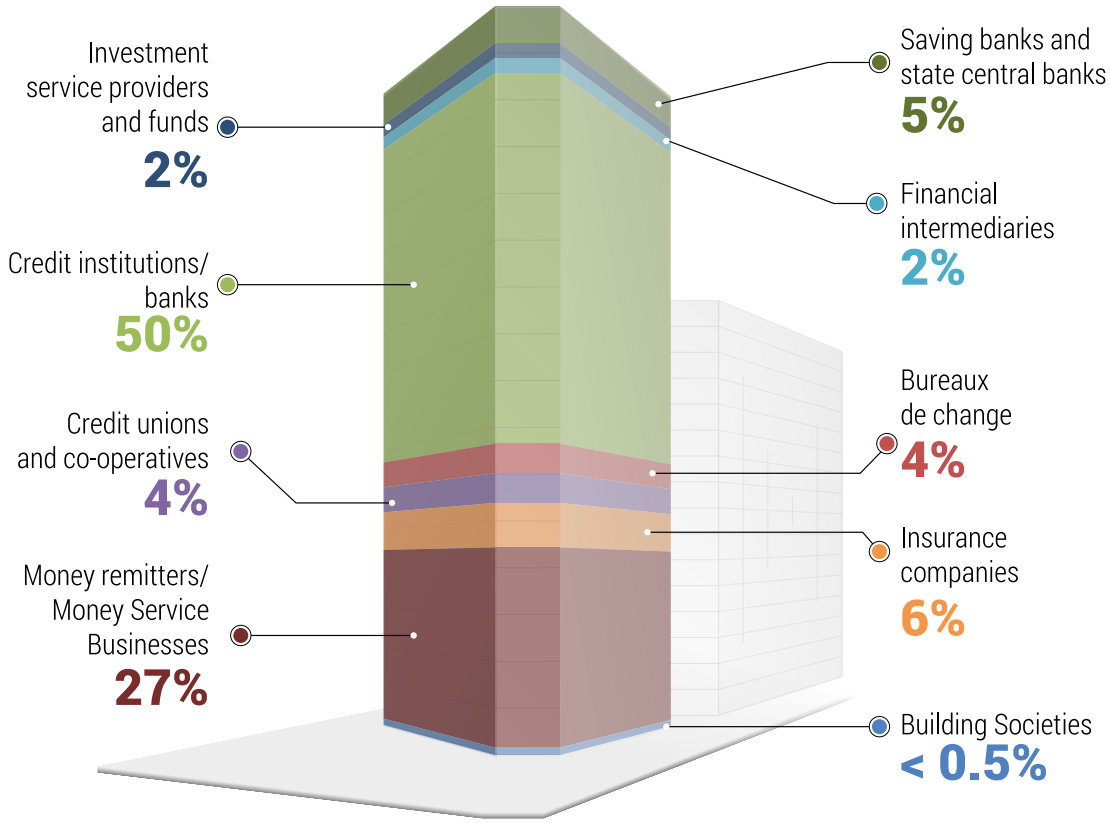
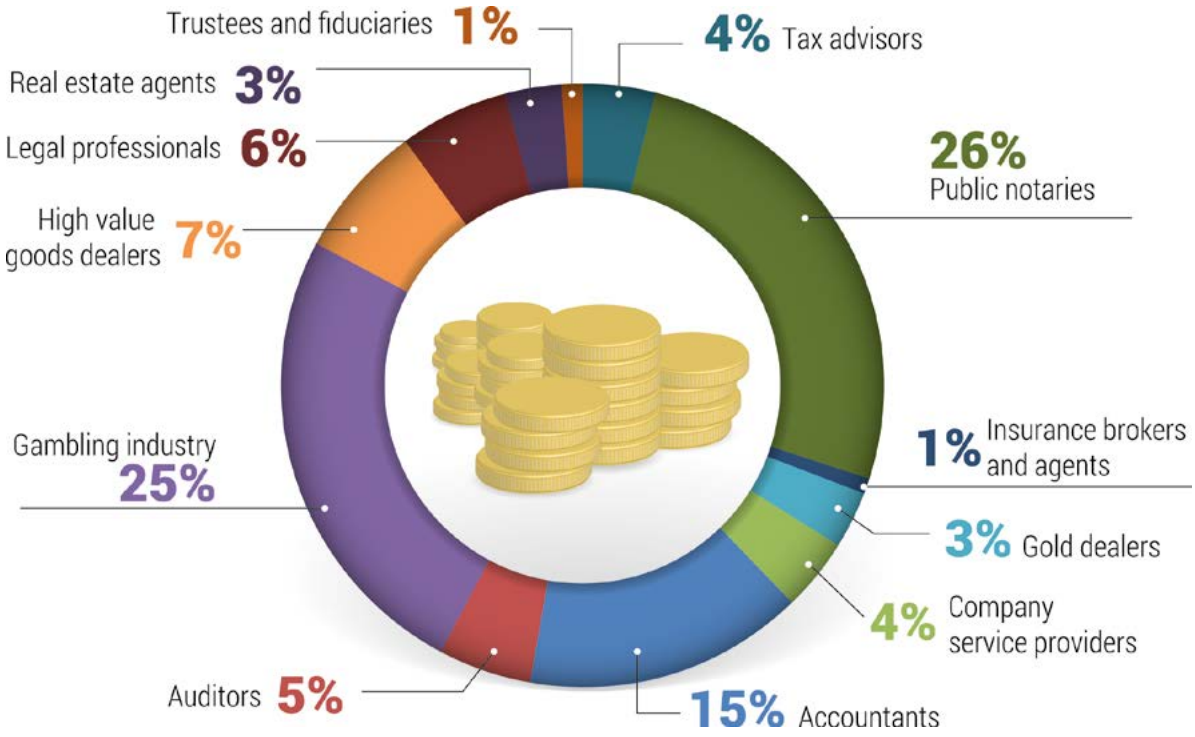


Chart 6 — Most frequent reporting entities 2013/2014 (Designated non-financial sector)



([13]) Charts 5 and 6 represent the proportion of FIUs citing the obliged entities as the most significant reporting sector.

High value goods dealers: Operation Cedar

On 24 January 2016, law enforcement and judicial authorities from France, the US, Germany, Belgium, Italy, the Netherlands and Spain, supported by Europol and Eurojust, took action against a prominent OCG responsible for the laundering of profits from cocaine sales throughout Europe.

Building on long-standing ties to South American drugs cartels, the OCG's modus operandi involved the use of cash couriers travelling across Europe by car to collect the proceeds of crime, followed by the purchase of expensive cars, luxury watches and jewellery. These high value goods were then exported to Lebanon where they were sold and the proceeds placed into the financial system for onward transfer to cartels in South America.

Financial investigations revealed that in 2014 alone, the group spent EUR 26 million in cash to purchase luxury watches, without triggering any STRs. The sums involved in 2015 are thought to have been even higher, by which time the group was laundering an estimated EUR 1 million per week.

The targeted OCG was mainly composed of Lebanese nationals also suspected of being involved in financing terrorism through Hezbollah's military wing. In the wake of coordinated days of action, one of the main suspects of Operation Cedar was designated by US OFAC (Office for Foreign Asset Control) for his involvement in the financing of terrorist activities ([14]).

Certain sectors, by contrast, are noted for their low levels of reporting. Bureaux de change, for example, emerge as a sector which rarely files reports with the competent FIUs. High value goods dealers are noted as the least frequent reporting category of designated non-financial business. The Fourth anti-Money Laundering Directive reduces the reporting threshold for high value goods dealers from EUR 15 000 to EUR 10 000. While this should mean that there will be greater onus on this under-reporting sector to alert the FIU to suspicious cases, it is generally accepted among law enforcement authorities (LEAs) that EUR 10 000 is still a very high threshold, that it is not in-keeping with some domestic cash payment thresholds that are as low as EUR 1000. Corporate Service providers, another reporting group which plays a pivotal role in preventing the misuse of the financial sector and ensuring that beneficial ownership can be traced, are also categorised as under-reporting entities. However, it is expected that central business registers required by the Fourth anti-Money Laundering Directive may help to mitigate some risks.

Evident discrepancies also emerge when comparing information provided by different countries: certain sectors, such as the gambling sector, appear simultaneously as the most and least frequent reporting entities depending on jurisdictions. This can only be explained by regional variations (for example under-reporting or lack of presence in one country versus over-reporting or a strong presence in another). These discrepancies are only seen in the non-financial sector, where the level of technical compliance to FATF recommendation 22 may be poor, leading to less uniformity in reporting entities than in the financial sector.

([14]) https://www.treasury.gov/press-center/press-releases/Pages/jl0331.aspx#.Vqp00KpE_ls.twitter

Chart 7([15]) — Least Frequent Reporting Entities 2013/2014 (Financial Sector)

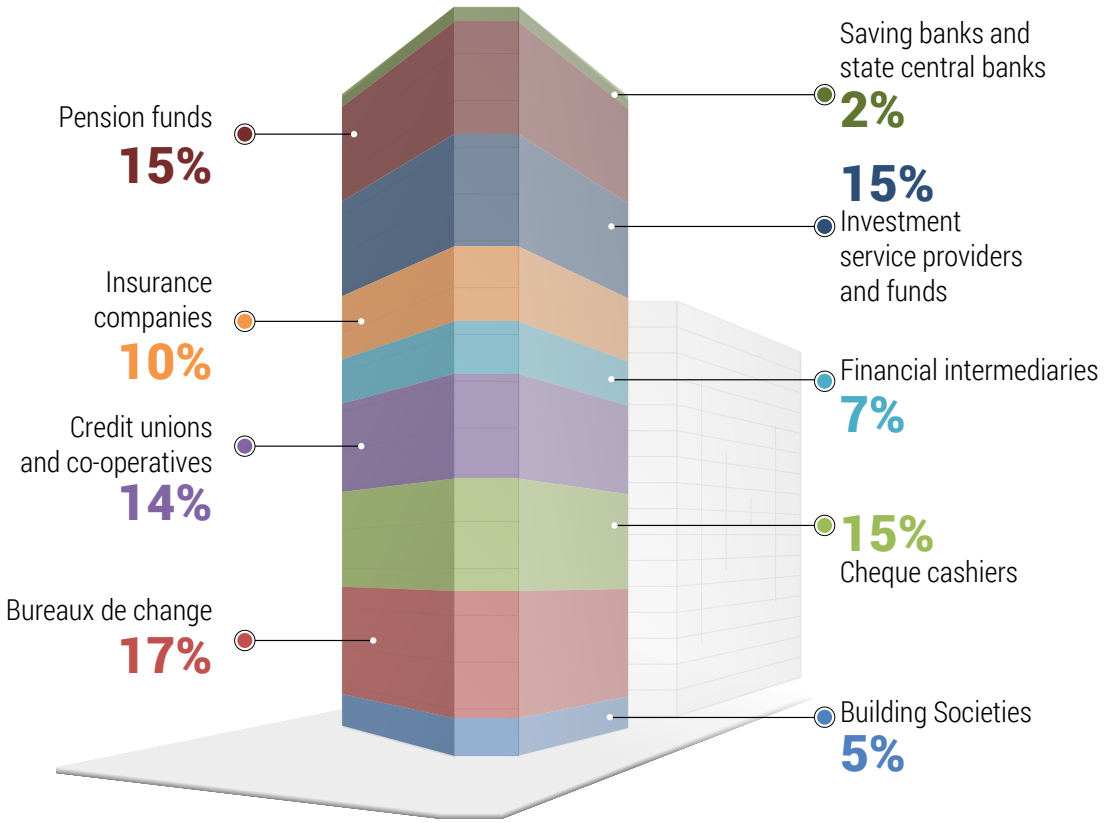
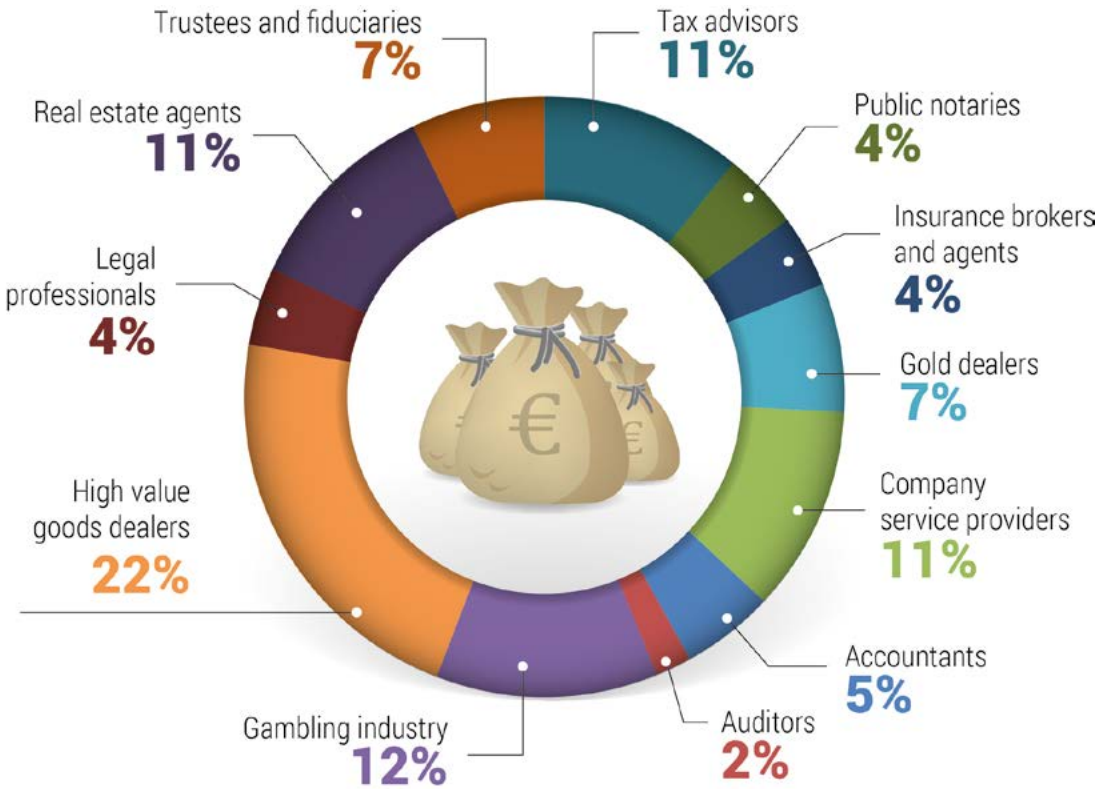


Chart 8 — Least Frequent Reporting Entities 2013/2014 (Designated non-financial sector)



([15]) Charts 7 and 8 represent the proportion of FIUs citing the obliged entities as the least significant reporting sector.

7.2 UNREGULATED SECTORS

A number of entities which have the potential to be exploited for money laundering and terrorist financing are not yet covered by the EU Directive (although in a limited number of cases, such entities may be captured by national legislation).

EU FIUs noted, in particular, the added value they potentially see in receiving reports from certain categories of non-obliged entities given that these sectors present significant vulnerabilities for money laundering and/or terrorist financing. Examples include virtual currency exchangers, NGOs, and security and cash transport companies (only Spain reported that the latter two categories are obliged entities under national AML legislation).

The recently proposed amendments to the Fourth Anti-money Laundering Directive intend to add virtual currency exchange platforms as well as custodian wallet providers to the list of obliged entities.

Unregulated Bitcoin exchanges

To operate with virtual currency, users need to place funds in and out of their accounts/wallets. Cashing in and out of a virtual currency account can be done in a number of ways. While licensed banks or MSB transfers are commonly used, other methods include credit cards and debit cards, prepaid cards, electronic money, money orders and mobile telephone transfers. Possibilities also exist for unlimited peer-to-peer transfers. Naturally, these different methods of crediting and debiting accounts present different risks that have a significant impact on the scope for money laundering and possibilities for financial investigations.

Typically, third party exchangers are used for this process of obtaining virtual currency or converting it to 'real world' money. In some countries these exchangers are already subject to regulation, however there is no uniformity across the EU. Increasingly, virtual currency exchangers aim to comply with AML requirements regarding customer due diligence and transaction monitoring. While there may be some dubious providers, many have shown themselves to be willing and capable of supporting LEA investigations.

In one instance, Europol became aware of information held by a virtual currency exchanger, which, given its country of incorporation and current legislation regarding STR reporting obligations, was not required to file reports. In spite of this fact, the exchanger in question conducted customer due diligence and account monitoring, and was keen to notify law enforcement of transactions they believed to be connected to criminal activities. Analysis conducted by the exchanger revealed that many of the transfers received on a customer's account originated from illegal markets on the dark web. It transpired that, by pure coincidence, Europol had been informed just days before about a money laundering and drug trafficking investigation in which the same individual was mentioned as an associate of the OCG. The information provided by the exchanger could confirm his role as a launderer and the exchanger was even able to provide a full package of information to assist LEA with following the money flows. As such, the value of enabling the widest audience to report, and in fact obliging them to do so, is put in relief.

7.3 CASH DECLARATIONS AND CASH SEIZURES

The regulated sector is not alone in sending reports to FIUs. Given the continued importance of cash in money laundering schemes, Customs agencies recording cash declarations also send reports.

The risk that the implementation of the EU anti-money laundering Directive could cause a shift away from the financial system towards other means of laundering criminal profits, in particular cash movements, led to the introduction of a complementary piece of legislation: Cash Control Regulation 1889/2005. This regulation establishes the requirement to declare all sums of cash in excess of EUR 10 000 entering or exiting the EU. Beyond Regulation 1889, some countries also have national provisions that oblige travellers to declare sums of money over a certain threshold when moving inside the EU territory.

Declarations, if properly analysed and utilised, can provide significant insight into patterns of possible criminal money flows.

The majority of FIUs in the EU state that they receive reports around cash declarations (usually provided by Customs); only five FIUs reported that they are not in receipt of cash declarations. However, of the 23 FIUs which reported receiving cash declaration reports, only 10 of these receive all declarations, while the rest receive only those declarations deemed suspicious by Customs. Given that few Customs agencies have access to FIU or police databases, it is highly probable that information which may help to establish suspicion in the first place may not be accessible to them.

In total, FIUs reported that they received records of 68 712 cash declarations in 2013 and 65 556 records in 2014. Of these declarations, 2266 and 2290 were further investigated by the FIUs in 2013 and 2014 respectively, the majority of which were subject to an administrative process.

Chart 9 — Total number of declarations received by FIUs and total number investigated

	2013	2014
Number of declarations	68 712	65 556
Number investigated	2266	2290

The picture around cash seizures is less complete and only 16 FIUs receive any data on cash seizures.

What happens with cash declarations and seizures sent to the FIUs varies. Other research conducted by the Financial Intelligence Group indicated that there is a lack of information exchange between the various authorities involved in controlling and investigating suspect cash movements. Frequently, information which could shed some light on the possible criminal origin of suspicious cross-border cash movements may be contained in databases of one agency (e.g. FIU, police, customs, revenue services, etc.) which is inaccessible to another: in response to a Europol survey, fewer than half of the MS Money Laundering Units reported having access to information contained in cash declarations, while the majority considered it would be beneficial to their investigations. Similarly, half of MS Money Laundering Units reported none, no direct, or limited access to STRs. Given that these three sources of information (cross-border cash movements, STRs and on-going investigations) combine to give a complete picture of the criminal activity with regards to money laundering, few countries dispose of a framework furnishing any single authority with a comprehensive and complete overview.

While customs databases collate some data stemming from declarations made under Regulation 1889/2005, this data is not transferred to or compared with police databases. As such, the potential criminal implications of such declarations cannot always be corroborated. Certainly better interconnection between databases would enable a fuller exploitation of this information to detect instances and indications of money laundering and terrorist financing. The use of Europol as a pan-European intelligence hub for data on suspicious cash movements could provide a possible solution for relevant stakeholders involved in cross-border cash movements.

Patterns in declarations: Cash flows to Gambia

Europol was notified of a significant anomaly concerning cash movements, specifically cash declarations from one EU Member State to Gambia. Findings showed that in 2014, Gambia became one of the most frequent destinations for cash declarations. Over EUR 27 million was declared to be moved to Gambia over the course of 2014. These declarations, both by number and value are unusually high in comparison with other countries (not only in that region).

Beyond these movements being highly anomalous, they could be indicative of money movements related to criminal activity. The Gambia is a small country of under 2 million people, with a GDP per capita of less than USD 2000 (equal to less than 10% of the average amount declared). The declarations are not explicable by way of the possible repatriation of funds by Gambian emigrants since their numbers are very low.

Gambia's geographical positioning in West Africa puts it in the heart of a region increasingly closely linked to drug (cocaine) trafficking from South America via West Africa to Europe. Concerns around the countries anti-money laundering capacity have been raised, in particular by GIABA (FATF-style Regional Body for West Africa) in their 2013 Annual Report ([16]).

However, there are indications that the Gambia may not be the ultimate destination of the funds. The same report also notes that: 'Cross-border movement of cash is a serious challenge due to the economic activities of nationals from other countries. Because of the strict monitoring of foreign exchange transfers in Senegal, the Gambia has become very attractive for such transactions because of its more liberal policies.'

([16]) http://www.giaba.org/media/f/765_Annual Report 2013.pdf

Non-conviction based confiscation

Law enforcement investigations regularly reveal instances of individuals who appear to live beyond their means. This is a particular problem in the case of cash detections. An individual with no source of legitimate income, stopped, for example, with a few hundred thousand euros, perhaps even ingested, may have that sum returned to them (minus a small administrative fee for non-declaration) due to the prevailing requirement for conviction-based confiscation. This requires that the predicate offence – i.e. the illegal source of the funds, is evidenced, and in some instances sums must be linked not only to criminality in general, but to specific criminality which accounts for the exact values in question.

Most European LEAs are required to demonstrate the predicate offence in order to prosecute money laundering: 60% of respondents to a Europol survey indicated that they are required to demonstrate the predicate offence to evidential standards while only 12% reported provisions for unexplained wealth. Given that cash is a bearer instrument, this is a challenging task, and successful investigations involving cash usually entail the use of traditional techniques such as surveillance and wiretapping. Very few MS have provisions for sanctioning unexplained wealth (only 12% report having such provisions) whereby if the individual is unable to account for the legitimate source of the funds, they may be confiscated (typically under a civil procedure). For this reason, very few MS can carry out simple and effective investigations in instances of international cash detections, even in cases where cash is detected while being smuggled in highly suspicious ways. In this particular field, legal harmonisation between all the EU MS allowing for the reverse burden of proof, would mean a strategic and substantial quick win for all law enforcement agencies and anti-ML supporters.

8 WHAT'S IN THEM?

8.1 REASONS FOR REPORTING SUSPICION

38% of FIUs reported that the use of cash is the primary reason triggering suspicious transaction reports.

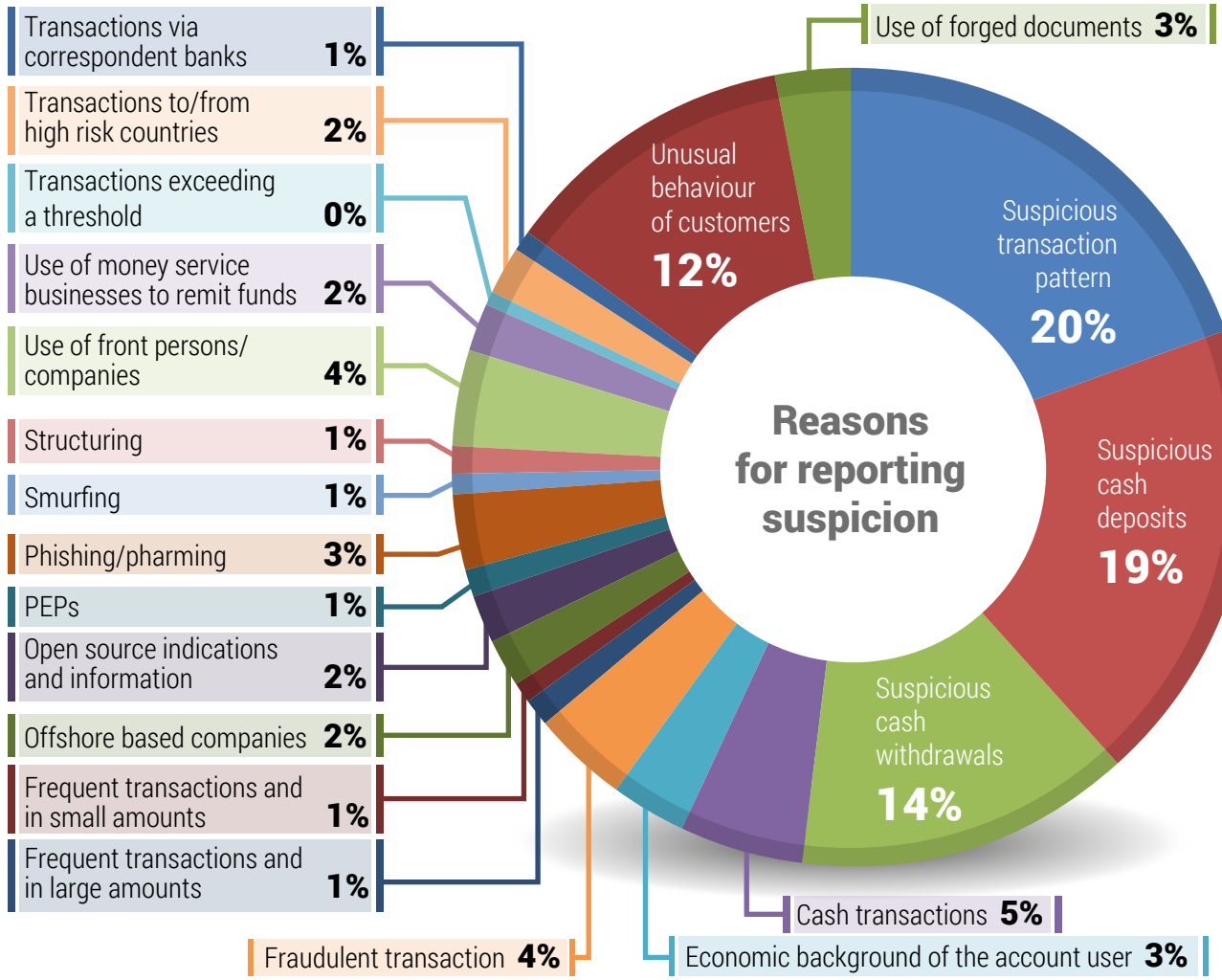
Beyond considering which obliged entities report (or do not) to their national FIUs, FIUs were asked to provide details of the main reasons behind STRs filed by regulated entities with the central authority. These reasons shed light on the factors and red flags that commonly trigger suspicion and the possible methods used by criminals to abuse the EU financial system.

The use of cash (deposits, withdrawals and cash transactions) remains the most common reason prompting suspicion of money laundering and/or illegal activities. 13 of 23 responding FIUs informed that the use of cash is the primary reason triggering STRs.

Surprisingly, however, Luxembourg, where banknote issuance is anomalously high ([17]), is one of the few Member States that does not cite the use of cash as a primary reason for reporting. This is likely because the majority of the reports received by the Luxembourg FIU are submitted by electronic payment institutions, which do not typically deal with cash. However, this means that the significant sums of cash issued by Luxembourg are either not injected into the Luxembourg economy or financial system through local obliged entities or, simply, do not trigger reporting, in spite of the fact that one could expect there would be substantial activities conducted with cash.

([17]) The net issuance of banknotes in Luxembourg grew significantly in 2013 (+EUR 11.2 billion, or +14.6 %) and reached EUR 87.5 billion by end-December 2013. This figure is twice the GDP of Luxembourg (approximately EUR 40 billion). In 2014 net issuance of banknotes grew to EUR 93.5 billion.

Chart 10 — Main reasons behind STR reporting 2013/14 ([18])



Why is cash still king?

In July 2015, Europol's Financial Intelligence Group released a detailed report on the use of cash by criminal groups as a facilitator for money laundering ([19]). Findings in 2012 revealed that the primary reason for reporting suspicious transactions to FIUs across the EU is the use of cash. In the years 2013- 2014 this trend has continued.

While Europol's report focused on the use of cash as a whole and its role as a facilitator for money laundering, it also raised the issue of high denomination notes, in particular the EUR 500 note. The report highlighted that the EUR 500 note alone accounts for around 30% of the value of banknotes in circulation, despite not being a common means of payment. In addition, operational cases evidenced that the EUR 500 banknote is used disproportionally in the various stages of criminal activity and the money laundering process. Subsequently the European Central Bank decided to stop the issuance of the EUR 500 from 2018 (although the notes will remain legal tender thereafter).

It is important to stress that the work of law enforcement agencies, central banks and reporting entities should not stop there. Efforts should be made to address other means of transporting values across borders which will likely attract criminals, for example, other high denominations such as the EUR 200 and CHF 1000 notes, gold, precious metals and stones, high value watches and jewellery. Furthermore the ECB, central banks, FIUs, Customs, LEAs and regulated entities should work in close cooperation to monitor the return and exchange of these notes over the coming years and investigate cases raising suspicions.

([18]) Based on total weighted results of FIUs' responses for the years 2013-14.

([19]) https://www.europol.europa.eu/content/why-cash-still-king-strategic-report-use-cash-criminal-groups-facilitator-money-laundering

20% of FIUs cited suspicious transaction patterns as the reason behind reporting suspicion. Given the increased use of automated systems for monitoring and detecting suspect activity, this is unsurprising. It should be noted that even very small changes in the algorithms behind these automatic systems can dramatically affect the number of reports filed, both positively and negatively.

In addition, two categories - 'economic background of the account user' and 'unusual behaviour' - are cited by 15% of FIUs as the reason behind reporting. These categories are of interest in that, despite the majority of countries operating transaction based, rather than activity based regimes, the bigger picture of a client's background, behaviour and general activities plays a large part in deciding whether to report suspicion or not.

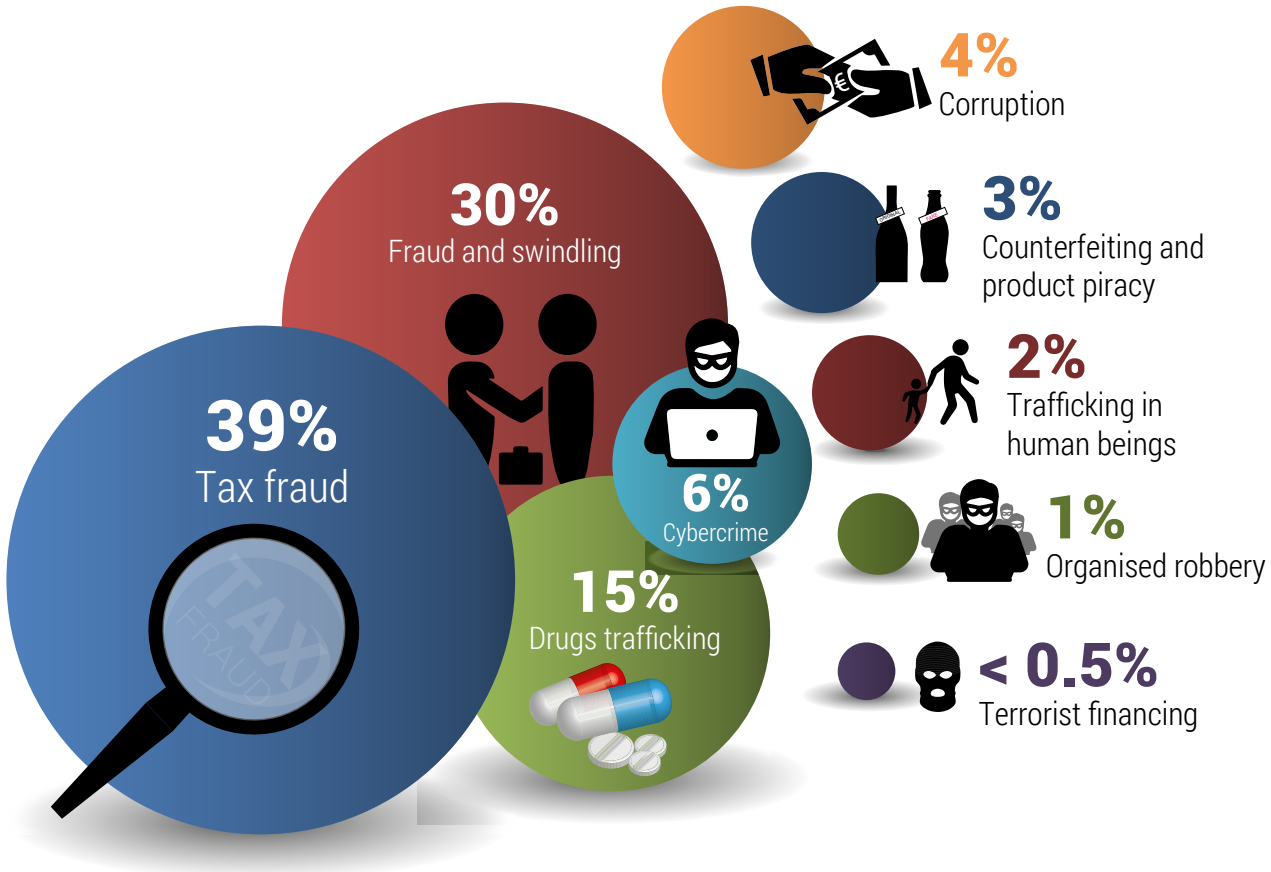
The involvement of Politically Exposed Persons (PEPs) ([20]) is not reported as a significant reason behind STR reporting. The Third anti-Money Laundering Directive limited reporting around PEPs to overseas persons. However, the Fourth anti-Money Laundering Directive extends this to domestic PEPs. As such, a corresponding rise in reports relating to PEPs would be expected once the directive is implemented.

([20]) Defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised that many PEPs are in positions that can be potentially abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

8.2 PREDICATE OFFENCES

One particular area of interest is the suspected predicate offence behind STRs, as verified by either the reporting entity or the FIU. While a number of FIUs do not record such information, for those that do, there is a clear trend: economic crimes, in particular fraud (tax fraud, fraud and swindling) dominate as the principle predicate offence behind STR reporting. Two thirds of respondents cited tax fraud or fraud as the suspected underlying offence behind STR reports. In spite of the rapid growth of cybercrimes, this category of offence is reported as the underlying offence behind relatively few STRs. This may however, be due to the fact that cybercrimes are recorded instead as fraud (albeit a cyber-enabled).

Chart 11 ([21]) – Main predicate offences behind reporting as verified by FIU (2013/2014)



([21]) Weighted survey responses.

Fighting fraud more effectively

While FIUs were established to receive reports relating to money laundering and terrorist financing, there are indications that they are increasingly overwhelmed by fraud reporting. Reporting entities send information around transactions that represent the initial fraudulent act, rather than the subsequent laundering. This raises questions about the most effective way to address the issue.

Modern on-line frauds have increased tremendously in recent years and the modus operandi of such crimes aims to rapidly transfer funds across borders and out of the financial system before detection. Fraudsters leverage the complexity of the internet and the fragmented cross-border information exchange to perpetrate frauds and gain profits. Often, when a bank officially reports an offence to their FIU, by the time it is addressed or reaches investigative services, the data provided is old and little can be done to identify the offenders or recover funds.

Clearly, a new approach to tackle the problem is needed, and one such example is the Italian-led initiative OF2CEN (Online Fraud Cyber Centre and Expert Network). OF2CEN aims to fight e-crime through connecting actors involved in combating on-line frauds, including the private sector, in order to consolidate fraud warnings, facilitate information exchange of fraudulent IP and IBAN data and conduct analysis that provides timely communication of suspicious activities to all participants. One of the key benefits of the platform is the information exchange bank-to-bank and bank-to-police. In this way early warnings about suspected criminal activity are shared rapidly, enabling more efficient investigation as well as empowering banks to strengthen their cybercrime prevention strategies and tactics.

In line with the fact that terrorist financing accounts for just a small fraction of reports received by all FIUs (less than 1%), it is unsurprising that it does not feature as a prominent offence.

As previously mentioned, the inclusion of domestic politically exposed persons (PEPs) in the Fourth anti-Money Laundering Directive may lead to an increase in reports relating to corruption.

It is significant that the offences thought to be behind STR reports are not entirely commensurate with the supposed most profitable criminal markets (drugs trafficking and trafficking in human beings according to UNODC), which may indicate that criminals avoid moving illegal proceeds through the regulated sector, or that the private sector is not well equipped to detect these transactions. Certain other offences suspected to generate significant profits, such as weapons trafficking and illegal migration, do not appear to generate many STRs.

Proceeds of people smuggling

In line with the European Commission's Action Plan against Migrant Smuggling (2015-2020) which identifies financial investigation techniques as a priority with regards to combating and preventing crimes, the Dutch FIU is leading a project focusing on financial flows related to current EU-wide migration crimes. The European Commission considers FIUs as crucial entities in combating the business of migrant smuggling through the analysis of illegal immigration proceeds, and promotes conducting financial investigations on a more systematic basis by authorities competent to investigate. In particular, the Dutch FIU project focuses on the possibility of identifying red flag indicators concerning financial flows related to migration crimes. Such indicators could assist the private sector in better identifying transactions linked to people smuggling.

Terrorist financing reports account for less than 1% of all reports received by FIUs across Europe

8.3 TERRORIST FINANCING

Terrorist financing is distinct from money laundering in that it aims at concealing the purpose for which funds will be used, rather than concealing the illicit origin of sums. However, both use similar methods to move and conceal funds. As such, the scope of the EU anti-money laundering regime also extends to reporting around suspected terrorist financing.

In contrast to the numbers of STRs concerning suspected money laundering sent by reporting entities, the volumes of reports received relating to terrorist financing are incredibly low. In fact, across the board, these reports account for less than 1% of all reports filed with FIUs. While it is understandable that figures for reports regarding the financing of terrorism are lower than those concerning organised crime, the overall figures are nonetheless extremely limited. Only in Austria (between 3-5%), Ireland (around 3%), Denmark (between 0.8-1.7%) and Estonia (between 16-20%) do figures exceed 1%. Estonia's high figure is in fact misleading and does not indicate that Estonia is a hotbed for terrorist financing activities. In fact, the Estonian figure reflects the fact that the FIU automatically records transactions to and from certain jurisdictions as terrorist financing (TF).

Chart 12 — Total TF reports sent in 2013 – 2014 ([22])

Country	Total reports filed relating to terrorist financing 2013	Total reports filed relating to terrorist financing 2014	Proportion TF reports 2013	Proportion TF reports 2014
AT	76	61	5.10%	3.65%
BE	126	154	0.55%	0.55%
BG	6	12	0.27%	0.53%
CY	0	0	0.00%	0.00%
CZ	0	0	0.00%	0.00%
DE	208	323	1.09%	1.34%
DK	86	56	1.66%	0.77%
EE	1858	2321	16.55%	20.72%
ES	47	22	1.17%	0.47%
FI	10	13	0.04%	0.06%
FR	200	323	0.73%	0.88%
HR	2	3	0.35%	0.43%
HU	2	4	0.02%	0.04%
IE	586	618	3.84%	3.38%
IT	131	93	0.20%	0.13%
LT	0	0	0.00%	0.00%
LU	47	50	0.96%	0.69%
LV	3	0	0.02%	0.00%
MT	0	0	0.00%	0.00%
RO	1	1	0.02%	0.03%
SE	40	50	0.36%	0.54%
SK	80	79	2.06%	2.01%
SI	7	7	1.17%	1.46%
UK	856	1342	0.27%	0.38%
Total	**4372**	**5532**	**0.53%**	**0.58%**

([22]) Countries not shown did not/could not provide figures.

Taking into account that of the few terrorist financing reports received by FIUs, the vast majority are reports filed based on semi-automated systems which detect matches between account holders and the names of persons and companies designated as potential terrorists in official (OFAC, UN, EU) and unofficial lists (usually based on open source intelligence (OSINT)), it is clear that more needs to be done to detect and report TF related transactions and to refine the current typologies used by regulated entities to detect such activity. Europol is nonetheless aware that there has been a surge in TF related reports since 2014 and that efforts have been significantly bolstered since the Paris attacks in January and November 2015.

In addition, it is notable that certain sectors known to be exploited in the financing of terrorist activities, for example charities and NGOs, do not fall within the scope of AML regulations and, therefore, are not obliged entities for reporting purposes. Detection of suspicious activity or their misuse relies only on the regulated financial institutions. From a regulatory point of view, broadening the scope of reporting obligations to include entities commonly used for terrorist financing may merit further consideration.

Strengthening the fight against the financing of terrorism

Certainly, the focus on terrorist financing issues and the role of the private sector in assisting authorities in detecting and preventing such activities is set to intensify. Almost immediately following the Paris attacks the French FIU, Tracfin, unveiled a series of measures ([23]) aimed at reducing anonymity, increasing due diligence and expediting asset freezing in order to tackle the threat of terrorist financing.

The measures are comprehensive and cover many aspects, from the use of cash (both movements and payments), through to strengthening cooperation. They also address several instruments with the potential to facilitate terrorist financing, for example pre-paid cards, known to have been used by the perpetrators of the Paris attacks. The prepaid cards, some bought in Belgium, were used to pay for cars and apartments used by the assailants in the hours preceding the attacks. The use of prepaid cards will in the future be more strictly controlled to limit the total amount that can be credited to these cards anonymously, as per the recent amendments to the 4th EU AML Directive.

Europol notes the importance of removing barriers and delays in international information exchange between all agencies. Efforts following the Paris attacks, for example, highlighted the problem of the limited domestic overview as concerns financial flows: while an isolated transaction at domestic level may appear innocuous, when viewed in its global context, the relevance becomes more apparent.

8.4 THE SUMS OF MONEY INVOLVED IN STRs

The scale of financial crime is enormous, yet largely unquantifiable. In 2011, the United Nations Office on Drugs and Crime (UNODC) estimated, through meta-analysis, the scale of financial crime to be some USD 2.1 trillion or 3.6% of global GDP in 2009. Of course, such estimates must be treated with caution since by their nature they are far from precise. Nonetheless, even accounting for significant margins of error, the fact remains that scale of financial flows relating to criminal activities are huge, and these figures do not account for the broader socio-economic costs of crime.

Europol findings from 2011 and 2012 indicated that the total sums of money involved in STRs in the EU exceeded EUR 29 billion ([24]). However, this figure was equivalent to just 0.1% of annual EU GDP, far short of the above estimates around the amount of money laundered through the financial system.

There has been a significant increase in the figures reported by FIUs regarding the total sums of money involved in STRs in 2013 – 2014. While only 10 FIUs provided figures, these show that in 2013, the total value was EUR 99.4 billion and in 2014 EUR 178.8 billion. Based on an EU GDP of around EUR 14 trillion, these equate to between 0.7-1.28% of annual EU GDP which is detected as being involved in suspect financial activity. However, this is largely attributable to figures provided by Italy alone, which are astounding and account for the majority of the sums reported in 2013/2014. Italy reports that the sums of money involved in STRs totalled EUR 84 billion in 2013 (some 5.25% of Italian GDP ([25])) and EUR 164 billion in 2014 (around 10.25% of domestic GDP). Excluding Italy, the sums involved in STRs from the other FIUs is again equivalent to just 0.1% of annual EU GDP.

Certainly, the sums of money involved in STRs across all EU MS are likely to be significantly higher - 18 MS FIUs did not provide figures, including the UK and the Netherlands, which account for the majority of all reports filed across the EU. Furthermore, while the STR regime knows domestic boundaries, criminal flows do not: it is probable that launderers select markets opportunistically, placing funds in countries perceived to be more lightly controlled, and integrating profits in stable and appealing economies.

([23]) http://www.economie.gouv.fr/files/dp_lutte_contre_le_financement_du_terrorisme_anglais.pdf

([24]) As reported by 17 FIUs in 2011 and 16 FIUs in 2012, the total sums of money involved in the STRs was €14,454,704,284 and €14,833,171,223 respectively.

([25]) Circa EUR 1.6 trillion.

8.5 SUBJECTS OF STRS

In order to identify any trends or anomalies across STRs, analysis was conducted on the principal nationalities reported across STRs; the main countries of incorporation where STRs concerned legal entities, and information around resident vs. non-resident accounts ([26]).

The majority of FIUs reported that the most common nationalities of individuals reported in STRs were nationals of their own countries, followed by individuals from neighbouring countries. However, a number of countries informed of significant STR reporting in relation foreign nationals owning non-resident accounts. Cyprus reports that non-residents are the subjects behind 75% of all STRs received, while Luxembourg receives almost five times as many STRs relating to non-residents than residents, and Malta receives around twice as many STRs around accounts held by foreign nationals. Regarding nationalities, Cyprus, Luxembourg and Malta all report that UK nationals are common subjects of these reports on non-resident activities. Both Luxembourg and Malta also note that Italians are another common nationality, while in the case of Cyprus, Russia is noted as more significant. More generally, across all EU FIUs, four nationalities were noted as generating comparably higher numbers of STRs: Russian, Chinese, Turkish and Ukrainian.

Regarding legal entities, most FIUs reported that a significant proportion of STRs related to activities involving companies located in offshore financial centres. In particular many noted a higher instance of STRs submitted in relation to companies incorporated in the British Virgin Islands (and other UK offshore territories) and Panama. Luxembourg also cited receiving a number of reports in relation to companies incorporated in Samoa. However, one of the most common countries of incorporation for legal entities reported in STRs across the EU is and EU MS itself: the UK. This may be related to a perceived increasing use of UK LLPs in money laundering schemes, given that there is some scope to conceal beneficial ownership through designating ownership to entities located in jurisdictions with significant banking secrecy (i.e. on the face of it the company may appear to be a UK company, however ultimate ownership details will in fact rest elsewhere). This issue has already been addressed through the recent UK Small Business Enterprise and Employment Act 2015, which requires most UK companies, including LLPs, to maintain registers of persons with significant control over a company (essentially a register of beneficial owners).

([26]) Non-personal data.

9 WHAT HAPPENS TO THEM?

Reporting entities are obliged to report suspicious transactions to a central authority, known as an FIU. FIUs play an important role in receiving, analysing and disseminating this information and the effectiveness of the system in combating money laundering and terrorist financing depends heavily on their ability to perform these tasks swiftly.

Although the MS FIUs all perform the same core functions of receiving, analysing, and disseminating STRs, how they perform these functions varies in many ways due to the different models and associated powers to be found across the EU.

9.1 FIU MODELS AND PRACTICES ACROSS THE EU

As regards FIU models, there is very limited harmonisation across the EU beyond the obligation to establish one. The structure and working practices of FIUs across the EU differ considerably, to a large degree because of their different statuses. FIU types within the EU are generally classified as one of four models: administrative, hybrid, judicial or law enforcement.

The most common FIU model in the EU is administrative. Twelve EU FIUs classify themselves as administrative ([27]), while ten have a law enforcement status ([28]), five are hybrid ([29]), and one is judicial ([30]). This of course means that each has its own distinct character, something of great relevance when considering the following sections around conversion rates and the effectiveness of STR reporting: given that what each FIU is tasked and empowered to do with STRs varies greatly, no direct comparisons are possible.

FIU types

Administrative: part of a structure (often the Ministry of Finance) separated from law enforcement or judicial authorities to create a buffer between reporting entities and those charged with investigation and prosecutions. The administrative FIU seeks to substantiate suspicion, and only then can a case be sent on to authorities in charge of criminal investigations.

Law enforcement: part of a law enforcement agency, therefore fewer restrictions on FIU access to law enforcement information and vice-versa may apply, potentially resulting in greater operational cooperation and the use of reports in investigations. Such FIUs may also benefit from exchange of information using national and international criminal information exchange networks.

Judicial: sits within the judiciary, commonly under the prosecutor's jurisdiction as in some legal systems, prosecutors are part of the judicial system and have authority over the investigatory bodies. Judicial FIUs are found in some countries with strong banking secrecy laws so actions such as freezing accounts can be swiftly undertaken.

Hybrid: have different characteristics from the other types of FIU. For example, it may sit within an administrative body but have staff from law enforcement agencies who continue to exercise criminal powers.

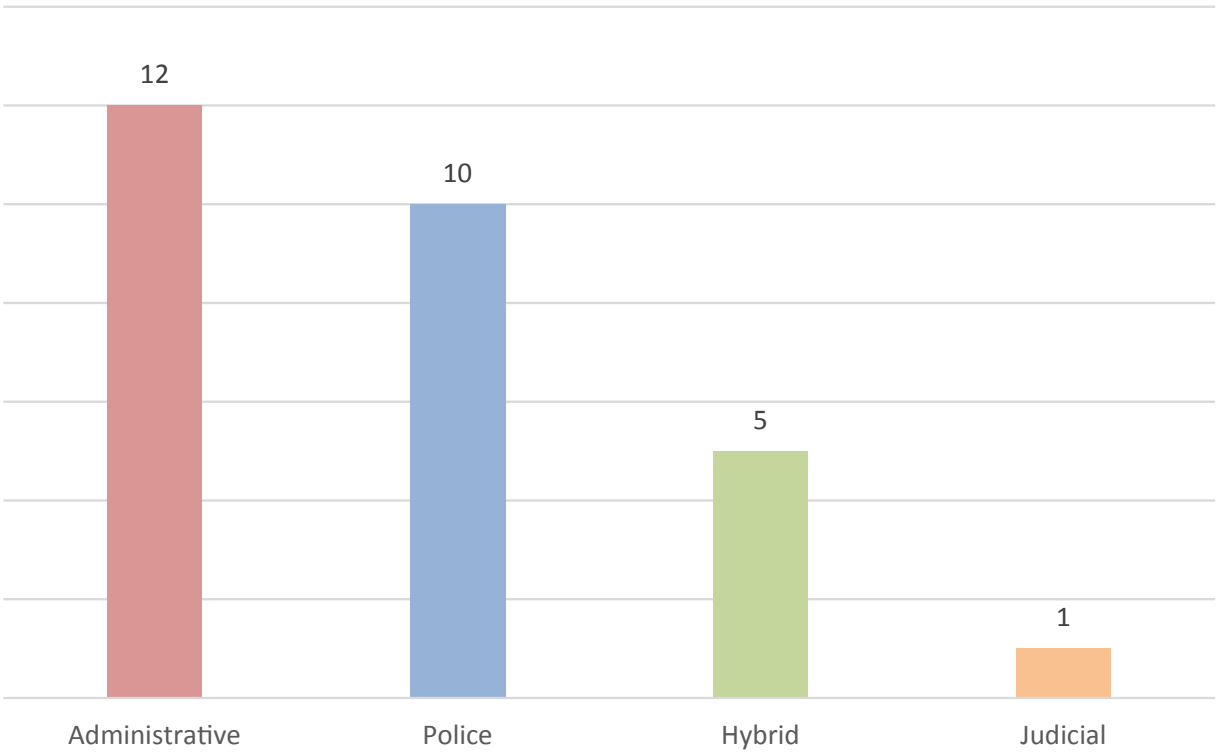
([27]) BE, BG, CZ, ES, FR, HR, IT, LV, MT, PL, RO, SI.

([28]) AT, DE, EE, FI, IE, LT, PT, SE, SK, UK.

([29]) CY, DK, EL, HU, NL.

([30]) LU.

Chart 13 — FIU models across the EU



9.2 CONVERSION RATES

Working practices and methods of recording information vary so considerably across the EU that it hampers analysis or comparisons and is almost impossible to assess the effectiveness of the regime.

The effectiveness of the STR regime is very difficult to measure. This is due to multiple factors, including the fact that the 'usefulness' of financial intelligence is not in itself a measurable quantity – one STR does not necessarily equate to one investigation, or one prosecution. They instead act as building blocks that can provide crucial leads to investigators. Effectiveness is also difficult to measure because information is often unavailable or recorded in such different ways that it hampers analysis or comparisons.

One aspect considered by Europol to gain a greater insight into the effectiveness of the regime is that of the conversion rate ([31]) i.e. what is actually done with reports filed by obliged entities. Although this is a somewhat crude measure of the value derived from STR reporting, that a STR is sent to an investigative body, initiates an investigation, or can be linked to an on-going case (possibly leading to successful convictions) is perhaps the simplest and most immediate example of the value derived from the regulated sector making such reports.

However, the different models, activities, working practices and methods of recording and analysing information vary so considerably across the EU FIUs as to make calculating a meaningful conversion rate impossible. Clearly, there is a need to increase the harmonisation of criteria for the collection of statistics, or at least the adoption of transparent standards.

Nonetheless, based on the information provided by FIUs and an understanding of the complexities of the information, charts 14 and 15 provide the best available picture of the conversion rate at EU level and one high level conclusion: on average just over 10% of the STRs submitted to FIUs are put to use. Previous analysis by Europol shows this has been the case since 2006.

Figures for 2013 and 2014 in chart 14 show that the rate is higher, nearly 20% in 2013. However, this is entirely the

([31]) For the purpose of this report, the conversion rate refers to the way in which a STR is used, e.g. whether it is used in some other way, be it subject to further analysis, used within the framework of on-going/existing investigations or to launch a new one.

The proportion of STRs which are further investigated after the collection is just over 10%

result of outlier figures reported by the Italian FIU, which reports a conversion rate for these years in excess of 100% ([32]). Without the figures reported by the Italian FIU, the conversion rate for the other MS remains at 10% as shown in chart 15.

The following charts should be viewed with caution: the conversion rate does not account for the many different reporting forms (e.g. STRs, SARs, UTRs etc.), varied FIU practices (some carrying out further investigations on all STRs received while others do not), nor how different end users might exploit the reports. So, for instance, the German and Irish FIUs, which are both police FIUs with investigative powers, always show a 100% conversion rate, given that every STR received is subject to further checks. Others, for example the UK FIU, function quite differently and can provide no figures at all, as reports are stored in a central database accessible only by authorised officers, who may query it in the course of investigations. In the Netherlands, for example, the conversion rate in fact refers to those UTRs which are eventually classified as suspicious and made available to law enforcement (which can mean that others that could be relevant are never released). Meanwhile the Italian FIU reports a conversion rate of in excess of 100% due to the fact they forward more reports than they receive (some carried on from previous years) to police authorities (Guardia de Finanza (GdF) and Direzione Investigativa Antimafia (DIA)) after a preliminary analysis process by the FIU. However, it does not demonstrate what actually happens to this vast body of forwarded STRs.

The reporting of suspicion is merely the first step in a complex process through which intelligence is developed and investigated, with a view to achieving judicial outcomes in the form of convictions and confiscation. Clearly there is room for improvement to ensure that more than 10% of reports reach investigative services, or that fewer irrelevant reports are not generated. It is somewhat alarming to consider, then, that even where further investigated, the likelihood of successful asset recovery is low. Europol findings show that from 2010 to 2014, just 2.2% of the estimated proceeds of crime were provisionally seized or frozen, and only 1.1% of the criminal profits were ultimately confiscated at EU level ([33]).

([32]) Italy reported receiving 64 601 STRs in 2013, while in the same year 92 415 were submitted for investigation, likely cases retrospectively forwarded to GdF and DIA.

([33]) https://www.europol.europa.eu/newsroom/news/does-crime-still-pay

Chart 14 — Conversion rate including Italy

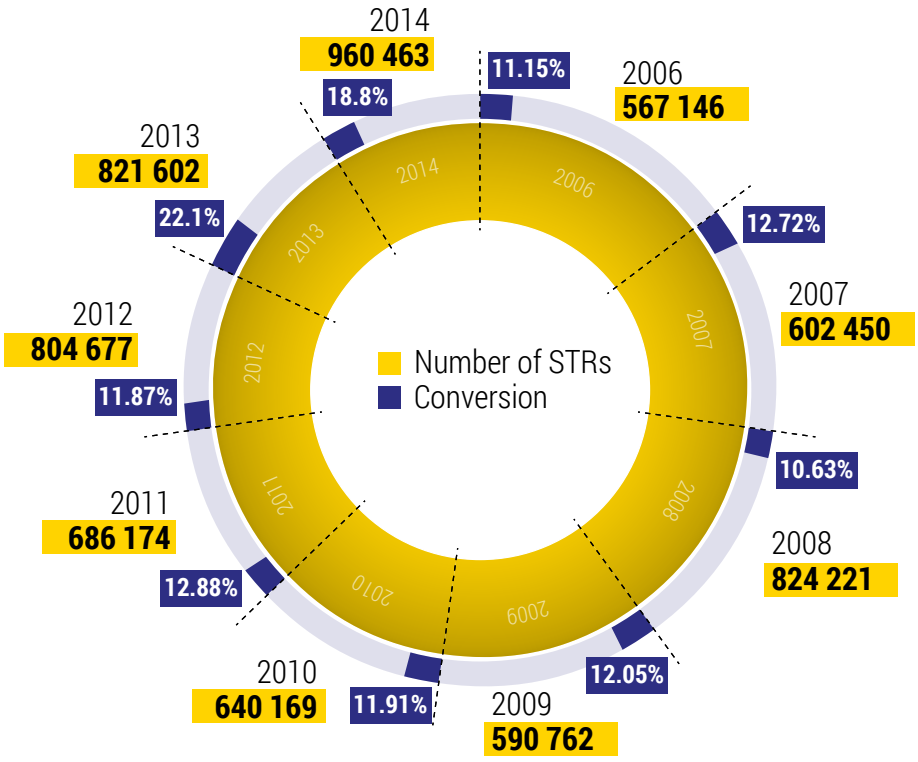
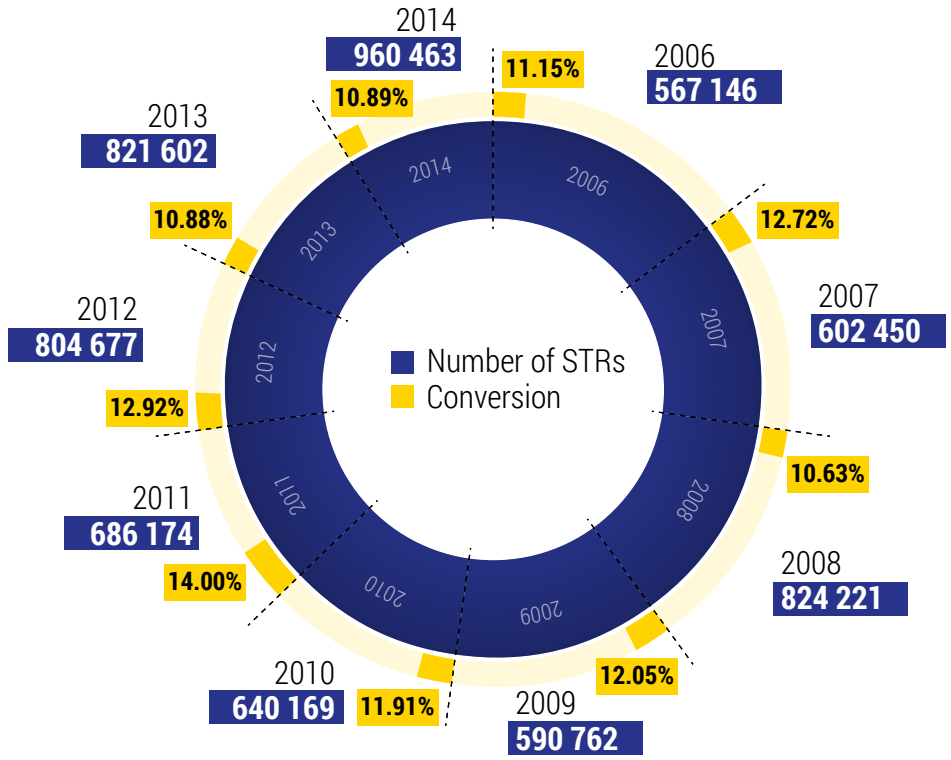


Chart 15 — Conversion rate excluding Italy



Most international exchanges of financial intelligence are organised in a 'symmetrical' way, between FIU counterparts. This can mean that the crucial information needed to confirm and develop STRs may never become apparent to the agency seeking it

The reason for the relatively stable but low conversion rate may be due to the incremental amount of reports generated by obliged entities, who due to raised awareness and better automated-monitoring systems, file more and more STRs. A number of FIUs note in their annual reports that the persistent increase in STR reporting volumes is a huge challenge. This topic is addressed in more detail below (see section 11 'The impact of new technology'). Defensive and/or over-reporting may also result in reports of limited quality that are difficult to develop.

Another factor which may prevent the fullest exploitation of STRs (thus leading to a higher conversion rate) are barriers in international and diagonal information exchange between different national and overseas agencies which are not FIU counterparts. Most international exchanges of financial intelligence are only organised in a 'symmetrical' way: each FIU communicates with its FIU counterparts of the same type abroad (although most FIUs have powers to exchange information with foreign law enforcement agencies). This can mean that the crucial information needed to confirm and develop STRs may never become apparent to the agency seeking it. This topic is addressed in more detail below (see section 'The international dimension of the STR regime').

Role of STRs: Operations Snake and Shadow

In early 2015 the Spanish Guardia Civil, supported by Europol, conducted a major anti-money laundering operation. 65 house searches were performed in several cities, 32 suspects were arrested, EUR 1 million in cash and 26 high value vehicles and 28 properties were seized.

The case, known as Operation Snake, was the culmination of an international investigation into a Chinese organised crime group (OCG) operating in Spain (the subsidiary of an even larger criminal network based in China), which laundered an estimated EUR 300 million in a 2-year period.

The entire investigation was initiated because of a set of STRs filed by banking entities, informing that in a 3-month period, a group of 25 Chinese nationals and 17 related companies made multiple cash deposits followed by transfers to China for a total of EUR 6.5 million.

Their ill-gotten profits derived from the importation of under-invoiced (excise fraud) and counterfeit goods via containers in sea ports located across Europe, as well as from the labour exploitation of Chinese citizens that worked in clothing factories controlled by the OCG in the industrial outskirts of Madrid.

Import activities were facilitated by the use of falsified documents and the abuse of real companies, or by pre-established shell companies controlled by front men (trafficked workers).

The reporting behind the case led the investigation to reveal the use of several money laundering MOs including: - smurfing; cash couriers and Fei-ch'ien (Chinese Hawala).

The case recently led to a second phase – Operation Shadow. In February 2016 Europol supported the Spanish Guardia Civil in carrying out this operation which targeted the governing structure of ICBC Spain due to suspicions of large scale money laundering services offered to clients in remitting the proceeds of various criminal activities to China. Evidence retrieved demonstrates that ICBC was responsible for siphoning hundreds of millions of euros from Spain to China over a 3-year period, belonging to the aforementioned OCGs. During this period, no STRs were ever filed, nor was customer due diligence duly implemented by ICBC, and highly suspicious activities regarding private banking, correspondent banking and cash in freight towards China were also identified and are currently undergoing further investigations.

9.3 BENEFITS OF FINANCIAL INTELLIGENCE

Beyond directly launching cases, that there is a STR regime in place serves as a deterrent, both to criminals who seek to abuse the legal economy, as well as to gatekeepers who may otherwise be inclined to accept such business and facilitate the laundering of criminal proceeds. Although counter-productive, the increasing tendency of criminals to use cash or unregulated financial systems to avoid detection is nonetheless testament to the success of the reporting regime in the EU.

Of course, STR reporting does not merely serve as a deterrent. Financial intelligence is also an investigative tool, providing crucial information on how criminals disguise and move proceeds. Financial intelligence is a core component of financial investigations, providing indications not only on origin, transfers, destination, beneficiaries, storage and usage of funds, but also to reconstruct geographical movements of criminals, to discover the current location of persons of interest, and to retrieve all types of data around suspects (contained in customer due diligence). More importantly, it allows for the identification of participants in a criminal network – the highest levels included - and provides the basis for seizure/confiscation opportunities. Financial intelligence is a precious resource not only in money laundering cases, but can also be fruitfully used for tackling a number of offences such as terrorist financing or tax offences, and accordingly, many countries now provide access to STR data to revenue authorities and terrorist financing units. However, it should be noted that in many MS, by legal limitation one can only use FIU services (including STR checks) if there is a suspicion of money laundering (linked to mandated criminal offences) or terrorist financing.

STRs are also a key source of financial intelligence, providing early warnings on emerging threats that can be used as tactical intelligence for investigations or for strategic purposes in order to inform and support policy decisions.

Effective STR regimes are also self-serving and feedback between reporting entities, end users (i.e. investigators) and the FIU can help to improve the quality of reporting with a view to ensuring that FIUs are not burdened with poor quality reports.

10 THE INTERNATIONAL DIMENSION OF STRs

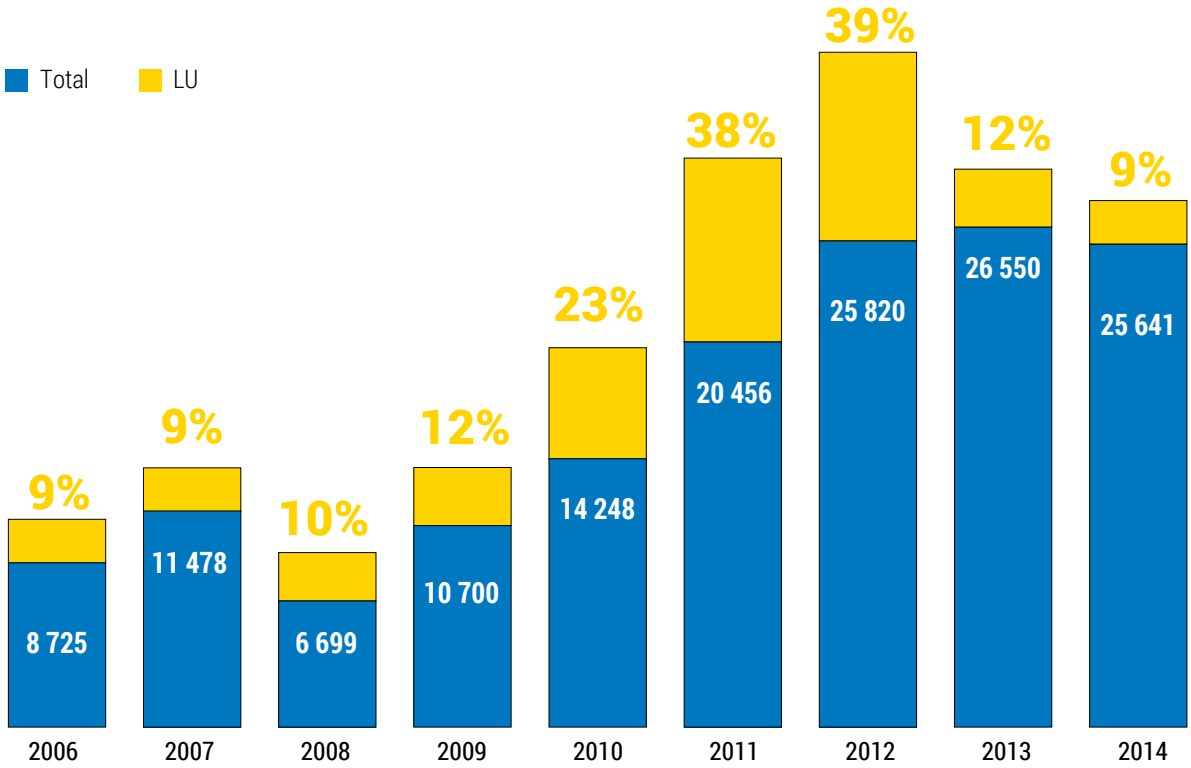
10.1 INTERNATIONAL REQUESTS

International collaboration and information exchange is crucial in the context of STRs as money laundering and terrorist financing are frequently carried out in an international context.

Correspondingly, the volume of international requests sent and received to and from other FIUs has increased significantly over time. This is understandable given the rising number of STRs across the EU.

Chart 16 shows the growth in international requests sent to and from FIUs since 2006. Although it appears relatively flat for the years 2012 – 2013, and in fact decreases in 2014, this is largely the result of a stabilisation in the number of requests sent by Luxembourg's FIU. For 2 years (2011 and 2012), Luxembourg accounted for almost 40% of international exchanges sent by EU FIUs (the proportion of requests relating to Luxembourg is shown in yellow in chart 16). Luxembourg experienced a significant increase in STR reports (jumping from just 574 in 2006, to 11 436 in 2012 for example), most of them filed by an online credit institution. Given the virtual nature of the financial service provided, it is likely that the vast majority of these STRs relate to transactions, persons or companies not based in Luxembourg, but in other MS (or non-EU countries). Correspondingly, reports were (and still are) forwarded to the countries which the transactions concern. Another reason for the decrease is the cross-border reporting function developed as part of the FIU.net system, specifically to assist Luxembourg in forwarding such reports. By 2016, Luxembourg had forwarded 30 000 of these cross-border reports (mainly dealing with online frauds) to other EU MS (primarily the UK and Germany) which, as they are not 'requests' in a traditional sense but rather a redirection of information, may not be recorded as such.

Chart 16 — Total international exchanges by EU FIUs



Greater exchange of information between FIUs and other agencies, as well as a FIUs ability to make use of international platforms such as Europol, would assist in valuable STRs reaching those tasked with criminal investigations

Excluding the decrease reported by Luxembourg, in fact the overall trend shows a continual increase in international requests. In particular, France has seen a dramatic rise in the number of international requests they are dealing with, having seen a roughly 100% rise in the number of international requests dealt with in 2013/14. In 2011/12 France reported that they dealt with roughly 2000 international incoming and outgoing requests annually (the majority sent by the French FIU). By 2013/14 this figure had more than doubled to 5730 and 5182 requests in 2013 and 2014 respectively (with the majority of requests received by the French FIU).

10.2 INTERNATIONAL COOPERATION: CHANNELS AND BARRIERS

The STR regime exits to prevent and detect the abuse of the financial system by criminal groups seeking to launder the profits of illegal activities. As such, the ultimate aim is that reports should launch investigations or complement on-going ones, and reach those tasked with investigating money laundering or terrorist financing (TF) and all associated predicate offences. As the majority of FIUs in the EU are of an administrative nature, very often they are not the body tasked with investigation and therefore play a crucial role in transmitting information to those competent to investigate.

Regardless of the model of FIU established in a given country, a fundamental principle of their work is identified as the unfettered exchange of financial data and intelligence, and the ability to cooperate with domestic and foreign authorities is critical to the success of this mission. The EC Council Decision from 2000 ([34]) sets out detailed requirements to improve the exchange of information between FIUs. The decision emphasises that a FIU should be able to fully perform its duties (including the exchange of information), 'regardless of whether they are administrative, law-enforcement or judicial authorities.' Several bodies and platforms exist to facilitate international cooperation between FIUs, most notably the Egmont Group of FIUs and FIU.net (Europol's Financial Intelligence Group, in which FIU.net is embedded also aspires to offer a multi-agency platform to share financial intelligence). Both are cited as the primary channels for international exchanges of information between FIUs (FIU.net is preferred for exchanges in the EU, and the Egmont Group for exchanges with third countries). However, these channels facilitate cooperation and information exchange between FIUs.

The Council Decision does not consider an FIU's ability to cooperate with non-FIU counterparts for purposes of criminal law enforcement work. While most FIUs have access to police databases (and often those of other agencies) at a domestic level, given the global nature of money laundering and TF offences, international cooperation with overseas law enforcement is also crucial: while a target may be reported to one country's FIU, it may well be under investigation by another country's police force.

Europol is well positioned to highlight the shortcomings in international cooperation and information exchange between FIUs and overseas law enforcement counterparts. AP Sustrans, Europol's project dedicated to money laundering, plays a role in the timely dissemination of FIU data to investigators across Europe in support of their on-going investigations. However, the ability to perform this role is limited by the classification of many FIUs as administrative, preventing the sharing of cross-border STRs diagonally with law enforcement. Europol regularly receives contributions from a handful of EU FIUs, but typically, such information exchange with non-FIU counterparts is prevented by 'legal barriers'. The reports Europol receives generate thousands of links with ongoing investigations conducted in other countries, which provide crucial leads for investigators. For example, a recent analysis of on EU MS' STR data at Europol revealed links to accounts used by a network of companies controlled by criminals in order to transfer and launder the proceeds of MTIC fraud.

([34]) Concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0642&from=EN

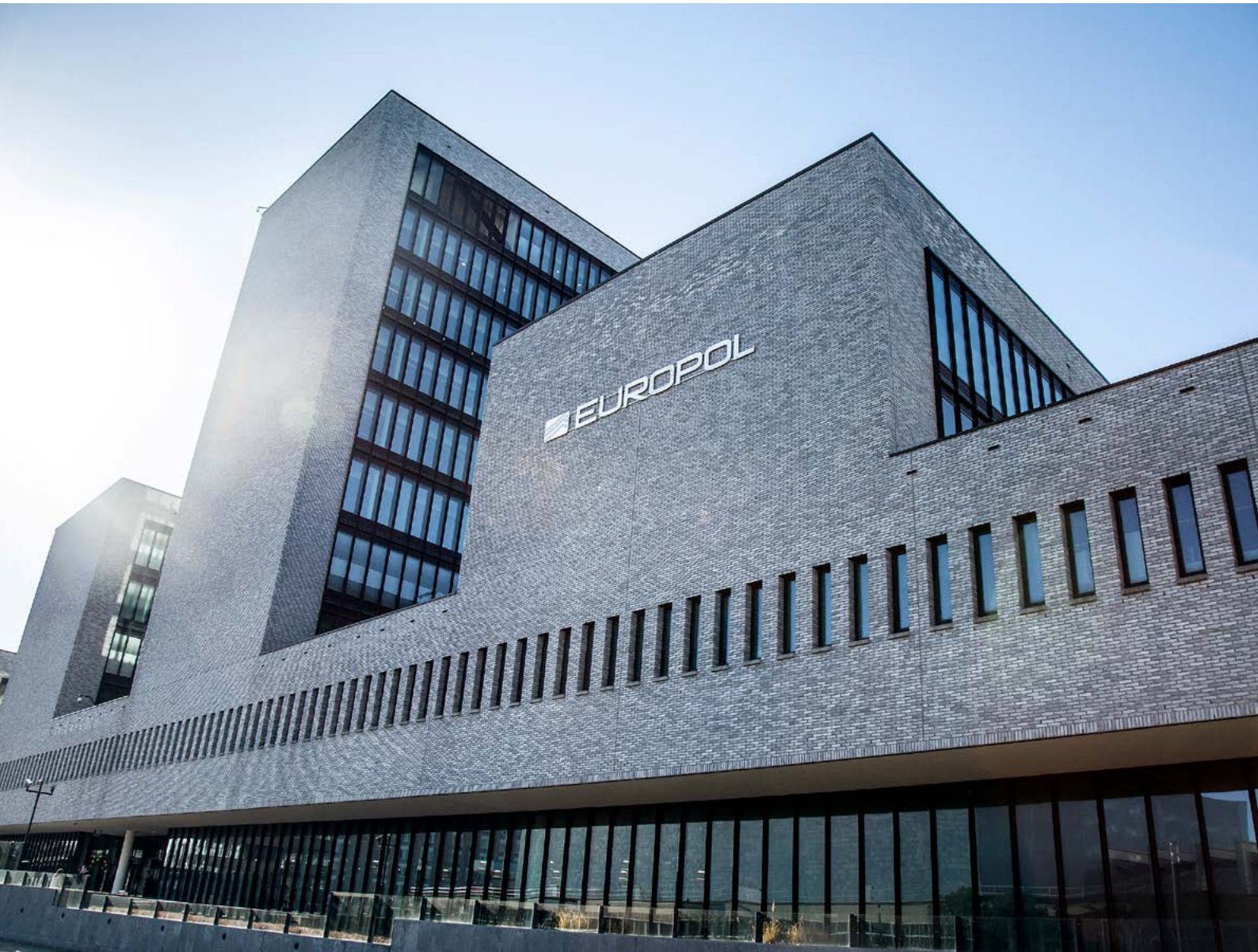
This analysis established links between Police, FIU and Tax services data to reveal a network involving more than 20 MTIC fraud cases investigated across no fewer than 13 different jurisdictions, each holding information pertinent to one another.

Clearly, greater exchange of information between FIUs and other agencies, as well as an FIU's ability to make use of international platforms such as Europol, would assist in valuable STRs reaching those tasked with criminal investigations. Europol notes that significant barriers in the fight against money laundering, terrorist financing and the pursuit of financial investigations more generally result from the often-fragmented cooperation at national and international levels, and lack of interoperable databases. Europol could assist in overcoming this barrier to some degree through acting as a pan-European hub for STRs, enabling information to be integrated with other sources stemming from multiple agencies across Europe and beyond. Notwithstanding the fact that FIUs must adhere to strict data protection concerns regarding the sharing of financial intelligence, the embedment of projects such as FIU.net at Europol may provide a solution for developing STRs while balancing these data protection concerns.

FIU.net embedment in Europol: greater exploitation of STRs?

FIU.net is a decentralised computer network that connects all 28 EU FIUs, which use FIU.net to exchange suspicious transaction reports (STRs). FIUs can use FIU.net to build cases to exchange information among themselves and use the system's matching tool share hashed datasets to establish if a person is known to another FIU.

FIU.net became operational in 2002. As of January 2016 FIU.net was embedded into Europol. The embedment of FIU.net in Europol should eventually enhance the exchange of financial intelligence available via this network by combining it with the products and services of Europol, with a view to creating more synergy between financial and criminal intelligence, ultimately boosting efforts to fighting organised crime and terrorism in the EU.



11 THE IMPACT OF NEW TECHNOLOGY

The impact of new technologies on the financial system and the development of borderless virtual environments call for reflection on how to adapt policies which are meant to be supervised only at national level, while the underlying business is already transnational and globalised

New technologies have brought new actors in financial services, and have a great impact on traditional financial institutions.

Technology can also be of great help to improve the monitoring of customer profiles and reporting of suspicious transactions, and to cater for better and more secure collaboration between reporting entities, FIUs and other law enforcement authorities.

11.1 INCREASINGLY GLOBAL MARKETS

The growing demand for online services and related internet payment systems, and the rise in cross-border transactions in volume and frequency, pose considerable challenges to the EU policies concerning money laundering and terrorist financing, in particular those of STRs and limitations in the sharing and exchange of information. Given the increasingly global and virtual nature of finances, similar cases to that of Luxembourg - where the vast majority of STRs received by its FIU relate to transactions, persons or companies not based in Luxembourg, but in other countries - might occur in other jurisdictions (but will be perhaps less apparent, diluted among the much higher STR volumes of other countries). The impact of new technologies on the financial system and the development of borderless virtual environments call for reflection on how to adapt policies which are meant to be supervised only at national level, while the underlying business is already transnational and globalised in its own nature: there is an urgent need for a supranational overview.

A supranational overview should not be understood in the regulatory sense alone, but more broadly as regards developing a full European picture of STRs, affording a better strategic overview of trends in criminal finances, greater operational efficiency and faster responses. There is a need to avoid the fragmentation and duplication of data concerning the same or complementary transactions, which limits the efficiency and effectiveness of reporting entities and FIUs.

Reporting entities (for example, banks) have informed Europol that they detect suspicious patterns across their global networks, however, they are obliged to fragment this global picture and provide only pieces of information at national level to the FIUs. In turn, this requires time and effort from FIUs to recreate the global vision that the private sector already had (and which, in some instances, may never be pieced back together due to inconsistent international cooperation efforts).

Efforts following the Paris attacks, for example, highlighted the problem of an overview limited to the domestic level. As concerns financial flows, while an isolated transaction at domestic level may appear innocuous, when viewed in its global context, the relevance becomes more apparent.

11.2 BIG DATA

Financial intelligence is a clear example of big data requiring advanced analysis to reveal patterns, trends and associations.

Big data is commonly understood to mean large and complex data, to the extent that its manipulation and management present significant logistical challenges. Financial intelligence is a clear example of big data: a transaction in isolation is meaningless, requiring contextualisation with multiple data sources. The increasing digitalisation of financial services results in growing volumes of transactions and extremely large data sets requiring computational analysis to reveal patterns, trends, and associations. The use of analytics is therefore becoming essential for both reporting entities and FIUs to cope with information and fully exploit its potential.

A number of FIUs note that the persistent increase in STR reporting volumes is a huge challenge. The volume of data both reporting entities and FIUs are confronted with is likely only to increase, in particular as virtual currency providers come into regulatory scope and services using distributed ledger technology (DLT) enter the mainstream.

The traditional model for detecting suspect financial flows is based on screening for pre-defined risk scenarios: this can inevitably lead to the problem that 'we don't know what we don't know', and more so that we don't know what risk scenarios look like for emerging products and services. Proponents of new analytical approaches believe that data-driven big data analytics hold the key to shifting towards a more effective intelligence-driven approach towards anti-money laundering and counter terrorist financing.

Certainly, with the investment in the right tools, big data may afford great possibilities: for example in DLT, all transactions are public, and it is therefore possible to follow money flows globally in almost real-time. A unique identifier in distributed ledger technology, with automated customer authentication, could generate advanced monitoring systems for reporting entities with better correlation between 'know-your-customer' (KYC) and transaction monitoring. However, no technology can overcome the limitation created by the partial knowledge of each financial institution, and shared utilities ([35]) between reporting entities could enable a secure way for efficient information sharing.

Similarly, technology could help in building targeted intelligence-led monitoring to leverage the quality of STRs through collaborative secure channels of communication. This would also enable financial institutions to cooperate on key investigations and speed up law enforcement access to relevant data. Big data analysis with artificial intelligence could enable the detection of sophisticated and cross-financial institution patterns that might be underreported, as they were not properly understood.

Currently, however, few EU FIUs dispose of resources to realise such ambitions. Most European initiatives which have taken considerable resources in past years have been aimed at easing the movement of information from one FIU to another with efforts put into transforming and sending different formats from one FIU to another. This is potentially at the expense of deploying resources to address the critical need to keep pace with the rapidly changing financial services industry and evolving technologies for which FIUs and LEAs are ill equipped to cope.

Nonetheless, there are some positive examples. AUSTRAC, the Australian FIU, is already in the process of constructing a new advanced data analytics platform. Recognising that anything built today will soon be out-of-date, its architecture focuses on inexpensive, loosely coupled components with compatible interfaces that can be more easily swapped in and out.

Europol strongly supports innovation and technology as a means to better combat crime, emphasising the need to couple big data analytics with safe and secure means to stimulate big data sharing, and of course, the willingness to build open and collaborative relationships with all relevant actors, from both the public and private sector.

([35]) Shared utilities are utility services provided by a third party. Pertinent end-client information is uploaded onto a single portal that is then shared only with authorised and approved banks.

11.3 FINTECH OPPORTUNITIES AND CHALLENGES

New technology has changed the financial services sector considerably over the last decades. The internet revolution and recent developments such as mobile payments, distributed ledger technology, and other innovations commonly referred to under the umbrella term of 'Fintech' ([36]) indicate that the transformation shows no signs of abating.

The Fintech revolution presents some challenges to the current anti-money laundering framework, both to reporting entities, regulators, policy makers, FIUs and LEAs who try to keep pace with, and even anticipate, the effect this may have on organised crime and terrorism and the ability to counter them.

Most Fintech and technology companies are not regulated and have no obligation to perform customer due diligence, nor report suspicious transactions. In order to give a fair treatment, for an effective anti-money laundering/ counter terrorist financing (AML/CTF) system, the regulatory status of new players should be considered. The Financial Conduct Authority in the United Kingdom has addressed this through setting up regulatory sandboxes ([37]) for innovation companies that do not easily fit in the existing regulatory framework.

New players may offer interesting opportunities that could help FIUs and law enforcement, with new ways of reporting and different approaches to analysis around transactions. RegTech could help to achieve that goal: RegTech means firms and start-ups that make innovative use of technology, especially analytics and assessment techniques, to automate and ease compliance tasks. This can leverage existing systems and data to produce regulatory data and reporting in a cost-effective and flexible way, and can be implemented by traditional reporting entities.

([36]) A term commonly understood to mean the innovative use of technology in financial services and products, FinTech encompasses: new payment services, including software companies which provide assistance for payment services; mobile banking; start-ups simplifying cross-border payments such as electronic cross-border money remittances; cryptocurrencies; smart contracts (automated performance of an agreement using block chain technology); peer-to-peer financing platforms (whether crowdfunding, crowd-investing or crowd-lending).

([37]) https://www.fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox

12 CONCLUSIONS AND RECOMMENDATIONS

The different models, activities, working practices and methods of recording and analysing information vary so considerably across the EU FIUs that it hinders thorough comparative analysis. This also makes any assessment of the effectiveness of the EU anti-money laundering regime and STR reporting challenging. Even the very subject matter of this report, STRs, creates problems regarding definitions. Clearly, there is a need to increase the harmonisation of criteria for the collection of statistics, or at least the adoption of transparent standards.

This said, available figures show that while considerable efforts are put into generating, handling and processing one million reports annually, these efforts achieve few outcomes and energy may be misdirected: only around 10% of reports lead to further investigation by competent authorities. When put into context against Europol estimates on asset recovery efforts in the EU, which show that barely 1% of criminal proceeds in the European Union are ultimately confiscated, the picture seems even bleaker. More needs to be done to exploit financial intelligence in order that it makes a more meaningful contribution to the fight against serious crime and achieves real outcomes in combating the misuse of the financial system for money laundering, terrorist financing and other criminal activities.

Efforts to address these problems at EU level in the past decade have focussed on improving FIU to FIU cooperation ([38]). Several revisions to the AMLD have attempted to remove FIU-FIU cooperation barriers and harmonise standards. Nonetheless, these efforts do not go far enough. A more far reaching approach is needed to improve the effectiveness of financial intelligence and investigations to tackle terrorism and organised crime. Most European initiatives which have taken considerable resources in past years have been aimed at easing the movement of information from one FIU to another with efforts put into transforming and sending different formats. This is potentially at the expense of deploying resources to address the critical need to keep pace with the rapidly changing financial services industry and evolving technologies for which FIUs and LEAs are ill-equipped to cope.

Two key approaches could lead to significant improvements: cultivating better, broader data-sharing practices and applying an 'intelligence-led' approach to the reporting mechanism.

These conceptual principles have not yet fully translated in to the anti-money laundering regime and partly reflect poor outcomes.

As regards better data-sharing practices, several obstacles still prevent greater exploitation of STRs, the most significant of which, from Europol's perspective as a cooperation body, relate to barriers in international cooperation between all actors involved in combatting money laundering and terrorist financing. This relates not only to information flows between FIUs and law enforcement counterparts, but also to others such as tax and customs authorities and the private sector. The anti-money laundering regime still operates at a domestic level, and has not yet fully adjusted to the reality of a problem that is defined by its international nature. While structures exist to facilitate cross-border cooperation between national units, significant barriers in international cooperation and information exchange remain, revealing the urgent need for supranational overview in increasingly global markets. The 'symmetrical' exchange of information between FIUs may prevent crucial information contained in STRs reaching authorities tasked with criminal investigations.

In the law enforcement and intelligence communities, an 'intelligence-led' approach of using enhanced knowledge of the threat to direct operational resources against the highest priority areas is at the heart of all counter-terrorist and other major security programmes. A shift from the current brute-force approach to scrutinising high volumes of accounts and transactions, towards a targeted approach focused on generating relevant information, rather than high volumes, is required. Better data sharing and cooperation practices among all actors, in particular regarding feedback to the private sector, would help to ensure that efforts are directed by competent authorities to better deploy resources and deliver outcomes against criminal groups.

Furthermore, new approaches are required to address the impact of new technologies, regarding emerging internet facilitated crimes and to cope with the changing nature of financial intelligence data. At present, efforts are ineffective to tackle burgeoning cyber-enabled crime and online frauds. These offences rely on the rapid transfer of funds across borders and out of the financial system before detection and, once moved, there is little hope of recovering them. By the time a warning notification reaches investigative services, the data provided is old and little can be done to identify the offenders or recover funds.

The findings of this report reveal a number of areas which should be addressed to improve the effectiveness of the anti-money laundering regime, increase the use of financial intelligence and investigation techniques, to deliver better outcomes against organised crime and terrorism.

([38]) The 2000 EC Council Decision (concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information) sets out requirements to improve the exchange of information between FIUs. The decision emphasises that an FIU should be able to fully perform its duties (including the exchange of information), *'regardless of whether they are administrative, law-enforcement or judicial authorities.'*; The recently implemented Fourth Anti-money laundering Directive creates new requirements for sharing of reports between FIUs under article 53: *'When an FIU receives a report pursuant to point (a) of the first subparagraph of Article 33(1) which concerns another Member State, it shall promptly forward it to the FIU of that Member State'.*

- **Standardising of statistics:** It is hard to assess any system, regarding trends or effectiveness, without a body of robust information to draw on. The variety of methods for reporting and recording figures related to STRs across EU FIUs, and even the absence of statistics altogether, is a limitation which should be addressed though increased harmonisation in the criteria for the collection of statistics, or adoption of transparent standards.
- **Supranational overview of financial reporting:** The impact of new technologies on the financial system and the development of borderless virtual environments call for reflection on how to adapt policies which are meant to be supervised only at national level, while the underlying business is already transnational and globalised. Reporting entities detect suspicious patterns across their global networks; however, this global picture is fragmented through providing only pieces of information at national level. There is an urgent need for a supranational overview. The recent call for an assessment of the need for the creation of an EU FIU ([39]) is a positive step towards creating a structure which could grant a direct and full picture of the suspicious flows. An EU FIU would also assist in simplifying and standardising processes and overcoming cooperation barriers, leading to greater exchange of information, ensuring valuable STRs reach those tasked with criminal investigations.
- **Public-private partnership at EU level:** New approaches to tackle financial crime are needed, and positive examples show the benefit of connecting all involved actors, including the private sector, in order to facilitate rapid information exchange, joint analysis and more efficient investigation. Re-directing even a fraction of the considerable resources of the regime under a more targeted approach would almost certainly yield greater benefits. A recently trialled project, conducted by major banks, aimed at taking intelligence feeds from law enforcement agencies as the basis for proactive financial crime investigations, led to extremely effective output. Another positive example is the UK Joint Money Laundering Intelligence Taskforce that brings together law enforcement agencies and major banks in an initiative to improve intelligence sharing and cooperation with encouraging results. Europol fully supports such initiatives and is actively working to replicate them at an EU level as a means by which to tackle another inherent flaw in the system: its over-dependence on national frameworks.
- **Use of Europol as a pan-European hub for financial intelligence:** A significant barrier in the fight against money laundering, terrorist financing and the pursuit of financial investigations more generally stems from a lack of interoperable databases. Europol could assist in overcoming this barrier to some degree through acting as a pan-European hub for STRs, enabling information to be integrated with other sources stemming from multiple agencies across Europe and beyond. In particular the recent embedment of FIU.net in Europol may eventually enhance the exchange of financial intelligence available via this network by combining it with the products and services of Europol, with a view to creating more synergy between financial and criminal intelligence.
- **Enable the tipping-off for cross-border reporting:** Cross-border reporting and dissemination is required between EU FIUs according to article 53.4 of the 4th Anti-Money Laundering Directive (enabled through FIU.net). Nonetheless, some obliged entities report that this obligation may be in conflict with restrictions on tipping-off. A reporting entity operating across several countries should be free to notify all relevant FIUs of their concerns without this falling under the restrictions of tipping-off.
- **Improved domestic and international cooperation:** Barriers in international and diagonal information exchange between different national and overseas agencies which are not FIU counterparts may prevent the fullest exploitation of STRs. This can mean that the crucial information needed to confirm and develop STRs may never become apparent to the agency seeking it. Legal barriers at domestic level preventing much needed diagonal cooperation and information flows should be addressed.
- **Financing of terrorism:** While it is understandable that figures for reports regarding the financing of terrorism are lower than those concerning organised crime, the overall figures are nonetheless extremely limited, accounting for less than 1% of all reports filed with FIUs. From a regulatory point of view, broadening the scope of reporting obligations to include entities commonly used for terrorist financing, for example charities and NGOs, may merit further consideration.
- **Dedicated resources to address new technology:** There is a critical need to keep pace with the rapidly changing financial services industry and evolving technologies. Resources are required to afford greater possibilities to cope with increasingly large and complex data and to fully exploit its potential.
- **Close monitoring of high denomination notes:** Europol welcomes the European Central Bank's decision to stop the issuance of the EUR 500 note. However, in particular as the use of cash remains a primary reason for reporting suspicion, it is important to stress that the work of law enforcement agencies, central banks and reporting entities should not stop there; they should work in close cooperation to monitor the return and exchange of these notes over the coming years and investigate cases raising suspicions.
- **Greater access to financial intelligence across crime areas:** Financial intelligence is a precious resource not only in money laundering cases. It can also be fruitfully used for tackling a number of offences, providing indications not only on origin, transfers, destination, beneficiaries, storage and usage of funds, but also to reconstruct geographical movements of criminals, to discover the current location of persons of interest, and to retrieve all types of data around suspects. Access to STR data should be broadened beyond limiting its use to suspicion of money laundering (linked to mandated criminal offences) or terrorist financing.

([39]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

13 ANNEXES

13.1 METHODOLOGY

The findings presented in this report are based on significant research conducted by the Financial Intelligence Group at Europol.

Findings are based on both quantitative and qualitative data sources available to Europol, including the following:

- Member State and third party intelligence contributions to Europol;
- Analysis of results from a dedicated questionnaire to EU Financial Intelligence Units (FIUs), prepared for the purpose of this public report;
- Analysis of historic STR data held by Europol;
- Review of EU FIUs' annual reports;
- Open source information.

All information has been sanitised so that only information of a strategic nature, and no operationally sensitive information, is contained within the report.

13.2 DEFINITIONS

Suspicious transaction reports (STRs)

According to recommendation 20 of the FATF standards, if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report suspicions promptly to the financial intelligence unit (FIU). This reporting requirement should be a direct mandatory obligation, as per the interpretive note to recommendation 20.

A suspicious transaction is a transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction. Reporting entities assess the suspicion according to a risk-based approach for customer due diligence, real-time payment screening, transaction monitoring and behavioural monitoring, to identify changes in the respondent's transaction risk profile.

Some countries have a SAR-based reporting regime: a SAR scope is broader as it may not include any transaction, but reveals any inconsistency with a customer's business or industry practice.

The Interpretative note of FATF Recommendation 10 on Customer Due Diligence underlines four categories of risk factors such as product, service and transactions; customer risk factors; country and geography related risk factors; and distribution channel risks.

13.3 STRs, SARs, UTRs AND FIU STATISTICS

The models and working practices of Financial Intelligence Units across the European Union are so varied that even the very subject matter of this report, Suspicious Transaction Reports (STRs), creates problems regarding definitions.

Some FIUs receive STRs, based on suspicious transactions, some receive Unusual Transaction Reports (UTRs), whereby the threshold for suspicion is much lower than that of an STR and may be triggered, for example, by an automatic threshold for reporting. Others deal with Suspicious Activity Reports (SARs) which do not necessarily need to be based on a transaction, but can be reported due to suspicion around a customer's activity as a whole. Some FIUs in fact receive a combination of different types of the aforementioned reports.

Given the above, FIUs may record even the most fundamental of statistics, for example, the number of reports received by an FIU each year, in very different ways. For example, some may record the numbers of UTRs separately from STRs, others may record a combined total, while some may deal with 'report' numbers – where multiple transactions relating to the same target are recorded as a single report to the FIU.

Clearly, these differences make any comparative analysis a challenging task. For the purpose of this report, the term STR is used throughout to refer to reports received by the FIU from the regulated sector, regardless of whether these are STRs, SARs, UTRs or 'combined' reports. Where there is a need to distinguish between these types of reporting practices, it is highlighted in the body of the text or by way of footnotes.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696, or
– by electronic mail via: http://europa.eu/contact

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and noncommercial purposes.

QL-01-17-932-EN-C

EUROPOL

www.europol.europa.eu

FOLLOW US

Publications Office

ISBN 978-92-95200-82-1