Fighting tax crimes – Cooperation between Financial Intelligence Units

Ex-Post Impact Assessment

STUDY

EPRS | European Parliamentary Research Service

Author: Amandine Scherrer

Ex-Post Impact Assessment Unit

PE 598.603 - March 2017

Fighting tax crimes: ex-post evaluation of the cooperation between Financial Intelligence Units

Study

In the wake of the 'Panama Papers' leaks, the European Parliament decided to establish a Committee of inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to money laundering, tax avoidance and tax evasion (the PANA committee), on 8 June 2016. The DG EPRS Ex-post Assessment Unit (IMPT) was requested, by a PANA Coordinators' decision of 12 October 2016, to provide a study on: **Fighting tax crime: ex-post evaluation of the cooperation between Financial Intelligence Units (FIUs) at the European and international level**.

The study is divided in two parts: (1) an opening analysis prepared in-house by the DG EPRS Ex-post Assessment Unit (IMPT) that covers EU FIUs and the EU legal framework, and (2) an outsourced comparative analysis that focuses on FIUs in Canada, France, Switzerland and the UK.

Abstract

Since the mid-1990s, the development of anti-money laundering (AML) strategies at the international level has led to the establishment of Financial Intelligence Units (FIUs) at national level. FIUs serve as national centres for the receipt and analysis of suspicious transaction reports (STRs). They collect and analyse data that help to establish links between suspicious financial transactions and illegal activities. FIUs are thus important players in the prevention of money laundering. Furthermore, given the strong cross-border dimensions of money laundering, the exchange of information across FIUs is key to ensure illicit flows of money are properly detected and subsequently investigated by law enforcement authorities. This study intends to provide a better understanding of the current state of play in relation to the role, powers and activities of FIUs in fighting financial crime in general and tax crimes in particular, both at European and international level.

AUTHOR of the opening analysis:
Dr Amandine Scherrer, Ex-Post Impact Assessment Unit

AUTHORS of the comparative analysis:
Dr Anthony Amicelle (International Centre for Comparative Criminology, Université de Montréal, Quebec, Canada), with Julien Berg (École de Criminologie, Université de Montréal) and Killian Chaudieu (École des sciences criminelles, Université de Lausanne, Switzerland)

The comparative analysis was written at the request of the Ex-Post Impact Assessment Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament.

ACKNOWLEDGMENTS
The authors would like to thank officials of the European Commission and participants of the EU FIU Platform, as well as the stakeholders interviewed for this assessment for their useful input.

RESPONSIBLE ADMINISTRATOR
Amandine Scherrer, Ex-Post Impact Assessment Unit
To contact the Unit, please e-mail EPRS-ExPostImpactAsessment@ep.europa.eu

ABOUT THE PUBLISHER
This paper has been compiled by the Ex-Post Impact Assessment Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate–General for Parliamentary Research Services of the Secretariat of the European Parliament.
To contact the Unit, please email EPRS-ExPostImpactAssessment@ep.europa.eu

LANGUAGE VERSIONS
Original: EN
This document is available on the internet at: www.europarl.europa.eu/thinktank

Manuscripts completed in March 2017. Brussels © European Union, 2017

PE 598.603
ISBN 978-92-846-0701-3
doi:10.2861/2427
QA-02-17-248-EN-N

Table of Contents

List of abbreviations and acronyms

CAD:	Canadian dollar
CRA:	Canada Revenue Agency
ESW:	Egmont Secure Web
EU:	European Union
FATF:	Financial Action Task Force
Fincen:	Financial Crimes Enforcement Network (USA)
FININT:	Financial Intelligence
Fintrac:	Financial Transactions and Reports Analysis Centre of Canada
FIU:	Financial Intelligence Unit
HoFIUs:	Head of Financial Intelligence Units
ICO:	Information Commissioner's Office
IMF:	International Monetary Fund
MROS:	Money Laundering Reporting Office Switzerland
NCA:	National Crime Agency (UK)
Tracfin:	Traitement du renseignement et action contre les circuits financiers clandestins (France)
SAR:	Suspicious Activity Report
STR:	Suspicious Transaction Report

List of tables and charts

Methodology

This study is divided in two parts: (1) an opening analysis prepared in-house by the Directorate–General for Parliamentary Research Services (DG EPRS) Ex-Post Impact Assessment Unit (IMPT), which covers EU FIUs and the applicable EU legal framework, and (2) an outsourced comparative analysis focusing on FIUs in Canada, France, Switzerland and the United Kingdom (UK).

The opening analysis aims at providing an assessment of the EU legal framework as regards EU FIUs and analyses their existing capacities to tackle tax-related crimes. The analysis therefore examines the extent to which the provisions related to FIUs in the third Anti-Money Laundering Directive – that were to be implemented by the Member States by 15 December 2007 – have been properly implemented. While the study takes the changes brought by the adoption of the fourth Anti-Money Laundering Directive adopted in 2015 into account, it refrains from drawing premature conclusions on proper implementation of these new provisions, since the Member States are to transpose the fourth Directive by the end of June 2017. The analysis of the EU framework is based on several sources that were extremely useful in assessing the capacities of EU FIUs to perform their tasks and exchange information at EU and international level.[1] The opening analysis naturally takes account of the outsourced comparative analysis.[2]

This comparative analysis examines four particular FIUs and investigates their differences and the challenges they encounter as regards transnational cooperation on financial intelligence. The sample chosen, which gathers FIUs from two EU Member States (France and the United Kingdom), one FIU from a European country with a major financial centre (Switzerland) and one North American FIU (Canada), intends to provide a better understanding of the current state of play in relation to the role, powers and activities of FIUs in fighting financial crime in general and tax crimes in particular. The comparative analysis relies both on qualitative and quantitative data. It draws on document analysis (official reports and statistics from the Egmont Group, the EU, the FATF and FIUs under examination), and semi-structured interviews with officials from FIUs and Europol.

The full study was peer-reviewed internally by DG EPRS Ex-ante Impact Assessment Unit (IMPA) staff, and the opening analysis was also submitted to representatives of the EU FIU Platform for comment.

[1] These include: The 2013 final report of the ECOLEF Project (*Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy*, funded by the European Commission, DG Home Affairs); A 2015 report published by the OECD: *Improving co-operation between tax and anti-money laundering authorities. Access by tax administrations to information held by financial intelligence units for criminal and civil purposes;* a 2017 report prepared for the EU FIUs Platform: *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information.*

[2] Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and the United Kingdom.*

Part I: EU FIUs and the applicable EU legal framework

Key Findings

EU FIUs have different structures, resources and powers across the Member States. These differences affect the ways in which EU FIUs collect and analyse information, and ultimately impact exchange of information between them:

(1) At a practical level, time delay in responses to requests affects FIUs cooperation, and the quality and content of the replies to requests are not necessarily helpful.

(2) Not all EU FIUs are empowered to approach banks and financial institutions with requests for information. This means that the capacity of some FIUs to request information from reporting entities on behalf of foreign FIUs can sometimes be hampered.

Concerning tax-related crimes, specific issues arise:

(3) Tax crime was only recently recognised as a predicate offence of money laundering (in the fourth AML Directive). Although the directive explicitly indicates that differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information, cooperation between FIUs can still be refused on the grounds of the significant differences across Member States as to how predicated offences to money laundering are defined and criminalised.

(4) In some EU Member States, mutual cooperation between FIUs and tax authorities still lacks clear agreement and/or memorandum of understanding to ensure tax compliance.

(5) Not all EU FIUs have proper access to information on bank account holders and beneficial ownership. Central registers of bank accounts are not necessarily in place in all EU Member States. While the fourth AML Directive encourages EU Member States to put such systems in place, this is not mandatory. As regards access information on beneficial owners, the obligation to set up central registers for this purpose laid down in the fourth AML Directive has not to date been fulfilled in all Member States. As a result, only a few EU FIUs can obtain such information at present. This lack of dedicated centralised national databases is an area of concern shared by many EU FIUs.

1. FIUs in the context of international standards and EU requirements

1.1. Establishment of FIUs in the anti-money laundering landscape

At international level:

Since the beginning of the 1990s and the development of anti-money laundering (AML) strategies at national level (especially in the United States of America (USA)), and their dissemination at international level, depriving criminals of the proceeds of their crimes has increasingly been seen as an important tool to combat all serious crimes.[3] As underlined in a 2004 International Monetary Fund (IMF) report dedicated to Financial Intelligence Units (FIUs),[4] as countries developed their anti-money laundering strategies they found that law enforcement agencies had limited access to the relevant financial information. It thus 'became clear that the strategy required them to engage the financial system in the effort to combat laundering while, at the same time, seeking to ensure the retention of the conditions necessary for its efficient operation'.[5] The first few financial intelligence units (FIUs) were established in the early 1990s, in response to the need for a central agency to receive, analyse, and disseminate financial information to combat money laundering.[6] FIUs were created as specialised units dealing with the analysis of suspicious financial transactions, and thus with distinct missions (intelligence analysis) as compared to law enforcement activities focusing on crimes (as opposed to suspicions).

In 1995, the 'Egmont group' (comprising a core group of FIUs) was established at the initiative of the US FIU (FinCen), its name originating in the organisation of the group's first meeting at the Egmont-Arenberg Palace in Brussels (Belgium). The Egmont Group was originally intended to serve as an international and informal network of FIUs, promoting and improving the international cooperation that had become key in a context of intensification of cross-border financial flows.[7] The group provided the first definition of an FIU:

> A financial intelligence unit (FIU) is a central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the

[3] See: Woodiwiss M., 'Transnational organized crime: The strange career of an American concept', in Beare M. (ed.), *Transnational Organized Crime*, Ashgate, 2003; Scherrer A., G8 against transnational organised crime, Ashgate, 2009.
[4] IMF, *Financial Intelligence Units: An Overview*, 2004.
[5] IMF Report, op. cit., p.1, quoting Gilmore W.C., *Dirty Money: The Evolution Of Money-Laundering Counter-Measures*, Council of Europe Press, 1999, p.103.
[6] See the comparative analysis in Part II: Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom.* The paper describes the emergence and evolutions of FIUs in-depth (see Section 1).
[7] Egmont Group, Annual report, 2015; See: United State General Accounting Office - GAO, Statement submitted to the Subcommittee on General Oversight and Investigations, Committee on Banking and Financial Services, House of Representatives, *FinCen's Law enforcement Support, Regulatory, and International Roles*, 1998, GAO/T-GDD-98-83.

> competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing.

The secretariat of the Egmont Group is hosted in Toronto (Canada) since 2008, and at the time of writing, the group comprises 152 members.[8]

In 2003, the Financial Action Task Force (FATF) – the inter-governmental body established in 1989 to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering – adopted a revised set of recommendations on combating money laundering that, for the first time, explicitly included recommendations on the establishment and functioning of FIUs, drawing from the Egmont Group's above-mentioned definition:

> (Recommendation 26): Countries should establish a FIU that serves as a national centre for receiving (and, as permitted, requesting), analysis and dissemination of Suspicious Transaction Reports (STRs) and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STRs.[9]

In terms of cooperation, the Egmont Group has, since its inception, enabled the establishment of arrangements and models for memorandum of understanding between FIUs around the world.[10]

At European Level:

Although not specifically denominated as such, FIUs were already envisaged in the first and second EU AML Directives of 1991 and 2001 as the authorities in charge of receiving and analysing suspicious transactions reports (STRs). As of 2000, all EU Member States had set up FIUs to collect and analyse information with the aim of establishing links between suspicious financial transactions and underlying criminal activity in order to prevent and to combat money laundering.[11]

The first Anti-Money Laundering (AML) Directive,[12] adopted in 1991, laid down rules for reporting suspicious transactions. The action plan to combat organised crime approved

[8] Egmont Group website.
[9] Financial Action Task Force (FATF), Recommendations, 2003.
[10] For the latest version of these principles, see: Egmont Group, Principles for information exchange between FIUs, June 2013, available on the Egmont Group website.
[11] As indicated in Recital 2 of the Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA).
[12] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system

by the Amsterdam European Council in 1997 recommended that cooperation should be improved between contact points competent to receive suspicious transaction reports (STRs) pursuant to the above-mentioned first AML Directive. This led to the adoption of the Council Decision of 17 October 2000, concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.[13] The Council Decision laid down provisions for the organisation of FIU at Member State level and for cooperation between them. It furthermore laid down specific provision as regards protected channels of communication between EU FIUs, which led to the setting up of FIU.NET in 2007-2008, with the financial support of the European Commission.

If the second AML Directive[14] adopted in 2001 does not refer explicitly to FIUs, it mentioned the 'authorities responsible for combating money laundering' and adopted a broader definition of money laundering, taking into account underlying offences such as corruption and thus expanding the predicate (prior) offences.

Adopted in 2005, the third AML Directive[15] expanded further the aim of EU AML efforts, by enlarging the scope of the AML requirements to serious offences and terrorist financing. It furthermore explicitly requires Member States to set up national FIUs.

The European Commission is tasked with assisting to facilitate coordination, including the exchange of information between FIUs within the Community (Article 38 of the third AML Directive). In 2006, the Commission set up the EU Financial Intelligence Units Platform, which brings together EU FIUs and helps them cooperate.[16]

1.2. Limits and opportunities of assessing FIU cooperation in the fight against tax crimes

Tax related crime has not necessarily been consistently dealt with across all the EU FIUs, as in some Member States these crimes are not recognised as predicated offence of money laundering. Although the fourth AML Directive explicitly includes 'tax crime' as a predicate offence of money laundering, it does not harmonise an EU level definition. There is a clear lack of consensus on tax crime, as developed in Section 3.

for the purpose of money laundering.

[13] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

[14] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

[15] Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[16] The EU FIU platform is not of operational nature. It is aimed at facilitating discussions and exchange of good practices at EU level among FIUs. The platform usually meets on a quarterly basis.

Furthermore, at the time of writing, the implementation of the new provisions introduced in the 2015 fourth AML Directive[17] is difficult to assess. Indeed, these provisions are to be transposed by the Member States by the end of June 2017, in accordance with Article 67 of the fourth directive. The table below outlines the main provisions of the third and fourth AML Directives related to FIUs. As shown, the fourth directive details the organisation of EU FIU cooperation much further:

Table 1 – EU legal framework: main provisions related to EU FIUs

Third AML Directive (2005)	Additional provisions in the 2015 Fourth AML Directive, to be transposed in June 2017
Each Member State shall establish an FIU in order to combat money laundering and terrorist financing (Article 21.1) Each national FIU must be given adequate resources to fulfil its tasks (Article 21.2) FIUs have to be given access on a timely basis to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks (Article 21.3) The institutions and persons covered by the directive[18] must inform their respective FIUs if they suspect that money laundering or terrorist financing is being or has been committed or attempted. They are also required to provide all necessary information if requested (Article 22.1). Member States must require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, in accordance with their national law (Article 32).	**On access to information**: Member States shall require that information on legal and beneficial owners can be accessed in a timely manner by competent authorities and FIUs (Article 30.2). Information on the beneficial ownership is accessible in all cases to FIUs without any restriction (Article 30.5). **On cooperation**: Member States shall ensure that FIUs cooperate with each other to the greatest extent possible, regardless of their organisational status (Article 52), and even if the type of predicate offences that may be involved is not identified at the time of the exchange (Article 53.1). When an FIU receives a suspicious transaction report which concerns another Member State, it shall promptly forward it to the FIU of that Member State (Article 53.1). In addition, EU FIUs are entitled to use all domestically available powers to respond to foreign requests (Article 53). When a request for information is made to an FIU from another EU FIU, the FIU to whom the request is made shall respond in a timely manner. When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall transfer requests and answers promptly (Article 53.2). An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law (Article 53.3).

[17] Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
[18] This directive applies to (Article 2): credit institutions; financial institutions; auditors, external accountants and tax advisors; notaries and other independent legal professionals; trust or company service providers; real estate agents; other natural or legal persons trading in goods and casinos.

Third AML Directive (2005)	Additional provisions in the 2015 Fourth AML Directive, to be transposed in June 2017
	When exchanging information and documents, the transmitting FIU may impose restrictions and conditions for the use of that information (Article 54). Member States shall ensure that the information exchanged is used only for the purpose for which it was sought or provided and that any dissemination of that information is made subject to the prior consent by the FIU providing the information (Article 55.1). Any refusal to grant consent shall be appropriately explained (Article 55.2). Differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law (Article 57).

As an addition, prompted by the terrorist attacks of late 2015 and the 'Panama Papers' leaks in April 2016, the European Commission decided to review the EU anti-money laundering framework once more and to propose new amendments that are, at the time of writing, under negotiation.[19] There are therefore some evident limits to assessing the role of FIUs in fighting tax crime in such a rapidly evolving framework.

However, as the third AML Directive (2005) was to be implemented by the Member States by 15 December 2007 (Article 45.1), it is worth noting that, as can be seen in the comparative analysis in Part II (which compares FIUs in Canada, France, Switzerland and the UK), although the third directive did not mention tax evasion per se, it did include 'serious offences' in the scope of the AML Directive. The latter are defined as 'all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months',[20] and as such, cover tax-related offences in a number of Member States.[21]

Moreover, several assessments of the transposition and the implementation of the third AML Directive are available, and these point out significant challenges affecting the capacities of FIUs to effectively fight money laundering and terrorist financing. Among

[19] Proposal for a Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Strasbourg, 5.7.2016, COM(2016) 450 final. For an EPRS initial appraisal of the European Commission Impact Assessment on these amendments, see: Collovà C., *Prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, PE 587.354, 2016.
[20] Directive 2005/60/EC, op.cit.
[21] See Section 1 of comparative analysis in Part II: Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom*.

these significant challenges, some bear particular relevance for the fight against tax crimes and efficient cooperation in that field, as developed in section 3 hereafter.

2. FIU structures, resources and cooperation channels

2.1. Different structures

The successive EU AML Directives do not lay down specific provisions on how FIUs should be structured and organised at the Member State level. In its 2004 report,[22] the IMF proposed a typology, used ever since, to classify FIUs. Depending on where FIUs are located in the Member States administrative bodies, the IMF report identified four types of FIUs:

- Administrative type FIUs
- Law enforcement type FIUs
- judicial or prosecutorial FIUs
- hybrid FIUs.

The final report of the EU-funded 'ECOLEF' project, released in 2013[23] (hereafter, the ECOLEF study) attempted to give a complete and comprehensive inventory of the then 27 EU Member States' FIUs and to classify them according to the IMF's typologies.[24] The report found that the vast majority of EU FIUs were either administrative or law enforcement and only four considered themselves to be of the judicial or hybrid types. The ECOLEF study concluded that, to a large extent, as only a handful of FIUs considered themselves to be of a different typology, Member States agreed with the typology assigned to their FIUs.[25]

These findings are confirmed in a recent report prepared for the EU FIU Platform[26] (hereafter, the EU FIU Platform report), even though the latter only refers to three models of FIUs: administrative, law enforcement (or judicial) and 'hybrid'. At present, the EU FIUs are distributed as follows:[27]

[22] IMF, *Financial Intelligence Units: An Overview*, 2004.
[23] Project 'Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy - ECOLEF' (funded by the European Commission - DG Home Affairs, JLS/2009/ISEC/AG/087), Final Report, February 2013.
[24] Ibid, p.140
[25] p.143.
[26] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information*, Report prepared for the EU FIUs Platform, December 2016 (led by FIU Italy - *Unità di Informazione Finanziaria per l'Italia* - UIF). It should be noted that this Mapping exercise is based on a comprehensive survey across EU FIUs. The results of the survey aim at describing challenges encountered in the implementation of EU anti-money laundering and terrorist financing provisions, with a view to devising possible solutions or mitigations. All information and data managed during this mapping exercise have remained confidential and anonymous. As a result, the report does not report back on individual FIUs.
[27] Ibid., p.5-7.

- 12 EU FIUs have indicated that they have an administrative nature (located for instance into the ministries of Finance, Justice or Interior, or embedded into the Central Bank or a supervisory authority): Belgium, Bulgaria, Croatia, the Czech Republic, France, Italy, Latvia, Malta, Poland, Romania, Slovenia and Spain;
- 11 EU FIUs have indicated that they are organised under a law enforcement (police and/or justice) model: Austria, Estonia, Finland, Germany, Ireland, Lithuania, Portugal, Slovakia, Sweden, Luxembourg and the UK;
- 5 EU FIUs have described themselves as having a 'hybrid' nature, due to the combined presence of administrative and police elements: Cyprus, Denmark, Greece, Hungary, and the Netherlands.

The EU FIU Platform report cautiously underscores that 'the identification of these different institutional models is purely conventional and the distribution of EU FIUs among them is somewhat arbitrary. Each FIU maintains its distinctive peculiarities, even within each category'.[28] The ECOLEF study already noted that critical aspects (such as FIU staff background, task distribution, or access to databases), were not necessarily correlated with the type of FIU.[29]

This aspect is confirmed in the comparative analysis (Part II of this study), which underlines that major differences exist between FIUs falling within the same model, including in relation to the types of reporting they receive, as well as their access to various national databases.[30] Furthermore, the commonly held assumption that 'law enforcement' FIUs have better access to police and intelligence information does not hold true in the four FIUs under examination.[31] As analysed further in section 3.1, and in relation to tax crimes, other elements – such as how the cooperation with tax authorities works in practice – are more relevant when assessing FIUs' capacity to perform their tasks adequately.

2.2. Resources

In terms of human resources, according to the EU FIU Platform report, EU FIU staff dedicated to FIU core functions (i.e., receipt of suspicious transactions reports (STRs), analysis, dissemination and international cooperation), varies greatly across Member States: from five (in Ireland) to 289 employees (in Germany).[32] The percentage of FIU staff dedicated to these core functions also varies greatly: from 33 % (Malta) to 100 % (in the UK).

[28] On this matter, the report reminds that besides the 'status' of an FIU, an important organisational element is the embedment of FIUs into bigger organisations, as this affects FIUs' autonomy. See: *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit.

[29] See: ECOLEF Study, op.cit., p.162.

[30] See our comparative analysis (Part II): Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom*, Section 1.1.

[31] Ibid.

[32] The comparative analysis gives the following number for Canada, France, Switzerland and the UK: 350 staff (Canada); 150 staff (France); 20 staff (Switzerland); 150 staff (UK). See: Amicelle A.,

FIUs may also perform other functions, such as drafting AML legislation, issuing guidelines for the reporting entities on how to report, supervising the reporting entities, and proposing sanctions when noticing irregularities during supervision controls.[33] However, these staffing figures should not lead to over-simplified conclusions: indeed, as suggested by in the EU FIU Platform report, the adequacy of human resources available should be assessed against FIUs' respective workloads, particularly as regards the number of disclosures received, the type of analyses and disseminations performed and the volume of international exchanges.[34] For instance, in 2014, the German FIU received approximately 24 000 suspicious transaction reports (STRs).[35] In comparison, in 2012, the Irish FIU received approximately 12 400 STRs.[36]

In terms of budget, according to the EU FIU Platform report, figures can vary extremely: from €600 000 to above €14 million per year.[37] However, these discrepancies, once again, are not necessarily helpful in assessing if FIUs are receiving enough financial means to perform the tasks they are assigned. FIUs' budget independence provides rather more valuable information in that regard. As outlined both by the ECOLEF study and the EU FIU Platform report, budget independence increases the FIUs' capacity to manage the sums required for their operational needs independently. Less than half of the EU FIUs have, in the context of the EU FIU Platform report, indicated that they dispose of an autonomous budget, i.e. an amount of funds assigned specifically (and exclusively) to them for expense coverage and managed independently. The majority of EU FIUs indicated that their budget was part of the budget of a larger institution.[38] As underlined in the ECOLEF study, this dependency can cause problems, specifically in times of budget cuts.[39]

The EU FIU Platform report notes that, overall, the available financial, human and technical resources are deemed adequate to meet EU FIUs' existing needs. It nevertheless underlines that concerns are voiced from FIU staff across the EU Member States regarding the FIUs' continued capacity to face expected developments – as envisaged in the implementation of the fourth AML Directive – in the absence of significant increases in available resources. The report refers notably to the fact that, in accordance with the fourth Directive, FIUs are now required to make use of available domestic powers to respond to foreign requests and to forward to interested foreign counterparts STRs that concern another Member State, which brings an increase in activities in addition with a workload that is constantly increasing, particularly as regards the volumes of STRs

Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom* (Introduction).

[33] On that matter, see: ECOLEF study, op.cit., p.149.

[34] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.12.

[35] See: Financial Intelligence Unit (FIU) Germany - Annual Report 2014.

[36] See: Department of Justice and Equality of Ireland, Anti-Money Laundering Compliance Unit, Statistics Report, 2012.

[37] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.13.

[38] Ibid., p.12.

[39] ECOLEF Study, op.cit., p.146.

received, the information exchanged between counterparts, and the demands associated with different forms of domestic cooperation.[40]

2.3. Suspicious transaction reports: various sources and varying quality

FIUs' activities are based on information concerning suspicious financial transactions. All FIUs receive completed suspicious transactions reports (STRs) from obliged reporting entities,[41] in accordance with the third AML Directive.

Several challenges arise when considering the quantity and quality of obliged entities' reporting. Our comparative analysis (Part II of this study) explains in detail how the process of reporting works in practice. It also analyses the origin of STRs that FIUs receive in the four countries under examination (Canada, France, Switzerland and the UK) and notes the following:[42]

- Firstly, financial institutions are the main providers of suspicious transaction/activity reports for FIUs. Legal professionals and accountants do not provide a significant proportion of STRs.
- Secondly, the number of STRs received is not necessarily correlated with the size of the national financial market at stake. The paper gives the example of Switzerland – regularly criticised for 'under-reporting'.
- Thirdly, for financial institutions, avoiding reputational damage is key in the performance of their reporting obligations: this can result in either over-reporting or under-reporting. The challenge here lies in knowing where to draw the line between defensive reporting (to avoid criticism of non-compliance with AML regulation) and intelligence-relevant reporting.

Despite significant methodological limitations, attempts have been undertaken to quantify the overall share of STRs sent to FIUs, analysed by them then transmitted to law enforcement authorities and ultimately leading to prosecution, to determine an average 'efficiency rate' of this type of reporting obligation. A 'Cost of non-Europe' report on organised crime (published in 2016 by the European Parliamentary Research Service) for instance looked at the EU Member States for which comparable data were available (Belgium, the Czech Republic, Estonia, Germany, Latvia, Lithuania, Luxembourg, Romania, Slovakia, and Slovenia,), and found, based on EUROSTAT figures from 2013, that of the overall number of STRs completed in these Member States and sent to their

[40] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.25.

[41] Obliged entities are, in accordance to Article 2 of the third AML Directive: credit institutions; financial institutions; auditors, external accountants and tax advisors; notaries and other independent legal professionals; trust or company service providers; real estate agents; other natural or legal persons trading in goods and casinos.

[42] See our comparative analysis (Part II): Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom* (Sections 1.2 and 1.3).

respective FIUs, 29 % were then transmitted to law enforcement; of those transmitted to law enforcement, 54 % resulted in a case being brought to court. Thus, approximately 16 % of all completed STRs led to actual prosecutions. However, no statistics exist on how many of these cases have led to convictions.[43]

Moreover, while all FIUs receive STRs, some have additional access to other sources of information, mainly based on monetary thresholds.[44] Threshold-based disclosures refer to particular types of transactions (for example, cash deposits or withdrawals or transfers of funds) that have to be reported whenever a specified quantitative threshold is reached or exceeded, regardless of the suspicious nature of the underlying activities. This notification differs from a STR, which applies regardless of the amount involved.

As the EU FIU Platform report reiterates, the majority of EU FIUs have access to mandatory disclosures filed with customs agencies concerning the physical cross-border transportation of cash, in accordance with EU Regulation (EC) 1889/2005.[45] However, only a minority of EU FIUs[46] receive threshold-based reports from obliged entities (which are the same as those of the entities obliged to disclose STRs), in addition. The threshold to trigger these cash disclosures in the EU Member States that apply this provision, ranges between €10 000 and €32 000.

As noted in our comparative analysis (Part II), threshold-based disclosures are seen as critical tools against tax evasion by some countries, such as Canada, where financial institutions have been required since 2015 to send electronic funds transfer reports of CAD10 000 (approximately €7 000) or more to the Canadian tax authority, in addition to the national FIU. Indeed, avoiding detection via the banking system through using cash seems widespread, especially in cash-based economies.

At the moment, threshold-based disclosures are not mandatory at EU level. The fourth AML Directive merely provides that FIUs can receive other information in addition to STRs, including threshold-based information (as specified in Recital 37).

Regarding virtual currencies, it is worth mentioning that the European Commission proposes amending Article 2 of the fourth AML Directive currently under discussion to add virtual currency exchange platforms as well as custodian wallet providers to the list of obliged entities.[47]

---

[43] See Annex 1 on Organised Crime in: van Ballegooij W. and Zandstra T., *The Cost of Non-Europe in the area of Organised Crime and Corruption*, PE 579.318, 2016, p.60.

[44] See annexed comparative analysis. This additional source of information is found in two of the four FIUs under examination: France and Canada.

[45] EU Regulation (EC) 1889/2005 on controls on cash entering or leaving the Community. Under Article 3, 'any natural person entering or leaving the Community and carrying cash of a value of €10 000 euro or more shall declare that sum to the competent authorities of the relevant Member States'.

[46] These include: Bulgaria, Croatia, Estonia, France, Lithuania, The Netherlands, Poland, Romania, Slovenia, Spain. See: *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.81.

[47] See: Proposal for amending Directive (EU) 2015/849 on the prevention of the use of the financial

2.4. Channels of cooperation

As our comparative analysis (Part II) describes, FIUs have various reasons to cooperate with other FIUs at European and international level. Cross-border transactions, bank customers of foreign nationality, and national citizens living or working in another country, are obvious reasons why exchange of information between FIUs is critical. Two main channels of communication for cooperation are in place for FIUs worldwide: via the Egmont Group (with the Egmont Secure Web (ESW), technically maintained by FinCen, the US FIU), and for EU Member States via a decentralised system: the FIU.NET, embedded in Europol since January 2016.

Both platforms provide secure channels of communication for the exchange of information. However, although the ESW and the FIU.NET are based on the same goal of sharing information between FIUs, our comparative analysis (Part II) outlines a number of differences between them that suggest FIU.NET's clear added-value[48] at the European level. FIU.NET's sophistication is seen as an asset for the following reasons:[49]

- data can be retrieved and integrated directly in FIU databases, whereas the ESW mainly works as a secure email connection;
- FIU.NET enables multilateral exchanges. FIUs who are members of the FIU.NET can choose to exchange bilaterally, multilaterally or even 'in full' with all connected counterparts. The exchanges can vary from a minimal approach (such as 'known/unknown requests' to check whether individual's names are found in another EU Member State database), to a 'case file' giving further details and justification to obtain information from the other FIU(s). In the latter scenario, the FIU can then link different entities to the case file;
- FIU.NET has recently introduced 'Ma3tch technology': EU FIUs now have a number of options available to them, including simple 'known/unknown' or 'hit/no hit' requests to one or several counterparts;
- matching subjects through the FIU.NET is also performed with other connected datasets, using open source tools such as World-Check.

Overall, from a European perspective, the ESW and the FIU.NET are widely perceived as complementary. FIU.NET is used in cooperation with EU counterparts, whereas the ESW is used for exchange of information with non-EU counterparts. For exchange of information with FIUs that are neither part of the FIU.NET nor the ESW, traditional means of communication are used, such as secure emails or even fax messages.[50]

system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Strasbourg, 5 July 2016 COM(2016) 450 final.

[48] See: Europol website.

[49] See our comparative analysis (Part II): Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom* (Section 2.1).

[50] Ibid.

2.5. FIU-to-FIU cooperation and exchange of information

The EU FIU Platform report and our comparative analysis (Part II) both point to significant obstacles regarding FIU-to-FIU cooperation. These include:

- Not all EU FIUs are empowered to approach obliged entities with requests for information. In many cases, these requests are conditional to the prior receipt of suspicious transaction reports (STRs). This also means that some FIUs cannot request information from reporting entities on behalf of foreign FIUs without related suspicious transactions in their database;
- Time delays in responses to requests affect FIU cooperation, and replies to requests are not necessarily helpful: sometimes replies are limited to 'known/unknown', without further explanation.

Other obstacles stem from differences in the nature and powers of FIUs, due to their domestic features (as noted above). Some of these challenges have been partly addressed in the fourth AML Directive. Under Article 32(3), EU FIUs should be able to obtain information from any obliged entity, regardless of the existence of prior disclosures. Article 53 of the Directive furthermore requires the EU FIUs to respond to EU counterparts 'in a timely manner'. The current amendments to the fourth AML Directive currently under discussion, include the aim of reducing the delay in exchange of information and including an obligation to answer requests.[51]

The exchange of information between FIUs is always associated with the explicit determination of appropriate conditions of use (purpose limitation), which depends largely on domestic requirements, as can be seen in the comparative analysis (Part II). The rules for information dissemination include three main options:

- As a general rule, and as agreed among all FIUs around the world, an FIU cannot disclose information received by another FIU outside its agency without the prior written permission of the disclosing FIU.[52]
- The disclosing FIU can authorise its FIU counterpart to disseminate the information outside its agency for intelligence purposes only (e.g. informally), not for evidence purposes.
- The FIU accepts that their counterpart disseminate and use the information beyond informal intelligence, for instance, for evidence purposes.

[51] The average time response between FIUs was examined in the ECOLEF study, which noted that response to request can vary from 24 hours to 30 days. On the basis of the set of data obtained, the study furthermore noted that cooperation between EU FIUs was not necessarily faster than with non-EU FIUs. See: ECOLEF study, p.237. This is confirmed in the EU FIU Platform report, according to which the time delay for responses to requests for information submitted by their counterparts can vary from hours to two months or more. See: *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.154.

[52] Egmont Group operation guidance for FIU activities and the exchange of information, 2013 (available on the Egmont Group website).

As detailed in section 3.3 hereafter, these information sharing principles can create significant obstacles for cooperation, including regarding detection of tax related crime. For example, some FIUs might accept to exchange some information, but will specify that this information cannot be used for tax related matters.

An additional and overarching challenge detailed in the EU FIU Platform report is the blurred distinction between intelligence and investigation. The report states 'FIU-to-FIU cooperation is exclusively aimed at facilitating the FIUs' typical function of analysis of suspicions, an activity which is well distinct and separate from investigation and prosecution on the same facts (performed by law enforcement bodies and prosecutors). Information exchanged between FIUs, therefore, is not destined to be used in the context of investigations, prosecutions or legal proceedings'.[53] However, as the report further notes, 'the distinction between analysis and investigation is not always neatly drawn and these two tasks may not be separated in a sufficiently clear-cut manner in all cases, both as regards domestic FIUs' functions and in the course of FIU-to-FIU cooperation'. As a result, 'in some cases the capacity to provide cooperation to other FIUs in support of analytical tasks is impaired by the existence of investigations or prosecutions in the country of the requested FIU and by the need to obtain prior authorisations from competent prosecutors (importantly, these limitations may apply equally to police and other types of FIUs)'.

To address these issues, the report suggests that the distinction between analysis and investigation, both as regards FIUs' domestic activities and their cooperation, should be reinforced and clarified.

3. Main challenges for FIU action to fight tax crimes

In addition to the above-mentioned challenges affecting FIUs' missions in general, specific issues arise where tax crimes are concerned:

- At national level, FIUs are not necessarily the sole recipient of suspicious transactions reports (STRs). This affects the ways in which cooperation with tax authorities works.
- Access to information on bank account holders and beneficial ownership, both at national, European and international level faces significant obstacles.
- The 'fiscal excuse' (whereby information received cannot be used in tax-related investigations) is often used to restrict exchange of information and cooperation.

[53] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.140-142.

3.1. At national level: cooperation between FIUs and tax authorities

The issue of multiple reporting:

In practice, EU FIUs do not act in 'silos' when it comes to the receipt of suspicious transactions reports (STRs), in particular in the area of tax-related crimes. While FIUs are the unique recipient of STRs in the majority of Member States, in some Member States the obliged entities transmit their report simultaneously, where relevant, to both the FIU and the relevant authorities. These include the fiscal authorities, which can then tackle the cases where suspicious transactions exist.[54]

Therefore, in relation to tax offences, analysis of STRs can be carried out by several bodies. Where this system of 'multiple reporting' is in place, the EU FIU Platform report indicates that this raises several concerns, including the fact that different investigations by different bodies may be launched 'on the same facts and based on the same information, which certainly may bring peculiar challenges in terms of coordination of actions by different agencies and consistencies in findings and results'.[55]

Models of FIUs/tax authorities' cooperation:

In its 2015 report dedicated to the cooperation between tax authorities and FIUs,[56] the OECD, based on a survey conducted in 28 countries (including 16 EU Member States), identifies various models of tax authority access to STRs:[57]

- Unfettered independent tax administration access to STRs (whereby both the FIU and the tax administration has equal opportunity to use STRs and can each make independent decisions about which cases to use and how).
- Joint FIU and tax administration decision-making on allocation of STRs (whereby a joint decision-making process between the FIU and the tax administration decides how STRs will be used).
- FIU decision-making on allocation of STRs (whereby the FIU decides which STR related information to share with the tax administration, according to national legislation).

The OECD report assesses both the strengths and the challenges of these three models. While not concluding which would be the best model to tackle tax crimes, the report provides interesting insights on how the challenges of these various models could be mitigated, and enforcement of tax compliance maximised:

---

[54] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.30.
[55] Ibid., p.31.
[56] OECD, *Improving co-operation between tax and anti-money laundering authorities. Access by tax administrations to information held by financial intelligence units for criminal and civil purposes*, September 2015.
[57] Ibid., p.15 and sub.

- for the first model, and to avoid conflict between each authority's approach to any specific case, clear administrative agreement (such as a memorandum of understanding) should be put in place;
- for the second model, building close working relationships between the persons responsible in each authority and ensuring regular meetings where the STRs are allocated should be provided (via a memorandum of understanding for instance);
- for the third model, and to ensure FIU staff properly identify elements of tax-related crime, specific training for FIU staff on tax-related issues could help. Another option would be to provide seconded staff to the FIU to assist in detecting tax risks

Access to tax-related information:

Mutual cooperation and reciprocal arrangements between FIUs and tax authorities furthermore require that FIUs have access to tax-related data and information to effectively fight tax crimes.

As noted in the EU FIU Platform report, some EU FIUs encounter limitations regarding access to information held by financial, administrative or law enforcement national bodies. The report highlights concerns on the narrow and little harmonised scope of information and databases available to FIUs for analysis and cooperation.

The ECOLEF study research team recently presented updated findings[58] that echo these concerns, showing that in at least two Member States, FIUs do not have access to tax-related information.[59] The state of play at EU level thus suggests that there is room for improvement in mutual cooperation between FIUs and tax authorities.

Ultimately, increasing levels of cooperation between tax administrations and FIUs, intensifying information-sharing and developing an agreed approach to the analysis of STRs is key to ensuring tax compliance.

3.2. Access to information on beneficial ownership

Article 8 of the third AML Directive laid down provisions for the identification of beneficial owners, as part of the customer due diligence (CDD) exercise to be performed by obliged entities. The fourth AML Directive provides further detailed provisions, including concerning FIU access to beneficial owners information:

> (Recital 14) 'With a view to enhancing transparency in order to combat the misuse of legal entities, Member States should ensure that beneficial ownership

[58] Prof. Dr. Brigitte Unger, Workshop organised for the PANA Committee on Money Laundering and Tax Evasion, 27 January 2017: power point presentation.
[59] Germany and Ireland.

> information is stored in a central register located outside the company, in full compliance with Union law. Member States can, for that purpose, use a central database which collects beneficial ownership information, or the business register, or another central register. Member States may decide that obliged entities are responsible for filling in the register. Member States should make sure that in all cases that information is made available to competent authorities and FIUs and is provided to obliged entities when the latter take customer due diligence measures'

The EU FIU Platform report notes that EU FIUs' capacity to access information on beneficial ownership means only a few EU FIUs can obtain this information and that the obligation to set up central registers for this purpose has not yet been fulfilled in all Member States.[60]

On the other hand, the report underlines that company registers with information on legal entities (including their legal ownership) appear to be widespread and generally available to EU FIUs.[61] The report specifies that the information available varies greatly across the Member States, from a legal address, collection of registered members, public annual reports, and financial statements, to information on bank accounts for the registration of a company. Furthermore, the report notes that a few EU FIUs cannot obtain information on the legal ownership of companies.

Despite an absence of central databases across the EU on beneficial ownership to date, the report notes that some FIUs are finding information on beneficial owners using other sources of information, such as information held by notaries (in Member States that have a notarial system for setting up companies), or additional information found in databases of account holders database. However, according to the report, these 'decentralised' means for obtaining information on beneficial owners are only useful if the FIU already knows where the relevant individual or entity holds a business relationship. However, it is not optimal if FIU is seeking information to determine if an individual holds beneficial ownership positions, what the interested entities or legal arrangements are, and the characteristics of beneficial ownership itself.

In addition, and as regards a database on account holders, it should be noted that such databases are not found in all Member States. According to the fourth AML Directive, Member States are encouraged to put banking registries or electronic data retrieval systems in place which would provide FIUs with access to information on bank accounts. However, this is not mandatory. This lack of dedicated centralised national databases is an area of concern in many EU FIUs.[62]

---

[60] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information*, op.cit., p.94-97.
[61] Ibid., p.95.
[62] See: *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information,* op.cit., p.232-233. It should be noted that the proposal for amendments currently under discussion include to require Member States to set up automated centralised mechanisms enabling to swiftly identify holders of bank and payment accounts. See: Proposal for a Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of

This lack of information at national level is supplemented by difficulties in obtaining beneficial ownership information on legal persons and arrangements established in another country. As reported in our comparative analysis (Part II), financial investigations often require additional information on beneficial owners which may be available in another jurisdiction: without access to such information, it is not possible to match financial traces against an identity. The comparative analysis specifically mentions testimonies from Canadian authorities, who encounter many difficulties in identifying beneficial owners of Canadian companies owned by entities established abroad, particularly in the Caribbean, Middle East, and Asia. Also, in a number of investigations where Canadian companies were owned by foreign entities or foreign trusts, law enforcement agencies could not identify the beneficial owners.[63]

As regard trusts, access to information by FIUs appears even thinner. The EU FIU Platform report indicates that, during the survey carried out for the purpose of the report, no reference was found to access to information on trusts or similar arrangements. The report furthermore notes that in at least one Member State, trusts are not even recognised in the national legal system.[64]

3.3. Tax-related cases as an obstacle for European and international cooperation

Since the early 1990s, the scope of FIUs' work has largely been extended. As underlined in our comparative analysis (Part II), successive AML Directives have decoupled the list of predicate offenses from an exclusive focus on drug money, to include an ever broader range of offenses, including the explicit reference to tax crimes in the fourth AML Directive adopted in 2015.

As regards EU FIUs' cooperation in relation to tax crimes, the fourth AML Directive explicitly indicates that 'differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law' (Article 57). However, as suggested in the report prepared for the EU FIU Platform, this provision is often difficult to apply, since cooperation can be refused on the grounds of significant differences across Member States on how predicated offences to money laundering are defined and criminalised.[65] As noted in the report, 'exchange of information can indeed be refused when a possible predicate offence related to the case for which cooperation is sought is not criminalised (or not criminalised in the same form) in the country of the requested FIU'. The report furthermore notes that this limitation very often concerns tax matters

money laundering or terrorist financing and amending Directive 2009/101/EC, Strasbourg, 5 July 2016, COM(2016) 450 final.

[63] See our comparative analysis (Part II): Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom*.

[64] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information*, op.cit., p.96, see footnote 97.

[65] *Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information*, op.cit., p.158-159.

and also affects the potential efficiency of new requirements introduced by the fourth AML Directive, especially regarding cross-border suspicious transactions reports (STRs).

Indeed, Article 53(1) of the Directive provides that, besides the provision of information on request from other FIUs or spontaneously, EU FIUs are now obliged to 'promptly forward' every suspicious transaction report (STR) 'which concerns another Member State' to the interested FIUs. On that matter the EU FIU Platform report notes that 'due to domestic restrictions, bank and financial information contained in cross-border STR cannot be shared in some cases. (...) Also due to general domestic restrictions to information-sharing, some FIUs are prevented from forwarding cross-border STRs connected to tax matters or involving tax information'.[66] The report ultimately concludes that 'given that tax offences are recurring predicate crimes in significant money laundering cases across EU Member States, the 'fiscal excuse' should not be allowed as a derogation to FIUs' cooperation obligations.[67] On this matter, the report recalls that the FATF standards' interpretive note to Recommendation 40 explicitly prohibits refusals to provide assistance 'on the grounds that (…) the request is also considered to involve fiscal matters'.[68] As an addition, and as noted in our comparative analysis (Part II), if spontaneous dissemination of STRs is encouraged in European and international standards, it is far from being the norm in practice.[69] The EU FIU platform is currently undertaking a project to develop a common approach at EU level on dispatching of cross-border STRs.

It is worth noting that, as regards the proposed enhancements to the current EU AML framework, the European Commission's proposal of July 2016 does not provide for new predicate offences. However, the Commission issued a roadmap on the criminalisation of money laundering in October 2016, in which it advocates the adoption of a specific Directive, thus aiming at enhancing harmonisation at EU level of the definition of money laundering and its predicate offences and at bridging enforcement gaps and obstacles to information exchange and cooperation between the competent authorities in different countries. A proposal for a Directive was submitted in December 2016.[70]

[66] Ibid., p.173.
[67] Ibidem, p.197.
[68] FATF, Recommendations, 2012 (updated in 2016), p.107.
[69] See our comparative analysis (Part II): Amicelle A., Berg J. and Chaudieu K., *Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom* (Section 2.2).
[70] Proposal for a Directive on countering money laundering by criminal law, Brussels, 21 December 2016 COM(2016) 826 final.

3.4. Assessing the change of professional cultures

An overarching challenge when considering FIUs and their capacity to tackle tax-related crimes is the professional culture surrounding financial intelligence and investigation. As regards EU FIUs' staff backgrounds, the ECOLEF study reported that most FIUs employ a wide array of staff, including academics, lawyers, economists, financial analysts, police officers, prosecutors, international relations officers, customs, tax officers and more.[71] As mentioned in relation to the cooperation between FIUs and tax authorities (see section 3.1), it is key to ensure that both FIU staff and tax officers properly identify elements related to tax-related crime and therefore receive adequate training.

As indicated in a previous EPRS report on organised crime, training for law enforcement officials in the field of AML at the EU level has considerably improved,[72] however, the inclusion of aspects related to tax crimes is rather new, as previously underlined. Various initiatives have been taken in the field of financial intelligence and financial investigation, such as the OECD International Academy for Tax Crime Investigation.[73] At EU level, the European Police College (CEPOL) is beginning to organise dedicated training in this field,[74] and the creation of a 'European College of Financial Investigations and analysis of Financial Crimes – CEIFAC'[75] suggests a step in the direction of an increasing inclusion of tax-related matters in intelligence and law enforcement activities.

In parallel, more collaboration between FIUs and reporting entities is needed to support a change of culture that would take full account of tax-related crimes. As indicated in the ECOLEF study, the close relationship between FIUs and the reporting entities from which they receive STRs is key to ensuring an efficient partnership. The study outlined the various forms of feedback from FIUs to these entities,[76] and noted that although formal contacts between FIUs and reporting entities are in place in all countries, the nature of feedback given to the reporting entities varies considerably, from sending a general annual report to giving individual feedback. Some EU FIUs provide training sessions to reporting entities, but their number varies greatly across Member States and in some Member States, no training was provided.

Further and consistent collaboration between FIUs and reporting entities is thus key to engage reporting entities in the fight against money laundering in general, and tax-related crimes in particular.

[71] ECOLEF Study, op.cit., p.148.
[72] See: Annex 1 in: van Ballegooij W. and Zandstra T., *The Cost of Non-Europe in the area of Organised Crime and Corruption*, op.cit.
[73] OECD International Academy for Tax Crime Investigation.
[74] For an illustration, this webpage announces a specific training on financial investigations.
[75] The CEIFAC was established in 2013 in Strasbourg in the context of the European Commission programme 'Prevention and fight against crime' (DG Home Affairs – Action Grant 2012- FINEC Financial and economic crime).
[76] ECOLEF Study, op.cit., p.161

Part II: Comparative analysis of Financial Intelligence Units (FIUs) in Canada, France, Switzerland and United Kingdom

AUTHORS:

Dr Anthony Amicelle (International Centre for Comparative Criminology, Université de Montréal, Quebec, Canada), with Julien Berg (École de Criminologie, Université de Montréal) and Killian Chaudieu (École des sciences criminelles, Université de Lausanne, Switzerland)

LINGUISTIC VERSIONS
Original: EN

Manuscript completed in March 2017
Brussels © European Union, 2017.

Executive summary

This briefing note provides the PANA Committee with background information concerning the everyday practices of national financial intelligences units (FIUs) to combat money laundering and terrorist financing, with a focus on their capacity to tackle tax crimes. The study looks at the differences between FIUs as well as the tensions and difficulties involved in developing international cooperation between them. It is based on **a comparative analysis of the designated FIUs in the following countries: France, UK,** Canada and Switzerland. The note has two main sections.

The first section underlines the ongoing redefinition of both 'dirty money' and FIUs identity. On one hand, it recalls that the scope of the notion of 'dirty money' has been radically extended from the proceeds of drug trafficking to illicit flows of money in general, including, after years of explicit exclusion, tax evasion. **The striking definitional malleability of 'dirty money' has largely transformed financial intelligence practices**, starting with a focus on both the origin and destination of money. Reporting entities' obligations and FIUs' powers have continued to increase significantly in the period considered here. The tremendous development of financial intelligence capabilities has been justified largely in the name of counter-terrorism, particularly in the EU following the adoption of the second Anti-Money Laundering Directive in December 2001. This prioritization of terrorist financing is very often associated with an increased effort in the fight against financial crime as a whole. However, our fieldwork found much more mitigated results with regard to 'mutual benefits' from terrorist financing to tax evasion. There are concerns that the effort to deal with terrorism is to focus on a tree and ignore the wood. On the other hand, the first section also examines key differences between countries with regard to the three core functions of FIUs (information collection, analysis, and dissemination). FIUs officials no longer define their units as exclusively anti-money laundering agencies, as was the case in the early years of their emergence. They define themselves largely as **specialised intelligence services that have become multi-taskers even if the wider question of FIU identity remains a matter of debate between and within FIUs.** This transformation in FIU identity does not eliminate the differences in the ways FIUs operate – far from it. Nevertheless, the main differences are not where they might be expected to be. This study emphasises that the classic typology of FIUs ('judicial model'; 'law-enforcement model'; 'administrative model'; 'hybrid model') is not sufficient to identify the key operational differences between FIUs. Moreover, it masks numerous critical elements that make a difference in practice, including those between FIUs that fall into the same model. It gives the mistaken impression that every question relates to status problems. On the contrary, we argue that being grouped into the same model often means very little in practice with regard to the three core functions of FIUs.

With regard to the first core function (information collection), the four FIUs we analysed do not receive the same disclosures of financial transactions from reporting entities, a variation that has nothing to do with the classic typology. **With reference to the second core function (information analysis)**, there are at least two critical issues at stake. First, another typology is needed that differentiates between FIUs depending on whether or not they have a national monopoly on analysing the financial transaction reports they collect. Second, the other critical difference between FIUs relates to the

ability to get direct and/or indirect access to other state databases. Which databases can an FIU access as part of its analytical activities? Here, the classic typology masks major disparities between FIUs in the same model. Third, **with reference to the third core function (analyses/financial intelligence dissemination)**, there is almost a difference in kind between countries where FIU dissemination is directed towards prosecution authorities and countries where FIU dissemination of financial intelligence goes well beyond prosecution authorities, including tax administration, intelligence services and social protection institutions.

Finally, this section shows that **the challenge of suspicious transaction reports still lies in knowing where to draw the line between defensive reporting and intelligence-relevant reporting.** Depending on the national context, defensive reporting from obliged entities (mainly financial institutions) may result either in over-reporting – creating more 'noise' than actionable intelligence for law enforcement – or under-reporting – reporting only when there is no other choice to avoid sanctions because the client is already being prosecuted or has been the subject of scandal-driven media coverage. Moreover, the prevalence of interpretation over facts is, inevitably, an unavoidable element in the rationale at the core of any suspicion-based model of denunciation. To the extent that they are not based on any clear-cut threshold, suspicious transaction reports *de facto* introduce a significant margin of interpretation. Along these lines, 'suspicion' is at the heart of financial intelligence practices but it is not interpreted the same way from one country to another (from 'unqualified suspicion' to 'well-founded suspicion').

The second section **sheds light on the cooperation channels the FIUs use, at European and International level**. On one hand, international cooperation between financial intelligence units is promoted as a way to prevent the internationalisation of financial flows from being used to make it more difficult to discern criminal activity. In practice, different types of situations encourage FIUs to cooperate with foreign counterparts. Regardless of the motive for requesting information, the FIUs use from one to three cooperation channels depending on geographic location, legal framework, and technical capacity:

1) **The Egmont Secure Web (ESW):** 152 national FIUs can make and respond to requests via the ESW, which is promoted as the international FIU-to-FIU channel of communication.
2) **The FIU.NET:** It is restricted to EU Member States only, with potential extension to other European countries such as Iceland and Norway in the near future.
3) **Other recognised cooperation channels:** FIUs also use other channels – secure e-mails or even fax messages – to exchange information with the minority of their counterparts that are neither members of the Egmont Group nor FIU.NET.

Although cooperation channels such as the ESW and the FIU.NET are based on the same goal of information sharing between financial intelligence units, **the briefing note insists on a number of significant differences between them, from the technological side to the possibility of multilateral information exchange.**

On the other hand, **cooperation practices between FIUs regularly come under fire in relation to a series of obstacles**, including some that are particularly problematic in tax-related cases:

- General inability to request information from reporting entities
- Conditional (in)ability to obtain information from reporting entities
- Inability to get access to beneficial ownership information
- Lack of (access to) databases
- Timeliness issues and lack of reciprocity
- Lack of spontaneous dissemination and 'abusive' restriction on the use of information

Introduction

> 'Establishing an FIU is an important step in combating financial crime. […] In this connection, it is useful to note that one of the critical functions of an FIU is the exchange of information with other FIUs. In addition to the contribution the FIU can be expected to make in combating domestic crime, it will also be called upon to respond to requests for intelligence from other FIUs'.[77]

The first national agencies, today referred to as financial intelligence units (FIUs), were created in 1990, starting with the Financial Crimes Enforcement Network (Fincen) in the United States of America in April 1990. In the same year and month, 'the forty recommendations of the Financial Action Task Force [FATF] on money laundering' were issued, less than one year after the creation of the FATF by the G-7 summit in Paris.[78] The number of FIUs has now climbed to more than 150 and the FATF recommendations – revised four times (1996, 2001, 2003, and 2012) – are recognised as the global standard for dealing with money laundering and counter-terrorist financing in 194 jurisdictions, including the EU, which has adopted four directives (1991, 2001, 2005, and 2015) on the issue. One of the revised FATF recommendations states that 'countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis' *(R. 29)*.[79]

Despite the possible chicken-and-egg analogy, the overlap between national and international initiatives is sufficiently rare to be worthy of note, especially in the field of policing. The development and evolution of national FIUs and international norms regarding 'dirty money' have been closely related for the last twenty-seven years. Both emerged in the early 1990s to track the money from drug trafficking and are now being promoted as a way to fight financial crime as a whole, from terrorist financing to tax evasion. According to the former director of the French FIU:

> 'The system that resulted in the creation of financial intelligence units, under the FATF auspices, has always been able to demonstrate its effectiveness and flexibility: initially designed for the fight against the financing of drug traffic, it has gradually been extended to the fight against all forms of illicit financial flows, and against terrorist financing. For several years, the economic and financial crisis has led to a new reflection on the need to strengthen regulatory instruments in the financial sector and it is likely that this reflection will lead to giving a stronger role to those original structures whose function of surveillance of financial flows has become an essential corollary of financial liberalisation'.[80]

[77] IMF, *Financial Intelligence Units: An Overview*, 2004.
[78] Financial Action Task Force (FATF), Recommendations, 1990.
[79] Financial Action Task Force (FATF), Recommendations, 2012.
[80] Tracfin, *Annual Report*, 2011, p. 3.

From 1990 to 2017, FIUs around the world have increased considerably not only in number but also in their sphere of action. Moreover, the original connection between FIUs and international activity took an operational turn as early as 1995 when a number of national agencies – then called 'financial disclosure units' - decided to create an informal forum and worldwide network to explore ways to cooperate: the Egmont Group. In a similar vein, information exchange between the FIUs has been a European objective since the second half of the 1990s, culminating in the Council decision of 17 October 2000 'concerning arrangements for cooperation between financial intelligence units of the member states in respect of exchanging information'.[81]

However, the 'historical' and multifaceted internationalisation of FIUs should not be overemphasized. On the normative side, an FIU is not a 'one size fits all' organisation, either at the international level or within the EU. On the operational side, transnational cooperation between FIUs is still a work-in-progress, which is regularly criticised.

This analysis looks at the differences between FIUs as well as the tensions and difficulties involved in developing transnational financial intelligence cooperation by analysing FIUs in Canada (established 2001; approximately 350 staff; annual budget: approximately 55 million Canadian dollars), France (established 1990; approximately 150 staff; annual budget: approximately 6 million euros), Switzerland (established 1998; approximately 20 staff; annual budget: approximately CHF 3 million), and UK (established 1992; approximately 150 staff; annual budget: n/a). It also assesses the cooperation channels used by these FIUs both within Europe and at the international level. This comparative analysis of two FIUs from the EU, one non-EU FIU from a European country with a major financial centre, and one North American FIU is intended to provide a better understanding of the current situation in relation to the role, powers, and activities of FIUs in fighting financial crime in general and tax crime in particular.

The analysis relies both on qualitative and quantitative data. The study draws on document analysis (official reports and statistics from the Egmont Group, the European Union, the FATF and FIUs under examination) and semi-structured interviews with officials from FIUs and Europol. The research team interviewed four officials from the Financial Transactions and Reports Analysis Centre (Fintrac) in Canada, three officials and one former official from *Traitement du renseignement et action contre les circuits financiers clandestins* (Tracfin) in France, one official from the Money Laundering Reporting Office (MROS) in Switzerland, and one official from the European Police Office (Europol). The input of the UK FIU has been gathered through document analysis and in light of a former fieldwork including interviews with UK officials. Recent fieldwork by the research team in these four countries is also used to complement the analysis.[82]

[81] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.
[82] Amicelle A., 'Towards a 'New' Political Anatomy of Financial Surveillance', *Security Dialogue*, Vol 42, No 2, 2011, p. 161-178; Amicelle A. and Favarel-Garrigues G., 'Financial Surveillance: Who Cares?', *Journal of Cultural Economy*, Vol. 5, No 1, 2012, pp. 105-124 ; Amicelle A., 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism. From Criticism to Imitation of Dataveillance', *CEPS Liberty and Security Series*, No 56, 2013, pp. 1-19 ; Amicelle A., 'Differential

The analysis has two main sections. The first section shows how the fight against 'dirty money' has evolved since the early 1990s and examines key differences between countries with regard to the three core functions of FIUs (information collection, analysis, and dissemination). The second section focuses on cooperation channels between FIUs and the main tensions in transnational information exchange about financial flows.

1. National financial intelligence units in practice

1.1. 'FININT' – the evolution of priorities

Twenty-seven years after the first EU Directive on money laundering, the abbreviation FININT (financial intelligence) is now commonly included in the myriad of acronyms used to distinguish various sources and kinds of intelligence.[83] National authorities – financial intelligence units (FIUs) – have been created to deal with this specific form of intelligence. While the first and second European Directives made only a general reference to national 'authorities responsible for combating money laundering', the third European Directive made explicit that 'each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing'.[84] This incremental clarification at the European level mirrors the semantic revision of international standards, from 'competent authorities' in 1990 to 'financial intelligence unit' since 2003.[85] The latest – fourth – Directive states: 'all Member States have, or should, set up operationally independent and autonomous FIUs to **collect** and **analyse** the information which they **receive** with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. […] Suspicious transactions and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIU, which should serve as **a central national unit for receiving, analysing and**

Management of Economic and Financial Illegalisms : Anti-Money Laundering and Tax Issues', *Penal field*, Vol 10, 2014, pp. 1-23 ; Amicelle A., 'Management of Tax Transgressions in France: a Foucauldian perspective', In J. van Herp, W. Huisman and G. Vande Walle (eds.), *The Routledge Handbook of White-Collar and Corporate Crime in Europe*, London, Routledge, 2015, pp. 379-398 ; Amicelle A. and Jacobsen K.U., E., 'The Cross-Colonization of Finance and Security through Lists: Banking Policing in the UK and India', *Environment and Planning D: Society and Space*, Vol 34, No 1, pp. 89-106. Amicelle A., *Suspicion in the Making: Everyday Policing against Money Laundering and Terrorist Financing in Canada*, TSAS report, forthcoming.

[83] HUMINT (*Human Intelligence*) ; TECHINT (*Technical Intelligence*) ; IMINT (*Imagery Intelligence*); COMINT (*Communications Intelligence*); TELINT (*Telemetry Intelligence*); ELINT (*Electronic Intelligence*); RADINT (*Radar Intelligence); SIGINT (Signals Intelligence); MASINT (Measurement and Signature Intelligence) ; FISINT (Foreign Instrumentation Signals Intelligence) ; OSINT (Open Source Intelligence); GEOINT (Geospatial Intelligence); SOCMINT (Social Media Intelligence).*

[84] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering; Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering; Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[85] Financial Action Task Force (FATF), Recommendations, 1990; Financial Action Task Force (FATF), Recommendations, 1996; Financial Action Task Force (FATF), Recommendations, 2003; Financial Action Task Force (FATF), Recommendations, 2012.

disseminating to the competent authorities the results of its analyses'.[86] Although the first European FIUs were established as early as in 1990 – Tracfin in France for example – they already dealt with the three 'core functions' of FIUs described in the fourth Directive. In accordance with international standards, FIUs' core functions consist in receiving, analysing, and disseminating financial-related information to deal with 'flows of illicit money',[87] widely known as 'dirty money'.[88]

From this perspective, the 'identity' of financial intelligence units seems to have been stable over time and harmonised throughout the EU as well as at the international level. However, the exclusive and formal focus on 'core functions' hides both the radical evolution of FIUs over the years and the wide range of differences between them.

The (re)definition of dirty money

First, the scope of the work of FIUs has been extended, if not transformed, by the near permanent renegotiation of the perimeter of the fight against 'dirty money', from various forms of money laundering to terrorist financing. On one hand, money laundering can be characterised as a 'dependent offence' as it depends on the existence of a predicate – prior – offence, from which money is being laundered. The list of predicate offences on the basis of which financial intelligence is deployed is therefore critical to understanding the contours of 'dirty money' and the role of FIUs. The first European Directive 'defined money laundering in terms of drugs offences'.[89] However, the list of predicate offences has been decoupled from an exclusive focus on drug money to include an ever broader range of offences and, in the fourth European Directive, explicit reference to tax crimes. This recent translation of tax crimes into predicate offences for money laundering is more than another step in extending the field of financial intelligence: it is a major change as **tax issues were explicitly excluded from the international standards against money laundering in the Financial Action Task Force (FATF) recommendations**[90].

The historical exclusion of tax issues has often been interpreted as selective tolerance for white-collar crime.[91] It derived in part from the hostility of some FATF founding member states, such as Luxembourg and Switzerland, toward consideration of tax issues. The lack of consensus on this topic was also apparent in both financial and law enforcement circles

[86] Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
[87] Ibid.
[88] Directive 91/308/EEC, op.cit. ; Directive 2001/97/EC, op.cit. ; Directive 2005/60/EC, op.cit.
[89] Directive 2015/849, op.cit.
[90] 'As regards the scope of its work, while the laundering of drug money will remain a principal focus for the FATF, its work will continue to cover money laundering of the proceeds of serious crime and/or offences which generate significant funds. However, as in the past, the FATF will not deal with tax issues' (Financial Action Task Force (FATF), Annual Report, 1994, p. 6).
[91] Favarel-Garrigues G., 'Domestic reformulation of the moral issues at stake in the drive against money laundering : the case of Russia', International Social Science Journal, Vol 57, No 185, 2005, pp. 529-540 ; Helleiner E., 'State Power and the Regulation of Illicit Activity in Global Finance', In Andreas P., Friman R. (eds.), *The Illicit Global Economy and State Power*, Lanham Md, Rowman and Littlefield, 1999, pp. 53-89 ; Strange, S., *Mad Money*, Manchester, Manchester University Press, 1998.

but for different reasons.[92] The first extension of money laundering beyond the proceeds of drug trafficking was intended to tackle the same broad category of criminal groups, leaving tax-related white-collar criminals largely untouched.

> 'In addition, drug organisations often engage in other criminal conduct that produces proceeds to be laundered. In these cases, it is often difficult to prove a direct link between the money launderer and the narcotics-related offences. Therefore, in criminalising money laundering, other formulations to criminalise non narcotic-based money laundering offences are preferable to requiring proof that the underlying offence be narcotics related or linked to narcotics. Countries should consider extending the offence of drug money laundering to all serious offences and/or all offences that generate a significant amount of proceeds on a wide range of enumerated serious offences'.[93]

In its beginnings in 1992, decoupling money laundering from drug money was presented as necessary to make it possible to intensify the financial intelligence effort against criminal organisations in which drug-trafficking was just one of many activities. Extending the perimeter of anti-money laundering was thus based on strategic considerations intended to target the same broad category of 'organised crime' rather than as a means to include more legitimate social, economic, and political actors through their relation to tax crimes.

The third European Directive in 2005 challenged this rationale to some extent. The Directive did not mention tax evasion but included 'serious offences' defined as: 'all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months'.[94] In numerous Member States, most tax-related offences fell within this set of criteria, but countries were not uniformly affected and the inclusion of tax issues within the perimeter of 'dirty money' remained largely indirect and implicit. The major change was formally initiated in the aftermath of the 2008 international financial crisis.

> 'In relation to the crisis, I would like to say that at the last FATF meeting this group agreed to examine a number of issues, particularly, for instance, the issue of bank secrecy laws, and also to consider the merits and difficulties of considering tax crimes (people meant tax evasion) as a predicate offence to money laundering. These certainly reflect the language of the expectations of the G20. In this respect the global financial crisis is already influencing the thought processes of the FATF and the [European] Commission is contributing to this'.[95]

---

[92] For further details, see Amicelle A. 'Differential Management of Economic and Financial Illegalisms', op.cit.
[93] Financial Action Task Force (FATF), Annual Report, 1992, p. 35.
[94] Directive 2005/60/EC, op.cit.
[95] House of Lords. European Union Committee. 19th Report of Session 2008-09: Money laundering and the financing of terrorism. Volume II : Evidence, London, The Stationery Office, 2009, p. 138.

This declaration was made by an EU official a few days before the G20 summit in London where the leader of the Group of Twenty put an emphasis on tax havens and ending bank secrecy. These 'thought processes' ended with the official inclusion of tax crimes in the revised version of the FATF recommendations in 2012 and in the fourth European directive in 2015.

This change is critical for FIUs. Making tax crime a predicate offence for money laundering has been presented as constituting the end of selective tolerance for specific illegalities committed by persons of 'respectability and high social status'. It also contributes to further modifying the previous logic of financial intelligence, which had consisted in following the (illicit) origin of money. **Tax crimes cover all mechanisms that disguise either the existence (by keeping it in cash) or nature (by attempting to make it appear in a category or place where it will be subject to little or no taxation) of legally obtained revenue**.[96] In this case, in contrast to the proceeds of drug trafficking, it is not the origin of money that is illicit *per se* but instead the attempt to avoid taxes that is illegal. **As a result, the inclusion of tax crimes implies that financial intelligence efforts will need to focus not only on the origin of funds, which might be licit, but also on their destination.** This critical re-definition of the notion of dirty money to include financial flows with licit origin but illegal uses should be understood as a paradigm shift in financial intelligence. However, this critical (r)evolution in FININT, and by extension in financial intelligence units, did not wait for the inclusion of tax crimes: it was endorsed in 2001 through the association between money laundering and terrorist financing.

> 'The revolution for financial intelligence came in 2001 when we said, rather quickly but because we could not say anything else that the fight against the financing of terrorist activities falls within the scope of anti-money laundering system. At this point, we didn't know where we were going! Same thing regarding our work method and in terms of cooperation. What does it mean in terms of work method? All the attention was on the financial flows until then; trying to know where they came from, the origin! And then we said to the financial sector: 'wait – now you must look at where the money goes. Furthermore, you must look at where the money goes even if its origin is legal!' That's complicated! Saying this is a revolution for financial intelligence'.[97]

FIUs were initially focused on the origin of money and a single category of offender (drug traffickers and money-launderers for profits from drug trafficking) but are now presented as agencies that are vital to dealing with all natural and legal persons linked to money that is 'dirty' because of either its origin or its destination. **They were initially designed for the fight against the proceeds of drug trafficking but are now seen as the information hub to provide actionable financial intelligence against crime and terrorism at large**.

[96] Blum J., Levi M., Naylor R., Williams P., *Financial Havens, Banking Secrecy and Money Laundering*, United Nations Office for Drug Control and Crime Prevention, New York, 1998.
[97] Interview FIU, 2016.

The inclusion of terrorist financing in the European and international framework against money laundering has a tremendous impact on the work and the 'identity' of FIUs. Among the four FIUs analysed in this analysis, Canada, France, and UK give priority to pursuing terrorist financing while in Switzerland specific federal resources for countering terrorism and terrorist financing activities have been increased since 2015.[98] **What has been the effect of the prioritisation of terrorist financing in the fight against 'dirty money' and in the role of financial intelligence units? This question is a matter of debate in the field of financial intelligence**. For some, the primary focus on terrorism has created a new dynamic that provides a 'major leverage effect against financial crime as a whole'.[99] In this context, current national, European, and international action plans to strengthen the fight against terrorist financing should be highly beneficial for the fight against all forms of illicit financial flows, starting with tax crimes. Others, however, question this idea of general progress.

> 'The question of terrorism is the number one priority and there are many things, many legal developments, that will allow us to share more information on this topic. But in terms of money laundering, it is… it has lost its cachet … When cooperating at the international level with financial intelligence units on tax evasion versus terrorism, we are not in the same galaxy here, it is completely different, even with the same close foreign partners'.[100]

Some are concerned that the effort to deal with terrorism is to focus on a tree and ignore the wood.[101] They argue that FIUs should not be primarily counterterrorism tools at the expense of other missions. This debate questions the assertion that FIUs are now officially at the heart of a 'fight against all forms of illicit financial flows'.[102]

The (re)definition of FIU identity

Whether they share the first or the second interpretation of the impact of the focus on terrorism, FIUs officials all refuse to define their own units as exclusively anti-money laundering agencies, as was the case in the early years of their emergence.

> 'We go beyond money laundering. We say that we do financial intelligence and that is what we have always wanted to be, namely a real financial intelligence unit, not simply an anti-money laundering unit. There is a clear difference between the two'.[103]

[98] Fintrac, Annual Report, 2016; MROS, Annual Report, 2016; NCA, SARs Annual Report, 2015; Tracfin, Annual Report, 2016.
[99] Interview FIU, 2016.
[100] Interview FIU, 2016.
[101] Interview FIU, 2017.
[102] Tracfin, Annual Report, 2011.
[103] Interview FIU, 2016.

They define themselves largely as specialised intelligence services that have become multi-taskers even if the wider question of FIU identity remains a matter of debate between and within FIUs.

> 'I mean, are we a national security agency? Are we part of law enforcement? What community do we identify with most? National security? Law enforcement? There's talk, you know, the potential of, well, disclosing to security regulators takes us into another place, right?'[104]

Ultimately, the transformation in FIU identity does not eliminate the differences in the ways FIUs operate – far from it. Nevertheless, the main differences are not where they might be expected to be. 'In their simplest form, FIUs are agencies that **receive** reports of suspicious transactions from financial institutions and other persons and entities, **analyse** them, and **disseminate** the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money laundering'.[105] The IMF's highly influential 2004 report then insisted on 'variations' between FIUs. According to the authors, the fundamental distinctions relate to the legal nature of FIUs, which fall into four models: 1) 'the administrative-type FIU (Canada, France, and Switzerland); 2) the law-enforcement-type FIU (UK); 3) the judicial or prosecurial-type FIU; 4) the mixed or hybrid FIU.[106]

These four models of FIUs are currently mentioned by the Egmont Group as follows:

> 'The **Judicial Model** is established within the judicial branch of government wherein "disclosures" of suspicious financial activity are received by the investigative agencies of a country from its financial sector such that the judiciary powers can be brought into play e.g. seizing funds, freezing accounts, conducting interrogations, detaining people, conducting searches, etc.
>
> The **Law Enforcement Model** implements anti-money laundering measures alongside already existing law enforcement systems, supporting the efforts of multiple law enforcement or judicial authorities with concurrent or sometimes competing jurisdictional authority to investigate money laundering.
>
> The **Administrative Model** is a centralized, independent, administrative authority, which receives and processes information from the financial sector and transmits disclosures to judicial or law enforcement authorities for prosecution. It functions as a "buffer" between the financial and the law enforcement communities.

[104] Interview FIU, 2016.
[105] IMF Report, op.cit.
[106] Ibid., 9-17 ; for an earlier but rather similar classification, see also Mitsilegas V., 'New Forms of Transnational Policing : The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights', *Journal of Money Laundering Control*, Vol 3, No 2, 1999, pp.147-160 and Vol 3, No 3, 2000, pp. 250-259.

> The **Hybrid Model** serves as a disclosure intermediary and a link to both judicial and law enforcement authorities. It combines elements of at least two of the FIU models'.[107]

The IMF classification has been largely used to shed light on key differences when assessing the comparative advantages and disadvantages between FIUs. For instance, it is regularly stressed that there is an information gap between law-enforcement and judicial FIUs on the one hand, and administrative and hybrid FIUs on the other. In the EU, for example, law-enforcement and judicial FIUs, on average, have better access to national police and judicial data.[108] **Our fieldwork suggests, however, that the classic typology is not sufficient to identify the key operational differences between FIUs.** Moreover, it masks numerous critical elements that make a difference in practice, including those between FIUs that fall into the same category on the model. It gives the mistaken impression that every question relates to status problems. On the contrary, **we argue that being grouped into the same category – like Canada, France, and Switzerland, which are all in the administrative group – often means very little in practice with regard to the three core functions of FIUs**. The main issue is not a matter of status as defined by the IMF typology. There is no one-size-fits-all solution in terms of models – there are major differences between FIUs in the same category while 'administrative FIUs', such as France's Tracfin, Canada's Fintrac, and Switzerland's MROS, sometimes have better access to police and intelligence databases than some law-enforcement FIUs.

With regard to the first core function (information collection), the four FIUs we analysed do not receive the same disclosures of financial transactions from reporting entities, a variation that has nothing to do with the IMF typology. **The reporting of suspicious transactions is at the heart of financial intelligence in the four countries (with slight differences) but FIUs in Canada and France also rely on other reporting obligations, based largely on monetary thresholds.** In other words, their reporting model is not based only on suspicion regarding crime. France's FIU (Tracfin) receives two forms of 'systematic communication of information' (*communications systématiques d'informations* – COSI). Since October 2013, credit institutions, payment institutions, and electronic money institutions have had to report information about money transfers, either cash or electronic currency, that total 1,000 euros or more per transaction or 2,000 euros or more per client per month. Since January 2016, the same institutions, in the name of counter-terrorism, also have to report money transfers and cash withdrawals totalling 10,000 euros or more per client per month.

The Financial Transactions and Reports Analysis Centre of Canada (Fintrac) also collects (1) 'electronic funds transfer reports', (2) 'terrorist property reports', (3) 'large cash transaction reports', and (4) 'casino disbursement reports'[109]. To what extent do the

[107] Egmont Group of FIUs, Financial Intelligence Units, 2017.
[108] Project 'Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy - ECOLEF' (funded by the European Commission - DG Home Affairs, JLS/2009/ISEC/AG/087), Final Report, February 2013.
[109] Available on the Fintrac website

monetary threshold–based reports constitute an added-value for financial intelligence in general and the fight against money laundering of tax evasion? Canada's authorities promote them as critical tools against tax evasion and aggressive tax avoidance. Since 2015, financial institutions have been required to also send their 'electronic funds transfer reports' of 10,000 Canadian dollars or more to the Canada Revenue Agency (CRA) rather than only to Fintrac. According to CRA representatives, this information helps their agency 'to identify taxpayers who may be participating in aggressive tax avoidance or who may be attempting to conceal income and assets offshore'.[110] The impact of this new measure in Canada and the potential use of threshold-based reports on financial crimes deserves further analysis.

With reference to the second core function (information analysis), there are at least two critical issues at stake. First, a typology is needed that **differentiates between FIUs depending on whether they have a national monopoly on analysing the financial transaction reports they collect.** Such an analytical monopoly is not found in FIUs that provide direct access to their database to various law-enforcement and intelligence partners, as is the case in the UK. Table 1 gives the list of 'end users with direct access' to the UK FIU database from the UK FIU 2015 annual report[111]:

[110] Canada Revenue Agency (CRA), Cracking down on tax evasion and avoidance, 2016.
[111] National Crime Agency (NCA), SARs Annual Report 2015, op.cit.

Table 2 End-users with direct access to the UK FIU database

Police forces		Multi agency teams and other agencies
Avon and Somerset	Merseyside	Eastern Regional Asset Recovery Team (RART)
Bedfordshire	Metropolitan Police Service	East Midlands RART
British Transport Police	Ministry of Defence Police	London RART
Cambridgeshire	Norfolk	North East RART
Cheshire	Northamptonshire	North West RART
City of London	Northumbria	South East RART
Cleveland	North Wales	South West RART
Cumbria	North Yorkshire	Wales RART
Derbyshire	Nottinghamshire	West Midlands RART
Devon and Cornwall	Police Scotland	Crown Office, Civil Recovery Unit, Scotland
Dorset	Police Service of Northern Ireland	Department for Business, Innovation and Skills
Durham	South Wales	Department for Environment, Food and Rural Affairs
Dyfed-Powys	South Yorkshire	Department for Work and Pensions
Essex	Staffordshire	Environment Agency
Gloucestershire	Suffolk	Financial Conduct Authority
Greater Manchester	Surrey	Gambling Commission
Gwent	Sussex	HM Revenue and Customs
Hampshire	Thames Valley	Home Office
Hertfordshire	Warwickshire	National Crime Agency
Humberside	West Mercia	National Port Analysis Centre
Kent	West Midlands	NHS Protect
Lancashire	West Yorkshire	Northern Ireland Department for Social Development
Leicestershire	Wiltshire	Northern Ireland Environment Agency
Lincolnshire		Serious Fraud Office

The UK FIU still acts as the central national unit for analysing information sent by reporting entities but, in contrast to Canada, France, and Switzerland, numerous UK FIU partners do not depend on FIU analysis in order to get access to the reported information. In this respect, the UK FIU can be seen as a simple (financial) data repository for law enforcement purposes. This situation is neither a common feature of nor specific to IMF law-enforcement/police-type FIUs, such as the UK financial intelligence unit. The US FIU (Fincen) database is directly accessible and searchable by a range of end users although Fincen falls within the IMF category of administrative-type FIUs. A major distinction thus emerges between the data repository model of an FIU – which collects and makes financial transaction reports directly available - and the analysis model of FIU – which never provides access to its database. While the comparative impact of each model on dealing with financial crimes deserves further systematic analysis, the choice of one model over the other suggests a fundamental difference between FIUs.

Second, the other critical difference between the FIUs we analysed relates to **the ability to get direct and/or indirect access to other state databases. Which databases can an FIU**

access as part of its analytical activities? Here, the famous IMF typology masks major disparities between FIUs in the same category. For instance, an IMF administrative-type FIU, such as in Italy, has no access to police and social security data bases and only indirect access to tax data[112], while France's FIU (Tracfin) has direct access to all of these. France's FIU has direct access to the national central register for all holders of bank accounts (*fichier des comptes bancaires ou assimilés* – FICOBA[113]) and to social data as well as direct or indirect access to databases from customs services, tax administration, and police/gendarmerie, including access to judicial records (records of criminal conviction) and the wanted person file. With regard to indirect access, Tracfin officials can generally obtain the desired information upon request to the database owner. In the name of counter-terrorism, Tracfin officials can also request information from other official members of the French 'intelligence community' (e.g. *direction générale de la sécurité extérieure*/General Directorate for External Security (DGSE) ; *direction de la protection et de la sécurité de la défense*/Directorate of Protection and Security of Defense (DPSD) ; direction du renseignement militaire/*Directorate of Military Intelligence* (DRM) ; *direction générale de la sécurité intérieure*/General Directorate of Internal Security (DGSI) ; *direction nationale du renseignement et des enquêtes douanières*/National Directorate of the Intelligence and Customs Investigations (DNRED). Despite some differences, the two other administrative-type FIUs studied (Canada and Switzerland) also challenge the mistaken assumption that administrative-type FIUs have systematically limited access to law-enforcement data.

In Switzerland, the MROS has access to a range of administrative, police, and judicial databases, including the data from the Swiss commercial register, the automated register of vehicles and vehicle owners, the automated register of driving licences, the police computerised research system, the federal police's computerised files and persons management and indexing system, the federal criminal police's computerised system, the computerised criminal records database, the federal Office of Justice's persons, files, and cases management system (which provides international legal assistance in criminal matters), and the general information and analysis system (a secure central system for the input, processing, and analysis of intelligence data).[114]

In Canada, Fintrac has access to a range of law-enforcement databases, including the Canadian police information centre, the Public Safety Portal, the Canada Border Services Agency's cross-border currency reports and seizure reports databases, the Royal Canadian Mounted Police's national security system, the Sûreté du Québec's criminal information, and the Canada Anti-Fraud Centre and the Canadian Security Intelligence Service's databases.[115] Paradoxically, as an administrative-type FIU, Fintrac is sometimes criticised for 'insufficient access to the information collected and/or maintained by – or on behalf of – administrative and other authorities, such as CRA [Canada Revenue

[112] ECOLEF Study, op.cit.
[113] Approximately ten European Member States have a central register for all holders of bank accounts.
[114] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016.
[115] Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, 2016.

Agency] databases'.[116] It is beyond the scope of this exploratory report to examine the effect of differential access to databases, but it is worth noting that such access varies substantially from one FIU to another within a single type of FIU.

The processing of suspicious transactions reports (STRs) also varies from one country to another. In Switzerland, every report (2,367 last year) is analysed within a matter of days to assess the 'quality' of the level of suspicion in order to determine whether the report should be sent to prosecution authorities. In France, suspicious transactions reports (43,266 in 2015) follow a four-step process: 1) integration, 2) orientation, 3) analysis, 4) dissemination. The second and third steps are critical for information analysis. Step 2 consists in filtering each STR according to a multi-criteria orientation manual to decide whether or not it should go to step 3 for in-depth analysis. The orientation manual, which is confidential, relies on criteria such as financial thresholds, typologies, information quality, investigation priorities and so on. Each dedicated Tracfin analyst examines from 15 to 30 STRs per day at step 2 in order to decide either to put the STR on hold in the database, to start a pre-investigation, or to send the STR to the Tracfin investigation unit for an in-depth analysis. Information analysis thus depends on an internal prioritization process. A rather similar logic is applied in Canada in connection with Fintrac national partners' prioritisation process to the extent that 'Fintrac tailors its analysis to the law enforcement agencies' priorities'.[117]

Finally, **with reference to the third core function (analyses/financial intelligence dissemination)**, there is almost a difference in kind between the Swiss administrative-type FIU and the Canadian one. In Switzerland, dissemination is directed towards prosecution authorities, on both the federal and cantonal level, as the FIU is seen as a part of justice system, with 1,635 disclosures to prosecution authorities in 2015. In Canada, dissemination of financial intelligence goes well beyond prosecution authorities. As an example, in 2015, 1,655 Fintrac case disclosures were sent to the Royal Canadian Mounted Police (976), municipal police (582), Canada Security Intelligence Service (429), foreign financial intelligence units (384), provincial police (303), Canada Border Services Agency (225), Canada Revenue Agency (205), provincial securities regulators (69), and the Communications Security Establishment (47)[118]. The Swiss and Canadian dissemination frameworks are thus very different, a difference that has been stable over time while the French orientation has evolved radically, from an original focus on justice, as in Switzerland, to a progressive extension to non-judicial partners, as in Canada:

> 'Yes, it was only justice for a long time, until 2008–2010. In 2010, we were told: 'you also fight against tax evasion' and justice administration does not deal with tax evasion, except for particular procedures. Consequently, we had to send information to tax administration. In 2012, we were told: 'you also have to contribute to the fight against social fraud'. Finally, in 2008 we were designated as

[116] Ibid., p. 184.
[117] Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, op.cit., p. 43.
[118] The total number of disclosures per partner is higher than 1,655 because a case disclosure may be sent to several partners.

> an intelligence service and were told: 'You must cooperate with other intelligence services".[119]

In 2008, 74 per cent of France's FIU (Tracfin) dissemination effort was directed toward judicial authorities – 359 disclosures as compared to 93 disclosures to Customs and 35 disclosures to the judicial police.[120] By contrast, in 2015 Tracfin officials sent a total of 1,675 disclosures, 448 of them to judicial officials. The top 3 non-judicial recipients were tax administration (410), intelligence services (349), and social protection institutions (109).[121]

Only a part of received suspicious transactions reports (STRs) – the number depending on the particular FIU (up to 70 per cent in Switzerland) – are ultimately disclosed to national partners; a single disclosure may include from one STR to thousands, depending on case and country. A significant distinction is between reactive and proactive disclosures. Reactive disclosures are made in response to an explicit request by a national partner, while proactive disclosures are made spontaneously by an FIU. The vast majority of disclosures in Canada are reactive while the vast majority in France and Switzerland are proactive.

1.2. Questioning reporting practices

In Canada, France, UK, and Switzerland, thousands of businesses must comply with anti-money laundering/counter-terrorism financing requirements, starting with reporting obligations. According to international standards, those obliged reporting entities include 'financial institutions' and 'designated non-businesses and professions', such as casinos, real estate agents, dealers in precious metals, dealers in precious stones, lawyers, notaries, other legal professionals, and accountants (practitioners, partners, or employed professionals within professional firms), and trust and company service providers in relation to specific services to third parties.[122] The range of professions and activities covered by EU obligations has been progressively extended in accordance with FATF recommendations from the financial sector in the first Directive in 1991 to non-financial professionals and institutions in the three subsequent Directives. Although there are some variations between the four countries, they all use, in one way or another, the same list of reporting entities, with the exception of Canada, where legal professionals (legal counsels, legal firms, and Quebec notaries) are not covered by the legislation following the 2015 definition by the Supreme Court of Canada of anti-money laundering and counter-terrorist financing requirements as breaches of the constitutional right to attorney-client privilege. According to the FATF, 'in light of these professionals' key gatekeeper role, in particular in high-risk sectors and activities such as real-estate transactions and the formation of corporations and trusts, this constitutes a serious

[119] Interview with a Tracfin official, 2016.
[120] Tracfin, Annual Report, 2008.
[121] Tracfin, Annual Report, 2016, op.cit.
[122] Financial Action Task Force (FATF), Recommendations, 2012, op.cit.

impediment to Canada's efforts to fight ML [money laundering]'.[123] **However, involving lawyers as reporting entities in the fight against dirty money remains controversial, on both EU and international level**.[124]

Regarding financial transactions that must be reported, as already mentioned, Canada and France differ from Switzerland and UK to the extent that Fintrac (Canada's FIU) and Tracfin (France's FIU) go beyond the reporting of suspicious transactions and include reporting based on monetary thresholds. In this context, Fintrac collected over 23 million financial transaction reports in 2015, including over 14 million 'electronic funds transfer reports', over 9 million 'large cash transaction reports', approximately 114,000 'suspicious transaction reports' and 172,000 'casino disbursement reports'.[125] Tracfin received over 1.4 million financial transaction reports in 2015, including 43,266 'suspicious transaction reports' and 1,360,000 *communications systématiques d'informations* – COSI based on monetary thresholds. Over the same period, the UK's FIU (NCA) collected 381,882 'suspicious activity reports' and the Swiss FIU (MROS) received 2,367 reports based on suspicion.[126]

Regardless of national discrepancies, reports based on suspicion are still seen as providing the most critical information for FIUs, even though they accounted for only 3 per cent of Tracfin (France's FIU) financial transaction reports in 2015 and comprise only 2 per cent of overall reports in the Fintrac database in Canada.

> 'The question is where to look for the needle in a haystack. It is nice to have 20,000 transactions by Mister X in my database, but it is the suspicious transaction report that will go 'bang', telling me that 'Mister X is a bad guy'. We will then do a disclosure with this [report] because you cannot expect that the analysts will look at the more than 22 million reports that we receive every year. It is the suspicious transactions reports that define the road map for identifying the bad guys'.[127]

Reporting suspicious transactions

Among reporting entities, **financial institutions – starting with banks – are the main providers of suspicious transaction/activity reports to the FIUs in the four countries.** Their reports are based on internal alerts produced either by those in contact with customers or technologically driven digital surveillance of financial transactions. Not every internal alert is intended to lead to the conclusion that the related financial transactions must be reported. After further internal investigation, the alerts are either categorised as false or become external suspicious transaction reports. This critical task of differentiation is assigned to operational units whose analysts are required to review all

[123] Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, 2016, op.cit., p.7.
[124] Helgesson K. S. and Mörth U., 'Involuntary Public Policy-making by For-Profit Professionals: European Lawyers on Anti-Money Laundering and Terrorism Financing', *Journal of Common Market Studies*, Vol. 54 (5), 2016, pp. 2216-2232.
[125] Fintrac, Annual Report 2016, op.cit.
[126] National Crime Agency (NCA), Annual Report 2015, op.cit.; MROS, Annual Report 2015, op.cit.
[127] Interview with a FINTRAC official, 2015.

internal alerts to decide whether flagged behaviours should be disclosed to the national FIU.

Paradoxically, many financial institutions' main aim is to protect themselves from the national regulator rather than from potential criminals and terrorists who could use and abuse their services.[128] The internal suspicion 'threshold' above which transactions must be reported to the national FIU can be set to avoid only 'institutional risk' (reputational, financial, and legal risk for the bank) rather than contributing to the management of 'societal risk' (risk of criminal violence and terrorist attack against the population and the state). These responsibility-avoidance strategies - which are meant to protect financial institutions - obviously affect the crime-fighting objective of financial intelligence. **Depending on the national context, defensive reporting may result either in over-reporting - creating more 'noise' than actionable intelligence for law enforcement – or under-reporting – reporting only when there is no other choice to avoid sanctions because the client is already being prosecuted or has been the subject of scandal-driven media coverage.**

In the UK, the issue of defensive over-reporting was officially discussed few years ago. In a report made public in 2011, the Information Commissioner's Office (ICO – the national data protection authority) questioned how the national database of suspicious activity reports was being managed. Like any other financial intelligence unit, the UK FIU is responsible for compiling these reports in a national file and keeping them for up to 10 years. By indicating the presumed amount, origin, and destination of suspicious funds, reporting entities identify the individuals connected with suspicious transactions and provide information about them. Each record includes the individual's full name, place and date of birth, nationality, address, bank account type and number, details about his or her profession, details taken from passport and driver's license, license plate number, phone number, email address, elements related to his or her revenue sources, and current loans as well as the extent of any inheritance. At the time of the ICO challenge, the UK database had 1,900,000 entries.[129] According to ICO officials, the size of the UK financial intelligence database, the largest in the EU, 'raises concerns about whether keeping [this] data is an unjustified interference into an individuals' private and family life'.[130] They also addressed the issue of the volume of reports by asking if there was 'a pressing social need justifying the necessity to report every transaction that raises the slightest suspicion about the potential proceeds from crime or money laundering'.[131] Following the ICO report and the ensuing debates, representatives from the UK FIU had to delete

[128] Favarel-Garrigues G., Godefroy T. & Lascoumes P., 'Reluctant partners? Banks in the fight against money laundering and terrorism financing in France', *Security Dialogue*, Vol 42, No 2, pp. 179-196 ; Hibou B., *The Bureaucratization of the world in the neoliberal era : An international and comparative perspective*, New York, Palgrave Macmillan, 2015.
[129] House of Lords. European Union Committee. *Money Laundering: Data protection for suspicious activity reports*, London, United Kingdom Parliament, 2011.
[130] Ibid., p. 19.
[131] Ibid., p. 20.

approximately 584,000 reports.[132] However, since then the annual number of suspicious activity reports has increased from 200,000 to over 380,000.

In Switzerland, the issue of defensive under-reporting was the subject of recent discussions. **In the aftermath of the Panama Papers scandal, the director of Switzerland's independent financial-market regulator (FINMA) publicly criticised the lack of reaction by Swiss banks to cases where there was suspicion that dirty money was involved**[133] and 'some law enforcement authorities interviewed on site pointed out that financial intermediaries often forwarded STRs too late, making the subsequent investigations and seizure or confiscation measures less effective'.[134]

In France, defensive over-reporting is less frequently publically debated than in the UK, but France FIU's officials recently noted that the 'quantitative evolution [of suspicious transactions reports (STRs)] must, however, be coupled with the continuation of efforts in terms of quality of reported information to the Service, especially regarding the description and characterisation of suspicion'.[135]

In Canada, defensive reporting does exist but the extent is difficult to accurately measure, although several interviewees argued that current practices are less defensive than before. 'Back in 2002, it was defensive because we weren't clear on what the triggers were, you know, indicators. So, we were floundering a bit, trying to find some of those. It was lot more defensive'.[136] Nevertheless, **the challenge still lies in knowing where to draw the line between defensive reporting and intelligence-relevant reporting.**

In each country, quality control of financial transaction reports has developed through a dual focus on false positives – reports that should not have been submitted to the national FIU – and false negatives – internal alerts that should have been submitted. With false negatives, there seems to be a simple question that FIUs and financial regulators should be asking in their assessments: Is the information and interpretation behind a decision not to report factually correct? However, their actual question is slightly different: Are financial institutions able to justify their decisions? The critical issue at stake is a matter of argument. For example:

> 'here is a transaction – a person has come in several times in a week and deposited 20,000 dollars in cash. And it says that he is unemployed. What's going on here? Tell me Mister Compliance Officer. Who is this person? So then the compliance officer would say: 'Yes. The person is unemployed and he received an inheritance.' They can explain it. Other times they are silent. One of your indicators is that if the

[132] Bamford J., *Privacy and data protection: Are they casualties in the fight against crime?* London, Information Commissioner's Office, 2012.
[133] Boder W., 'La Finma veut changer la culture de la lutte contre le blanchiment d'argent', *Le Temps*, 2016.
[134] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, op.cit., p. 51.
[135] Tracfin, Press Release: Tracfin présente son rapport annuel - Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2015, 2016.
[136] Interview with a bank compliance officer, Canada, 2015.

> person's income or employment do not match the transactions in their account, then it is reportable. Again, why wasn't this reported? So I always bring it back to the policies and procedures'.[137]

In this context, a decision not to report can be factually correct (it was a false alert) but can be sanctioned as non-compliant because of lack of justification. By contrast, another non-reporting decision can be factually wrong but compliant because it is based on an argument that is credible and documented. This prevalence of interpretation over facts is, inevitably, an unavoidable element in the rationale at the core of any suspicion-based model of denunciation. **To the extent that they are not based on a monetary threshold, suspicious transactions reports (STRs) *de facto* introduce a significant margin of interpretation. Decisions over what one person sees as a false alert and another sees as a suspicious act create tension, dispute, and concern in the field of financial intelligence.** Given this element of ambiguity, FIUs and regulators are not necessarily in a position of strength in the argumentative battle with reporting entities, except when they detect unjustified incoherence between an entity's internal policy on reporting and its implementation (or lack thereof).

Typology of suspicious transaction reports

Finally, although quality control of reporting includes a dual focus on false-positive and false-negative reports, the emphasis is largely on the problem of false-negatives (when internal alerts should have been submitted). **In most countries, penalties for non-compliance are primarily directed at failure to report suspicious transactions, not at purely defensive disclosures. Consequently, from the banks' perspective, over-reporting is far less problematic and has far less impact in terms of legal, financial, and reputational risk than under-reporting. The question is then when and why does an investigated internal alert lead to a disclosure to financial intelligence units?**

Everyday reporting practices make it difficult to distinguish suspicious from unusual. In 1993, Interpol representatives proposed a clear-cut distinction between 'unusual' transactions and 'suspicious' transactions:

> 'A suspicious transaction or series of them is conduct which, because of the circumstances, has reached a level of suspicion sufficient to identify a criminal offence (e.g., subject is suspected of money-laundering and drug trafficking or other stated offence). An unusual transaction, on the other hand, is one or several transactions of an unusual nature but where a criminal offence has yet to be determined'.[138]

Our fieldwork shows that it can be assumed that not all suspicious transaction reports correspond to the Interpol definition. Moreover, agreement with the definition is often

[137] Interview with a FINTRAC official, 2015.
[138] Gold M., and Levi M., *Money laundering in the UK: An appraisal of suspicion-based reporting*, London, The Police Foundation and University of Wales, 1994, p. 89.

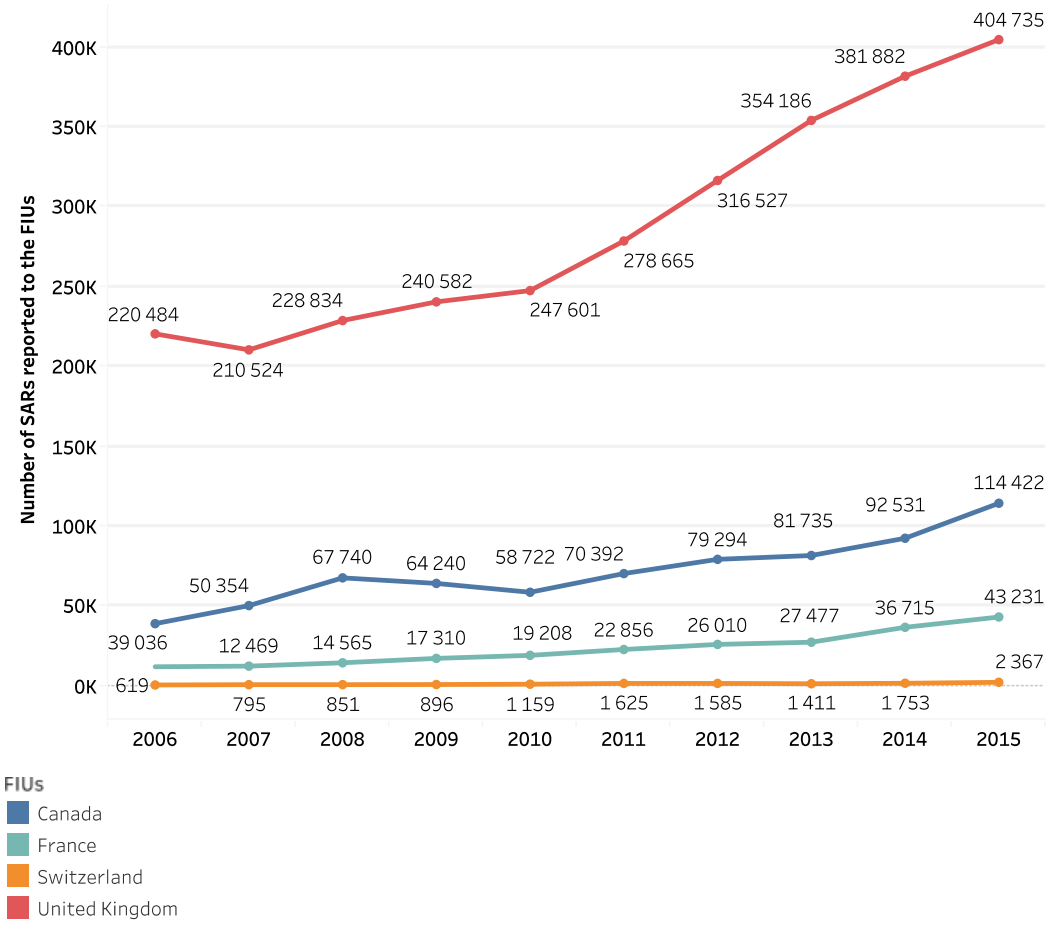
limited to the most obvious cases, many of which are reported on the basis of 'transferred suspicion'[139] from negative news (media), judicial orders, and law enforcement requests. In Switzerland (the only country that provides public statistics on this topic), 'most reports are made on the basis of external sources of information such as press articles (34 per cent) or requests by national or international judicial authorities. The proportion of reports that originate in alerts raised by the monitoring systems of the financial institutions themselves remains small and is decreasing (18 per cent in 2014, 7 per cent in 2015)'.[140] The most obvious cases are also reported as being 'visibly suspicious'[141] in relation to unsophisticated transactions involving known individuals (e.g., barely competent petty crooks involved in money-laundering schemes). In contrast, a large number of suspicious transactions reports seem to correspond to the Interpol definition of an unusual transaction – every transaction that falls outside what has been determined to be usual or which matches pre-defined unusual financial behaviours tends to be reported if the reporting entities do not know the factors that explain why it occurred. It is the lack of explanation or the lack of credibility associated with the client's explanation - if (s)he is questioned during the inquiry process - that explains the denunciation. This reflects the many interpretations of the concept of suspicion. While the definitions of suspicion (unqualified suspicion vs reasonable suspicion vs well-founded suspicion) as well as the distinction between suspicious transaction report, and suspicious activity report is beyond the scope of this study, the current variations from one country to another – including within the EU - are a critical issue that deserves further analysis. **'Suspicion' is at the heart of financial intelligence practices but it is not interpreted the same way from one country to another**.

1.3. FININT in Numbers

The following tables and graphs are designed on the basis of public information obtained from the FIUs' annual reports from 2006 to 2016.

[139] Ibid., p. 61
[140] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016, op.cit., p.102.
[141] Gold M., and Levi M., *Money laundering in the UK: An appraisal of suspicion-based reporting*, op.cit.

Chart 1 Suspicious transactions reported to FIUs



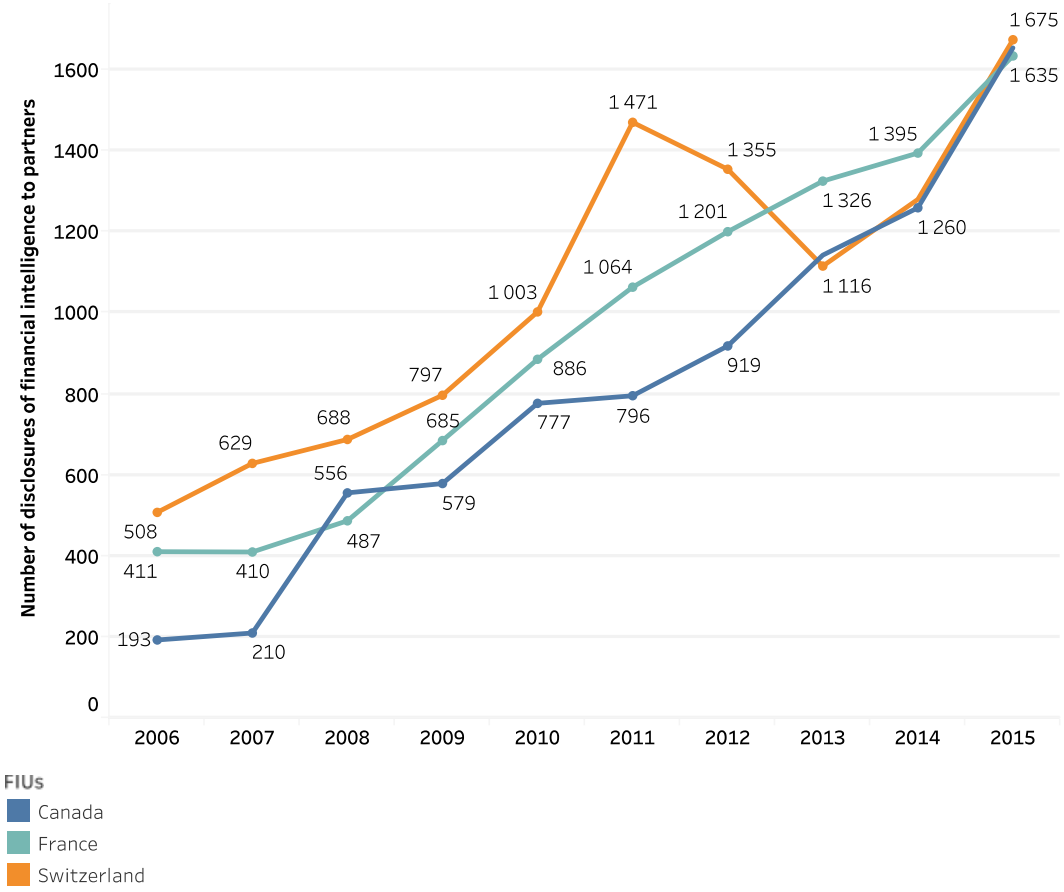
	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
United Kingdom's NCA	220 484	210 524	228 834	240 582	247 601	278 665	316 527	354 186	381 882	404 735	2 884 020
Canada's Fintrac	39 036	50 354	67 740	64 240	58 722	70 392	79 294	81 735	92 531	114 422	718 466
France's Tracfin	12 047	12 469	14 565	17 310	19 208	22 856	26 010	27 477	36 715	43 231	231 888
Switzerland's MROS	619	795	851	896	1 159	1 625	1 585	1 411	1 753	2 367	13 061

- The number of reports increased significantly between 2006 and 2015 for every FIU: UK: +184 per cent; Canada: +293 per cent; France: +359 per cent; Switzerland: +382 per cent.
- The differential 'growth rate' of reports over the last ten years has gone down slightly for every FIU but has not transformed the degree of difference between FIUs. In 2006, the UK FIU received 356 times more reports than the Swiss FIU and 170 times more reports in 2015. **Differences between FIUs are sometimes proportionate to the size of national financial markets but this explanation falls short in the case of Switzerland, which is a major financial centre with approximately 26 per cent of the world market for the management of foreign**

private assets.[142] While Switzerland is regularly criticised for this comparatively low number of reports, MROS officials argue that the difference relates primarily to a different definition of the notion of suspicion : 'In contrast to most foreign reporting systems, which are based on a "suspicious transaction report - STR" (i.e. an unqualified suspicion), or even merely on a "currency transaction report - CTR" (i.e. a transaction exceeding a certain monetary threshold), the Swiss reporting system is based on a well-founded suspicion of money laundering — as the name SAR or "suspicious activity report" suggests. Foreign systems result in a much higher number of reports, but their content does not compare with the high quality of the Swiss reports, however. The efficiency and effectiveness of money laundering legislation should be measured not only against the number of reports or statistics, but — more relevantly — by comparing the proportion of forwarded reports. Compared with foreign reporting systems, the Swiss reporting system boasts a high proportion of SARs forwarded to prosecution authorities'.[143] In addition to semantic debate, the huge difference in reporting between the UK and Switzerland also illustrates different defensive strategies, from over-reporting in the former case to under-reporting in the latter (e.g. section 1.1).

[142] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016, op.cit.
[143] MROS, Annual Report, 2013, pp. 18-19; see also Palmieri R. and Rigotti E., 'Suspicion as an argumentative move. Semantic analysis of a pivotal concept in banks' *anti-money laundering* argumentative activities', *Journal of Argumentation in Context*, Vol. 3(3), 2014, pp. 287–321.

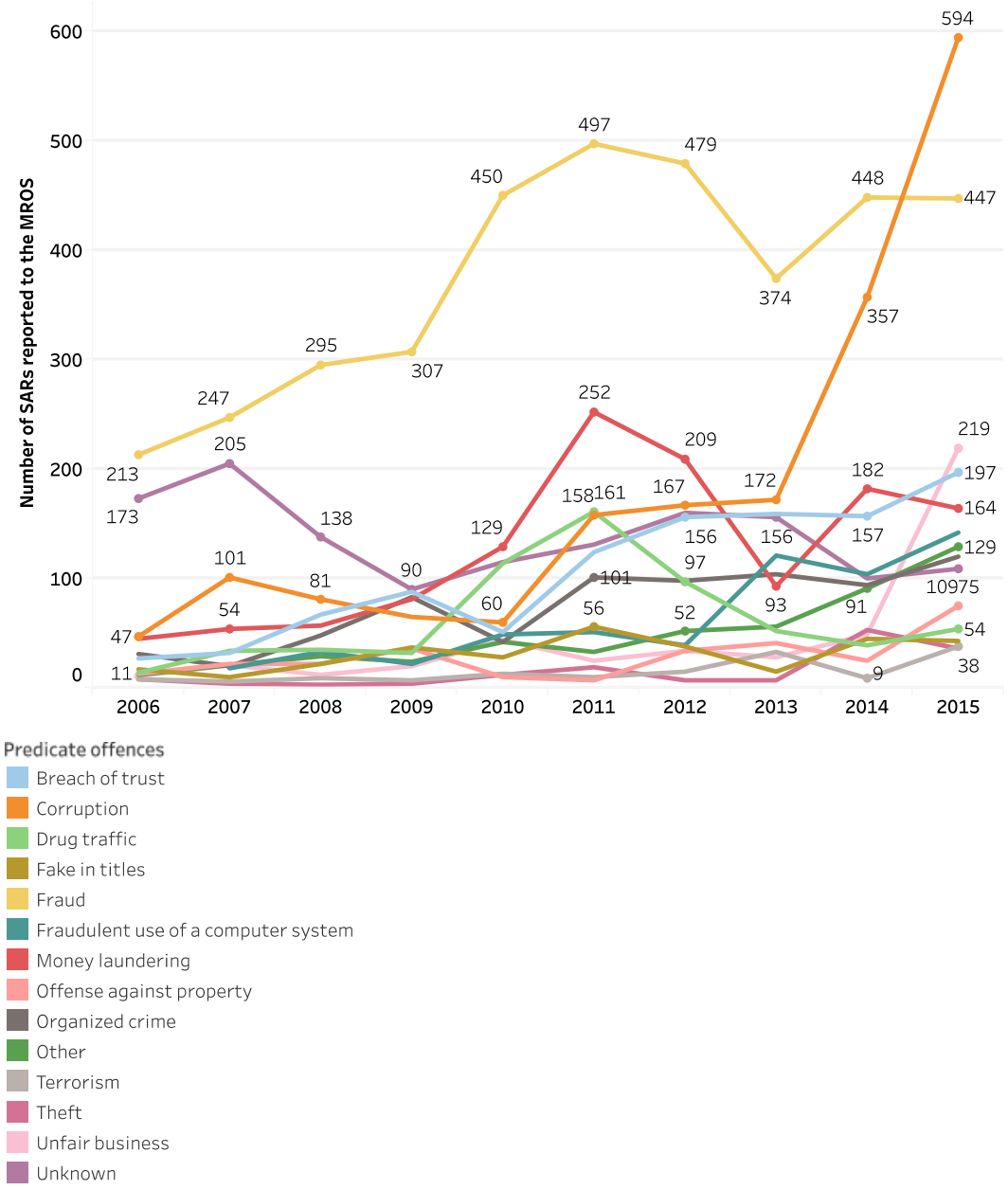
Chart 2 Disclosures of FININT to national partners – numbers by FIU under examination



	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Switzerland's MROS	508	629	688	797	1 003	1 471	1 355	1 116	1 281	1 675	10 523
France's Tracfin	411	410	487	685	886	1 064	1 201	1 326	1 395	1 635	9 500
Canada's Fintrac	193	210	556	579	777	796	919	1 143	1 260	1 655	8 088

- The constant increase in disclosures between 2006 and 2015 illustrates a common trend towards closer cooperation between FIUs and their national partners.
- Notwithstanding the huge difference between FIUs with regard to the number of reports from obligated entities, there is a growing similarity with regard to the number of subsequent disclosures to national partners.
- This high similarity masks, however, three main variations between the FIUs under examination: 1) The number of suspicious transaction reports (STRs)/suspicious activities reports (SARs) included in each disclosure may vary considerably from one case to the other and from one country to the other. 2) The vast majority of disclosures to national partners is 'reactive' in Canada and 'proactive' in France and Switzerland. 3) The range of national partners varies widely across jurisdictions, from prosecution authorities only to a set of judicial, police, intelligence, and administrative agencies.

Chart 3 Switzerland's FIU: suspicious transaction reports by predicate offence



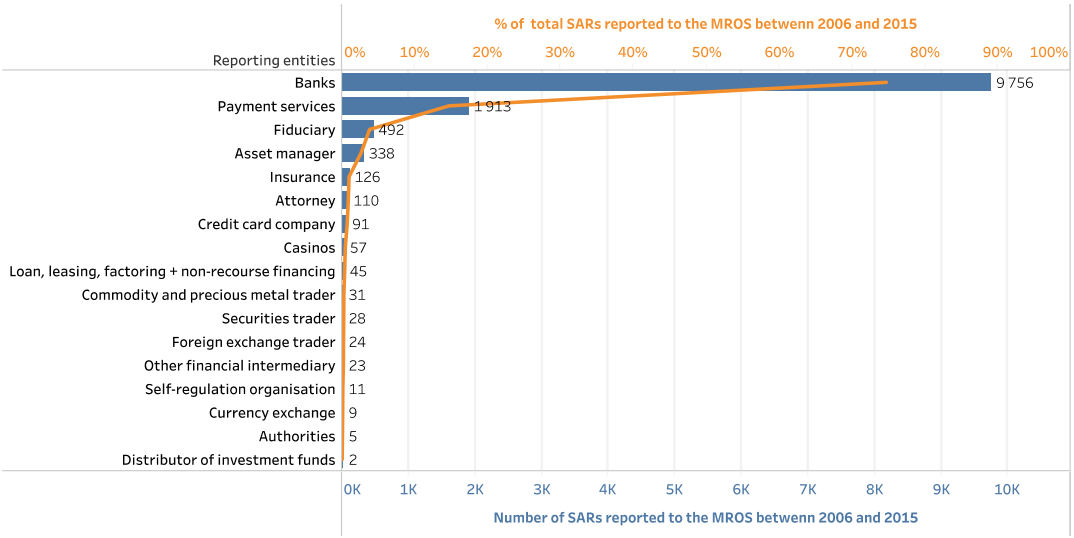
Predicate offences	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Fraud	213	247	295	307	450	497	479	374	448	447	3 757
Corruption	47	101	81	65	60	158	167	172	357	594	1 802
Unknown	173	205	138	90	115	131	160	156	100	109	1 377
Money laundering	45	54	57	81	129	252	209	93	182	164	1 266
Breach of trust	27	32	67	88	51	124	156	159	157	197	1 058
Organized crime	31	20	48	83	42	101	98	104	94	120	741
Drug traffic	14	34	35	32	114	161	97	52	39	54	632
Fraudulent use of a computer system		18	33	22	49	51	39	121	104	142	579
Other	12	21	29	24	42	33	52	56	91	129	489
Unfair business	11	21	12	20	44	25	34	28	49	219	463
Fake in titles	17	10	22	37	28	56	38	15	45	43	311
Offense against property	13	22	22	36	10	7	34	41	25	75	285
Theft	8	4	3	4	12	19	7	7	53	36	153
Terrorism	8	6	9	7	13	10	15	33	9	38	148
Total	619	795	851	896	1 159	1 625	1 585	1 411	1 753	2 367	13 061

- It is worth mentioning that the notion of 'fraud' does not cover at all tax evasion in relation to direct taxes as this crime has been considered a predicate offence to money laundering only since 2016.
- Although the number of reports in connection with drug traffic is lower than many other predicate offences, such as fraud and corruption, 50 per cent of all convictions for money laundering between 2008 and 2012 were related to drug trafficking, compared to 9 per cent for fraud and even fewer for corruption.[144] The sharp contrast between the number of reports per predicate offence and the number of convictions is partly related to international connections: 'numerous money laundering cases in Switzerland concern predicate offences committed abroad'.[145] In other words, convictions for money laundering in Switzerland often depend on international cooperation to obtain evidence of the predicate offence. Two hypotheses deserve further analysis to explain the above-mentioned contrast: 1) International cooperation with Switzerland is more efficient in drug trafficking cases than corruption cases. 2) Swiss money-laundering cases related to corruption involve international elements more frequently than money-laundering cases related to drug traffic.

[144] Fedpol, Blanchiment d'argent - Jugements prononcés en Suisse en matière de blanchiment d'argent, Bern, Publication de la Police judiciaire fédérales PJF, fedpol, 2014.
[145] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016, op.cit., p. 61.

Chart 4 Switzerland's FIU: suspicious transaction reports by reporting entity

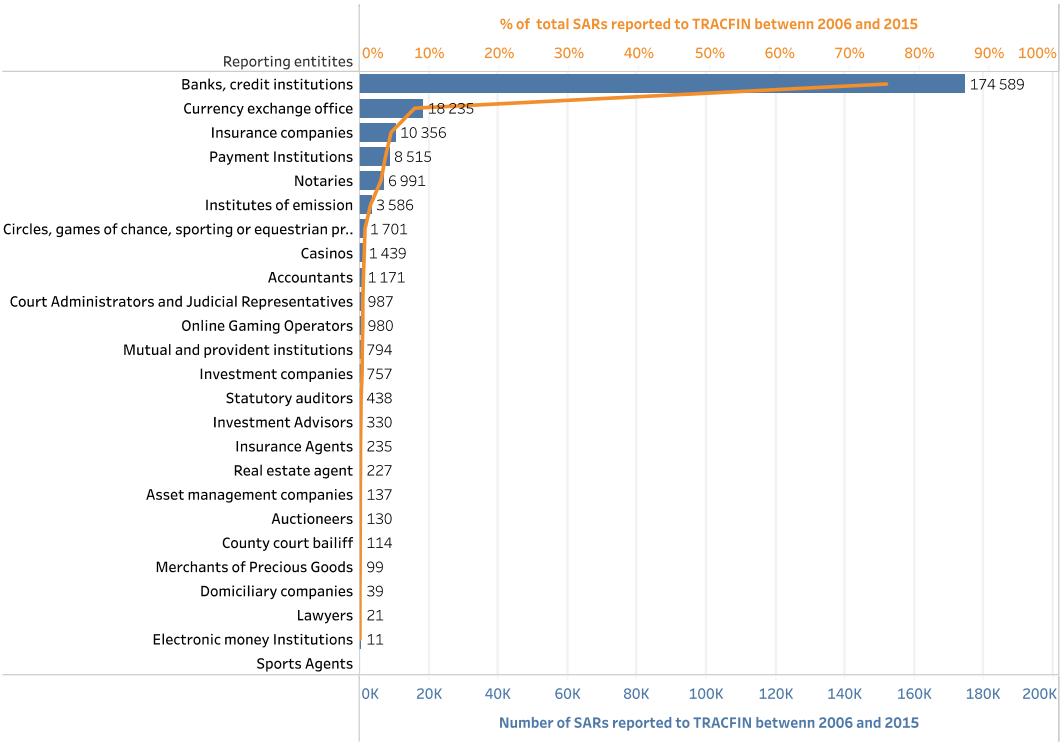
Reporting entities	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Banks	359	492	573	603	822	1 080	1 050	1 123	1 495	2 159	9 756
Payment services	164	231	185	168	184	379	363	74	107	58	1 913
Fiduciary	45	23	37	36	58	62	65	69	49	48	492
Asset manager	6	8	19	30	40	27	49	74	40	45	338
Insurance	18	13	15	9	9	11	9	19	11	12	126
Attorney	1	7	10	11	13	31	12	9	10	6	110
Credit card company		2	2	10	9	10	22	14	9	13	91
Casinos	8	3	1	5	8	6	6	8	9	3	57
Loan, leasing, factoring + non-recourse financing	8	4	1	11	1	5	1	4	3	7	45
Commodity and precious metal trader	1	5	1		1	1	3	10	3	6	31
Securities trader		2	5	2	4		1	1	10	3	28
Foreign exchange trader	1			5	6	7		5			24
Other financial intermediary	1	2		1	4	2	4	1	3	5	23
Self-regulation organisation	3	1		4		1			2		11
Currency exchange	2	1	1	1		3				1	9
Authorities	2		1						2		5
Distributor of investment funds		1								1	2
Total	619	795	851	896	1 159	1 625	1 585	1 411	1 753	2 367	13 061



- Banks are the reporters of suspicion *par excellence* in Switzerland while the number of reports from other obliged entities, such as legal professions, casinos and securities trader, raises questions.

Chart 5 France's FIU: suspicious transaction reports by reporting entity

Type of profession	Reporting entitites	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Financial professions	Banks, credit institutions	9 967	10 047	11 511	12 254	13 206	15 582	19 288	21 950	29 508	31 276	174 589
	Currency exchange office	1 121	992	1 467	2 249	3 002	3 251	2 104	1 199	1 141	1 709	18 235
	Insurance companies	520	619	703	1 007	808	889	1 059	1 169	1 423	2 159	10 356
	Payment Institutions						290	1 218	831	1 641	4 535	8 515
	Institutes of emission		233	200	675	608	779	436	259	254	142	3 586
	Mutual and provident institutions	7	11	10	58	56	98	35	60	139	320	794
	Investment companies	51	60	58	67	134	133	52	46	51	105	757
	Investment Advisors			14	46	78	92	20	20	25	35	330
	Insurance Agents				2	3	40	38	25	62	65	235
	Asset management companies				3	10	10	13	20	23	58	137
	Electronic money Institutions									1	10	11
Non-financial professions	Notaries	217	313	347	370	674	1 069	995	970	1 040	996	6 991
	Circles, games of chance, sporting or equestrian predictions	99	107	148	361	269	73	120	127	185	212	1 701
	Casinos	30	40	37	30	137	149	171	153	270	422	1 439
	Accountants	12	11	19	55	98	135	145	195	215	286	1 171
	Court Administrators and Judicial Representatives	14	19	18	57	55	62	52	82	100	528	987
	Online Gaming Operators						76	127	181	450	146	980
	Statutory auditors	4	6	5	22	46	57	54	72	84	88	438
	Real estate agent	1	5	3	33	14	19	34	54	29	35	227
	Auctioneers	1	4	5	5	8	16	7	25	26	33	130
	County court bailiff			1	2		17	14	18	23	39	114
	Merchants of Precious Goods		1	11	12	2	13	3	12	16	29	99
	Domiciliary companies						4	21	3	8	3	39
	Lawyers	3	1	3	2		1	4	6	1		21
	Sports Agents											
Total		12 047	12 469	14 560	17 310	19 208	22 855	26 010	27 477	36 715	43 231	231 882

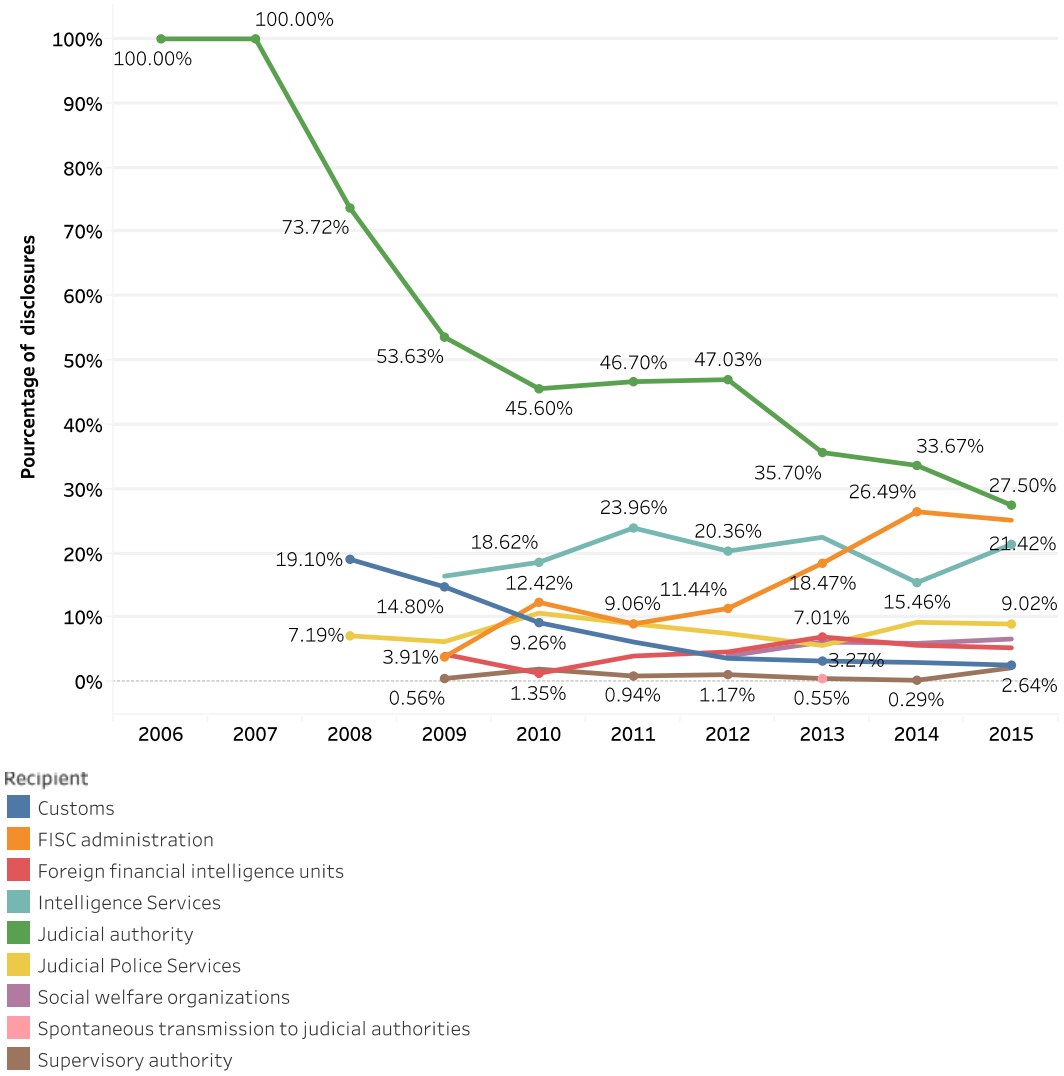


- The largest increase in the number of suspicious transaction reports in France occurred between 2013 and 2014 (+33 per cent, from 27,477 to 36,715). According to Tracfin, 'the increase in reports on tax evasion partly explains this growth. The political, economic, and legislative context also contributes to professionals' awareness on this type of fraud. Moreover, the media coverage of financial scandals may have reinforced this trend'.[146]
- While financial institutions in general, and banks in particular, are also the major reporters in France, the current low level of reporting by lawyers merits further consideration.

Chart 6 France's FIU: disclosures of FININT to partners

Recipient	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Judicial authority	411	410	359	384	404	495	522	458	464	448	4 355
Intelligence Services				118	165	254	226	289	213	349	1 614
FISC administration				28	110	96	127	237	365	410	1 373
Judicial Police Services			35	45	95	96	84	73	128	147	703
Customs			93	106	82	66	41	42	42	43	515
Foreign financial intelligence units				31	12	43	52	90	79	87	394
Social welfare organizations							45	80	83	109	317
Supervisory authority				4	18	10	13	7	4	36	92
Spontaneous transmission to judicial authorities								7			7

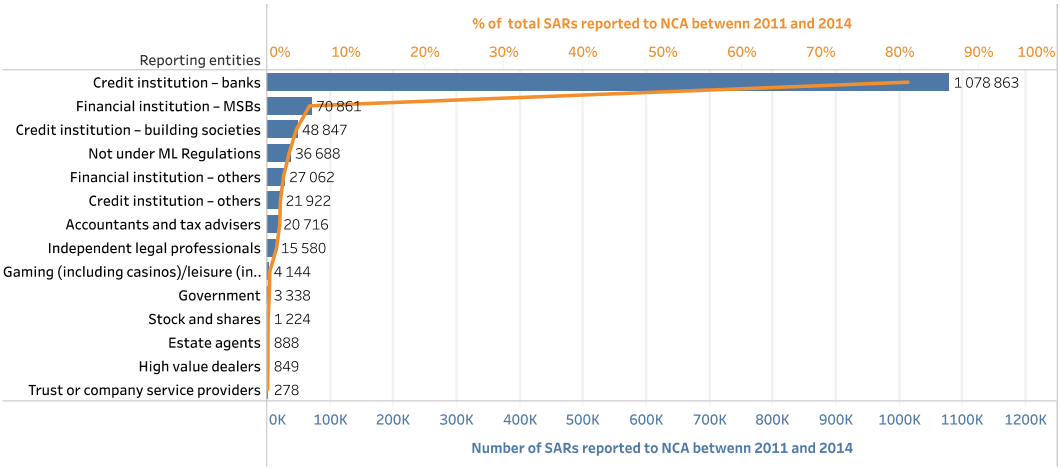
[146] Tracfin, Annual Report, 2015, p. 8.



- Since 2013, tax administration authorities have become the second highest recipient of France's FIU (Tracfin) disclosures. 80 per cent of these disclosures led to further controls by the tax administration with 'positive results'. Their main focus is on 'serious tax crime', often in relation to cases of one million euros or more.
- With regard to Tracfin disclosures to judicial authorities (their main partner), tax crimes were the second most represented predicate offence in 2015 (105 disclosures).
- Tracfin disclosures to partners are largely proactive, except for cooperation with intelligence agencies, which accounts for two thirds of reactive disclosures.

Chart 7 UK FIU: suspicious transactions reports by reporting entity

Reporting entities	2011	2012	2013	2014	Total
Credit institution – banks	218 027	251 336	291 055	318 445	1 078 863
Financial institution – MSBs	23 408	21 343	14 990	11 120	70 861
Credit institution – building societies	9 363	10 844	12 834	15 806	48 847
Not under ML Regulations	16 833	4 060	8 414	7 381	36 688
Financial institution – others		13 359	6 868	6 835	27 062
Credit institution – others			10 094	11 828	21 922
Accountants and tax advisers	5 740	5 428	4 930	4 618	20 716
Independent legal professionals	4 208	3 935	3 610	3 827	15 580
Gaming (including casinos)/leisure (including some not under ML Regulations)	947	1 062	704	1 431	4 144
Government		3 338			3 338
Stock and shares		1 224			1 224
Estate agents	139	215	179	355	888
High value dealers		383	331	135	849
Trust or company service providers			177	101	278

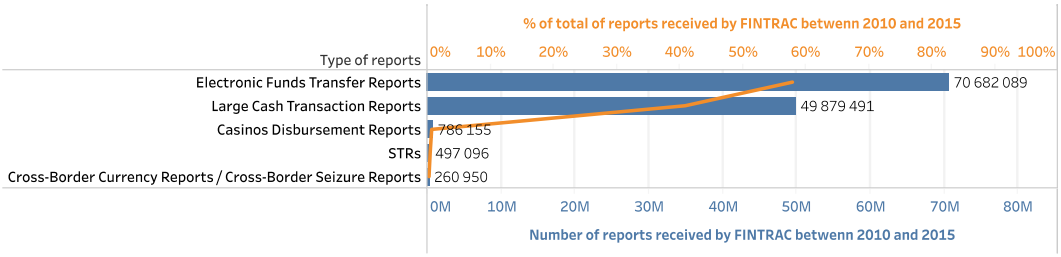


- Although money service businesses (MSBs) are the second major category of reporters in the UK, they are also considered to be high money laundering risks in the financial industry. Numerous MSBs have been targeted by bank 'de-risking' strategies, with banks deciding to discontinue business relationships with them. 'We are aware that some banks are no longer offering financial services to entire categories of customers that they associate with higher money-laundering risk'.[147] The growing trend to exit high-risk businesses entirely – starting with MSBs - is only just beginning to be questioned by financial regulatory bodies in some countries, especially in the UK in terms of consumer protection and competition issues.

[147] Financial Conduct Authority (FCA), De-risking: Managing Money-Laundering Risk, 2016.

Chart 8 Canada's FIU: financial transactions reports

Type of reports	2010	2011	2012	2013	2014	2015	Total
Electronic Funds Transfer Reports	11 878 508	10 251 643	10 993 457	11 182 829	12 348 360	14 027 292	70 682 089
Large Cash Transaction Reports	7 184 831	8 062 689	8 523 416	8 313 098	8 445 431	9 350 026	49 879 491
Casinos Disbursement Reports	102 438	109 172	116 930	130 141	155 185	172 289	786 155
STRs	58 722	70 392	79 294	81 735	92 531	114 422	497 096
Cross-Border Currency Reports / Cross-Border Seizure Reports	40 856	35 026	31 826	42 650	47 228	63 364	260 950

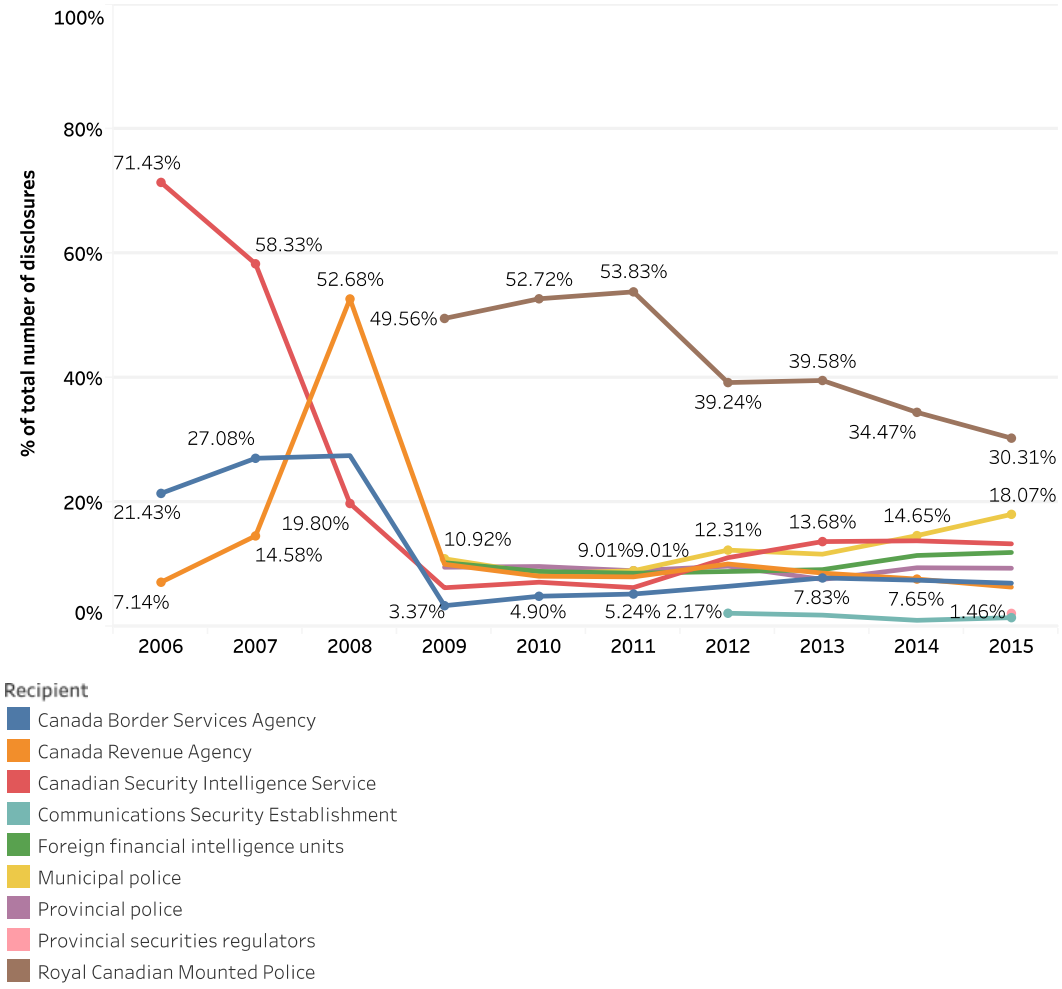


- 'The suspicious transaction reports are the most important reports, no contest'.[148] Although STRs account for only 2 per cent of the overall financial transactions reports in the Fintrac database, they are perceived and promoted as 'the key to many other things', e.g., the most critical piece of information. STRs are at the heart of financial intelligence practices. In this respect, Fintrac is highly dependent on banks, by far the largest reporters among the range of regulated businesses.

Chart 9 Canada's FIU: disclosures of FININT to partners

Recipient	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Royal Canadian Mounted Police				617	883	914	580	703	779	976	5 452
Municipal police				136	143	153	182	207	331	582	1 734
Canadian Security Intelligence Service	20	28	59	78	120	107	164	243	312	429	1 560
Foreign financial intelligence units				128	149	146	131	163	259	384	1 360
Canada Revenue Agency	2	7	157	125	136	136	149	153	173	205	1 243
Provincial police				119	162	153	144	135	214	303	1 230
Canada Border Services Agency	6	13	82	42	82	89	96	139	169	225	943
Communications Security Establishment							32	33	23	47	135
Provincial securities regulators										69	69

[148] Interview with a FINTRAC official, 2015.



- By contrast to Tracfin in France, Canada's FIU (Fintrac) disclosures to partners are more reactive than proactive. Moreover, law enforcement agencies note 'that due to time and resource considerations, in line with their prioritization process, fewer investigations are initiated on the basis of a proactive disclosure [from Fintrac] which has no link to an ongoing investigation'.[149]

[149] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016, op.cit., p. 46.

2. Transnational financial intelligence in practice

2.1. European and international communication channels

> 'Given the growing internationalisation of financial flows, we really cannot manage with national financial intelligence alone. We have to be able to look for information abroad very quickly. The importance of cooperation has exploded compared to what was envisaged in the 1990s'.[150]

In accordance with international standards, any FIU will 'follow the money' to determine 1) the origin of financial flows, 2) their destination, 3) the economic reason for the transaction(s)/operation(s), and 4) the beneficial owner(s) of the assets. While financial intelligence practices to control dirty money were not designed to either challenge or hinder the functioning of the financial system, they have been defined as a corollary of financial liberalisation. In this context, international cooperation between FIUs is promoted as a way to prevent the internationalisation of financial flows from being used to make it more difficult to discern criminal activity. In practice, different types of situations encourage FIUs to cooperate with foreign counterparts.

First, **the request for information from another FIU can be initiated by proactive analysis of suspicious transaction reports (STRs).** In this case, one or several reports include an international element, such as cross-border transactions, bank customers of foreign nationality, or national citizens living or working in another country, that justifies the request. A request for international cooperation is sent when access to further information at the national level is deemed insufficient to determine whether the reported transactions are relevant for intelligence and/or judicial purposes. For example, a reporting entity justifies a disclosure to the FIU by arguing that it concerns a customer of foreign nationality who is party to legal proceedings in his country. The FIU analysts will first access national databases and, if they cannot verify the assertion of the entity, then they will ask their foreign counterparts if they have any relevant information, using their right to request confirmation that they need to analyse suspicious transaction reports (STRs). If, in a similar case, FIU analysts can confirm through national databases or open source information that the flagged client is party to legal proceedings in a foreign country, they can decide to share information spontaneously with the foreign FIU:

> 'Here, we are not asking for anything. We tell them that we have received a suspicious transaction report in relation to a person who is currently party to legal proceedings in their country and we give them the information we have on the basis of the report'.[151]

[150] Interview FIU, 2016.
[151] Interview FIU, 2016.

As stated in the international principles for information exchange between FIUs, 'FIUs should exchange information freely, spontaneously and upon request, on the basis of reciprocity'.[152]

Second, **FIUs can receive sensitive information or requests from their national law enforcement partners that lead them to follow the money trail abroad through international cooperation.** FIU officials can either be asked by their partners to make a request for information from another FIU or they can proactively seek information from foreign FIUs in order to be able to help their national partners. In the case of an explicit demand from a national partner, **some law enforcement officers see cooperation between FIUs as providing a faster channel for information exchange in a criminal matter than international legal assistance. They often use the FIU channel as a first step to determine if it is worth sending a request for international legal assistance in order to collect evidence.** In proactive searches, before using information provided by a national partner to justify a request to foreign FIU(s), FIU officials must generally obtain the national partner's permission.

Third, **the FIU channel can be used for 'diagonal cooperation' in connection with previous situations:**

> 'I think there is also another approach and we practice it a lot with close partners. This is diagonal cooperation. It is not necessarily from FIU to FIU only. I mean, if we know that the information we want is held by a specific law-enforcement agency, we can specify this to the foreign FIU, which is thus being used as a postal box. And the reverse is also true – the foreign law-enforcement agency will ask their FIU to ask us if we have information on X or Y. Diagonal cooperation is very frequent between us and them. We actually have relations with police forces and intelligence services in this country and they use our financial intelligence as long as there is a link with our country'.[153]

In this case, one of the FIUs acts as a facilitator since it mediates the cooperation between its national partners and a foreign FIU.

Regardless of the motive for requesting information, the FIUs under examination use from one to three cooperation channels depending on geographic location, legal framework and technical capacity, as described hereafter.

The Egmont Secure Web

First, in accordance with the FATF recommendations, FIUs are expected to apply for membership in the Egmont Group. In 1995, a group of FIU representatives met at the Egmont Arenberg Palace in Brussels and decided to create a forum for FIUs around the world. More than twenty years later, this 'informal network' is now largely formalised in

[152] Egmont Group of FIUs, Principles for information exchange between FIUs, June 2013, p. 4.
[153] Interview FIU, 2016.

the 'Head of financial intelligence units' (HoFIUs – the governing body of the Egmont Group), four working groups, the Egmont committee (the consultation and coordination mechanism for the HoFIUs and the working groups), and a secretariat established ten years ago in Toronto (Canada). The secretariat, committee, and working groups meet three times per year, including the Egmont annual plenary session. The governance and standards of the Egmont Group rely on a set of key documents such as the 'Egmont Charter', the 'Egmont Principles for information exchange', and 'Operational Guidance for FIU activities'.[154] In general terms, the Egmont Group aims to improve both international cooperation in the fight against dirty money and national implementation of FININT programs in the areas of information exchange, training, and the sharing of expertise. This includes the goal of 'fostering better and secure communication among FIUs through the application of technology, presently via the Egmont Secure Web (ESW)'.[155]

As members of the Egmont Group, 152 FIUs can make and respond to requests via the ESW, which is promoted as a secure and reliable FIU-to-FIU channel of communication. 'The ESW is an electronic communication system that allows encrypted sharing among members of emails and financial intelligence, as well as information of interest to members and to the functioning of the Egmont Group'.[156] The use of this channel is not limited to operational purposes. It 'permits members to communicate with one another via secure e-mail, requesting and sharing case information as well as posting and assessing information on typologies, analytical tools, and technological developments'.[157] One FIU may have several ESW e-mail addresses, including one for operational purposes, one that allows the director to contact foreign FIU directors directly, and others to deal with international strategic and policy issues.[158] The ESW is maintained technically by FinCen (the US FIU) on behalf of the Egmont Group.

Regarding operational communication, any FIU receiving a request for information is encouraged to respond as soon as possible, 'consistent with the urgency of the request, or within a month if possible. Additional time is reasonable if there is a need to query external databases or third parties'.[159] Following the official Egmont query form, the FIU can indicate if the request for information is urgent. 'For me, there are two types of requests: in the case of urgent requests, we try to reply within a week. With normal requests, it can take a month'.[160] FIUs usually classify their requests from 'normal' to 'urgent' and even 'very urgent' in some cases, but the definition of urgency can be a matter of debate:

[154] Egmont Group of FIUs, Charter, July 2013; Egmont Group of FIUs, Principles for information exchange between FIUs, op.cit.; Egmont Group of FIUs, Operational Guidance for FIU Activities and the Exchange of Information, July 2013 (revised June 2014).
[155] Egmont Group of FIUs, Benefits of Egmont Group Membership, 2017.
[156] Egmont Group of FIUs, Charter, op.cit., p. 8.
[157] FinCEN, The Egmont Group of Financial Intelligence Units, 2017.
[158] Interviews FIUs, 2016.
[159] Egmont Group of FIUs, Operational Guidance for FIU Activities and the Exchange of Information, op.cit., p. 5.
[160] Interview FIU, 2016.

'When we are told that it is urgent, we tend to respond more quickly. Now the problem is that certain FIUs think that everything is urgent … Therefore, it is useful to contact them to know if it is really urgent and we often nuance the degree of urgency when we talk to them. Nonetheless, we do try to process the urgencies first, the real ones'.[161]

Informally, phone calls often complement e-mail messages to either specify the degree of urgency or give further contextual details if necessary to allow the request to proceed more quickly. According to certain FIU officials, the meaning and implication of the indication 'urgent' should be further specified to avoid everyone ticking the same box, which poses a challenge for the prioritisation of information sharing. In practice, however, **the degree of responsiveness is not linked only to the degree of urgency of the incoming request but also to relations and experiences between two FIUs:**

> 'We often receive demands with 40 or 50 names. We need to have an analyst working on them and this is a very difficult kind of request. Consequently, if we really want to reply, we categorise the request. Does it come from our top 5 partners, yes or no? If so, we will do it, notwithstanding the time and effort. If not, or if it comes from a partner who is very slow to respond to our own requests or who does not respond at all, its priority will be downgraded. We will reply in the end but we will probably limit ourselves to providing information about five to ten key people rather than the forty or fifty persons mentioned in the request'.[162]

There is also criticism of 'phishing expeditions' – sending the same request to 'everyone'. 'We still receive lots of requests that make no sense and there are also FIUs sending their requests to everyone everywhere and we struggle to find a link with us'.[163] The FIUs under examination criticize the use of phishing expeditions except in cases of 'maximum urgency,' such as after a terrorist attack.

If there are manifest and recurrent problems with cooperation in relation to a particular FIU, the HoFIUs of the Egmont Group may eventually take countermeasures. 'When an FIU joins the Egmont Group, it is required to sign the Egmont Charter and commit to working according to its founding documents. However, countries that join Egmont are not part of any treaty or convention; therefore, no international sanctions or legal action can be taken against a non-complying country' although 'the Egmont Group has an internal Compliance Procedure that defines the actions to be taken against an FIU that does not comply with the Egmont Charter and Principles for Information Exchange document'.[164] **The governing body of the Egmont Group (HoFIUs) has the power to suspend and/or expel non-compliant FIUs**.[165] In July 2011, the HoFIUs accused the Swiss financial intelligence unit of insufficient international co-operation and issued a warning of suspension.[166] As a result, Switzerland's anti-money laundering act was amended in

[161] Interview FIU, 2016.
[162] Interview FIU, 2016.
[163] Interview FIU, 2016.
[164] Egmont Group of FIUs, FAQ, 2017.
[165] Egmont Group of FIUs, Charter, op.cit.
[166] MROS, Annual Report, 2012.

2012 to enable the exchange of financial information from FIU to FIU.[167] The legislative amendments came into force in 2013 and the warning of suspension was lifted the same year.[168] Compliance does not mean that FIUs are systematically obliged to respond to a request and their national legislation generally specifies an FIU's differential obligations to national and international partners. Usually, the FIU 'must' reply to the requests of national partners while it 'can' respond to the international requests. **National legislations also mention exceptional situations in which the FIU may refuse to exchange information on the basis of national interests, security, public order, or fundamental principles**. Exceptions vary slightly among countries but can include refusal to exchange information about political opponents in 'non-democratic states', with the countries of origin of asylum seekers, about persons who can be jailed for a crime of opinion, or about individuals who are liable to be sentenced to death on the basis of the information provided. Interviewees all mentioned specific cases in which they had not replied based on those situations, although the reason for non-response was not always made explicit to the requesting agency. **It is recognised that exceptions are legitimate but some FIUs complain that the 'political argument' is occasionally used to mask non-compliant activities that ultimately protect corrupt foreign politicians. In this regard, the fourth European Directive specifies that 'those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes'**.[169]

The exchange of information between FIUs is systematically associated with explicit determination of appropriate conditions of use. The rules for information dissemination include three main options. First, the default option always indicates that the FIU cannot 'disclose the [received] information outside its agency without the prior written permission of the disclosing FIU.[170] Regarding the second option, the disclosing FIU can authorise its FIU counterpart to disseminate the information outside its agency but for intelligence purposes only, e.g. informally, not for evidence purposes. Third, the FIU agrees that their counterpart can disseminate and use the information beyond informal intelligence, for instance as evidence.

FIU.NET

In October 2000, Council Decision 2000/642/JAI was adopted concerning arrangements for cooperation between FIUs of Member States with respect to exchanging information. While the arrangements already adopted by EU Member States in relation to the Egmont Group and the ESW were mentioned, the community legislation noted that 'it is necessary that close cooperation take place between the relevant authorities of the Member States involved in the fight against money laundering and that provision be made for direct communication between those authorities'.[171] This resulted in the

[167] MROS, Annual Report, 2013.
[168] MROS, Annual Report, 2014.
[169] Directive 2015/849, op.cit.
[170] Egmont Group of FIUs, Operational Guidance for FIU Activities and the Exchange of Information, op.cit., p. 22.
[171] Council Decision of 17 October 2000, op.cit.

FIU.NET initiative led by the Dutch Ministry of Security and the Dutch FIU, joined in 2002 by FIUs in France, Italy, Luxembourg, and the United Kingdom. FIU.NET was launched as a pilot program in 2004 with the financial support of the European Commission and has been officially operational since 2007.[172] It is now accessible to the twenty-eight member states. FIU.NET is promoted as 'a decentralised and sophisticated computer network supporting the FIUs in the European Union in their fight against money laundering and the financing of terrorism'.[173] Since 2004, it has been governed mainly by a board of FIU partners with several meetings a year to set policy rules and establish priorities. Until the end of 2015 the budget of the FIU.NET depended on European Commission grants (95 per cent of its budget) and FIUs financial contribution. Since then, maintenance of the network has been integrated into Europol's budget.[174]

Although Egmont Secure Web (ESW) and FIU.NET are based on the same goal of information sharing between financial intelligence units, there are a number of differences between them.

- First, 152 FIUs around the world can use the Egmont secure web while the FIU.NET is restricted to EU member states only, with potential extension to other European countries such as Iceland and Norway in the near future.

- Second, on the technological side, the sophistication of FIU.NET compared to the Egmont Secure Web is largely acknowledged within the EU and by Egmont Group representatives, especially with regard to easier retrieval of data that can be directly integrated into FIUs databases.[175] 'The ESW is a technology of the 20th century, a bit old and it would be helpful to change the current query form for something more dynamic or automated for data retrieval. The ways of sharing intelligence at the international level with Microsoft Word documents … We are no longer convinced'.[176]

- Third, the sophistication of FIU.NET compared to the Egmont Secure Web is also coupled with the possibility of multilateral exchanges. The Egmont Secure Web and FIU.NET both allow bilateral exchanges between financial intelligence units but only FIU.NET really permits multilateral operational cooperation. It allows FIUs to exchange information bilaterally, multilaterally, or even 'in full' with all connected counterparts, from 'known/unknown requests' to 'case files'. If the response to an FIU's request regarding whether an individual or organization is known or unknown is positive, it can move to what is called the case file approach, providing further details and justifications to obtain information from the other FIU(s). Taking a case-centric view, the FIU can then link different

[172] Carlisle D., *Making Information Flow. Instruments and Innovations for Enhancing Financial Intelligence*, RUSI, occasional paper, 2016.
[173] Europol, Financial Intelligence Units – FIU.NET, available on the Europol website.
[174] Ibid.
[175] European Commission, 25th Meeting of the EU FIUs Platform, 1st June 2015, p.8; Interview FIU, 2016.
[176] Interview FIU, 2016.

entities to its case file. The case file is like a box and inside the box the FIU can put information on a person, ID documents linked to a person, a company, or an account, and transactions linked to the account without needing to re-send the message via FIU.NET:

> 'You can share different elements in that case with different FIUs depending on relevance. For instance, you have a person in Italy who you are interested in because of a suspicious transaction report (STR) you have received. You send a known/unknown to, let's say, the UK, because you see that the transaction is going there. They [the UK FIU officials] reply that the person is known and you start building a case file and it becomes a joined case file, with user protocols that state precisely how it can be used'.[177]

In 2012 FIU.NET introduced 'Ma3tch technology' as an option to allow encrypted data exchange and a Ma3tch-engaged pilot was launched in 2013. The 'a3' stands for autonomous, anonymous, and analysis. FIUs have a number of option available to them for using the Ma3tch process, including sending simple 'know/unknown' or 'hit/no hit' requests to one or several counterparts. To do this, the FIU translates the subject (usually individuals) under examination into an anonymised entity (e.g., a 'filter') and shares the result with one or several selected FIUs through FIU.NET to determine if there are any positive matches. Such requests work only for names and dates of birth according to the director of the Dutch FIU, who insists on the 'anonymous' and 'autonomous' dimension of the analysis through the Ma3tch process :

> 'As a simplified example, an information resource contains: Philip Tattaglia (12/28/16), Luka Brasi (3/13/26), Johnny Fontane (10/7/27). The anonymization algorithm minimizes these 3 individual records into a single combined anonymous 4-character fuzzy logic data structure: 'tnUG'. This 4-character code captures the 'characteristics' of the combined original sensitive information, making it impossible to recover the individual records. The extreme data minimization enables (configurable) false positives (collisions) that enhance anonymity. In addition, the information owner controls which data are included in the filter, and if, when, and where filters are shared (multiple filters can be created for a single dataset, for example with lower accuracy for sensitive data). Other parties that receive the filter can use it to ma3tch local sensitive data against the anonymized data structure 'tnUG' without knowing the underlying data. … Positive hits are optionally or automatically followed up for (anonymous) validation, compliance check, and/or a fully detailed 'need to know' information exchange'.[178]

More generally, the underlying logic of the Ma3tch functionality encourages automated cross-matching practices between EU FIUs' filters. Personal data is normally shared only if there is a hit:

[177] Interview FIU, 2017.
[178] Kroon U., 'Ma3tch: Privacy AND Knowledge. Dynamic Networked Collective Intelligence', IEEE International Conference on Big Data, 2013.

> 'Some of the FIUs put their entire suspicious transactions reports' database into a match filter which batches the names and dates of birth and encrypts them. You share that filter with another FIU or with all of the FIUs and depending on what they put into their filters it will match and tell you if any of those names are known by another FIU. So it is effectively doing the 'known/unknown' but in mass'.[179]

The automated logic of cross matching is thus available via FIU.NET but is far from being part of FIUs' daily routine. Potential increase of use depends on the creation and sharing of larger encrypted data-sets (filters) between FIUs. According to its supporters, 'automated cross matching means that I make available a data-set and FIU.NET tells me that persons 1, 2, and 3 are also targeted by an STR in the Czech Republic, for instance. This is central because I will make requests for information to places I would have never thought of'.[180] Other FIU officials remain reluctant about this possible evolution of the European computer network, in particular because they consider that the nature of the fairly new link between FIU.NET and Europol is not sufficiently clear. Issues concerning information security, confidence, and data processing are regularly expressed by some FIUs that fear extensive policiarisation and judicialisation of financial intelligence and FIU.NET in connection with Europol.

Matching subjects through FIU.NET is also performed with connected data-sets other than FIU filters, starting with commercial databases. Europol currently provides open source tools such as World-Check, a data company that is now part of Thompson Reuters. As described by Marieke de Goede and Gavin Sullivan, this company 'collects, collates and sells listing information and due diligence compliance solutions to clients within (and beyond) the financial industries. Its main rationale is to compile into one master database the more than 400 sanctions lists, counterterrorism watch lists, regulatory and law enforcement lists in existence worldwide … However, World-Check does not only compile pre-existing list entries. It also ''value-adds'' by adding their own nominations of heightened risk banking clients – including, for example, persons indicted for fraud or terrorism and persons otherwise publicly associated with, but not necessarily convicted of, such offenses. Inclusion in the World-Check database is based on open-source information research performed by multi-lingual teams around the world. In this process, web-based sources, public indictment records, newspaper articles and other publicly available information of very diverse quality – including blogs, news sites and online photographs – are reviewed for possible connections to ''financial crime, narcotics trafficking, money laundering, gambling and internet fraud [and] those types of things.'' Protocols for database inclusion are recognised to be subjective and listing categories are flexible and overlapping'.[181] Subscriptions to World-Check can cost up to 1 million euros annually. For the FIU.NET, Europol officers put WorldCheck list entries into a filter

[179] Interview FIU, 2016.
[180] Interview FIU, 2017.
[181] de Goede M., and Sullivan G., 'The Politics of Security Lists', *Environment and Planning D - Society & Space*, Vol. 34, No. 1, 2016, pp. 67-88. On the questionable maintenance of information accuracy for commercial data-bases such as World-Check, see also Amicelle A. and Favarel-Garrigues G., 'Financial Surveillance: Who Cares?', *Journal of Cultural Economy*, Vol. 5, No. 1, pp. 105-124.

accessible to FIUs. When an FIU creates a case file or a filter, the Europol filter is supposed to alert them if there is a match with sanctions lists, lists of politically exposed persons, and so on.

Finally, for the last few years FIU.NET has also included a cross-border reporting function in connection with a pilot project with FIU Luxembourg under the pressure from other European FIUs. This project is associated with the ambiguous situation of several reporting entities registered and established in Luxembourg: PayPal, Amazon, and IPay. While these business companies operate commercially largely in other EU Member States, they do not have the same legal presence in those states as compared to Luxembourg, given that their registered offices in Europe are limited to this country. Consequently, they are legally obliged to send their suspicious transactions reports (STRs) to the Luxembourg FIU, even if the transactions are related to other member states such as France and UK. The pilot project was launched to require FIU Luxembourg to share spontaneously 'all STRs filed by Amazon, Paypal and Ipay with other national FIUs via the FIU.NET Crossborder system. 90 percent of cross-border reports were transferred to another FIU within 24 hours and 99 percent within 3 days'.[182] **Following this logic, the fourth EU Directive (article 53.1) now mentions that when an EU FIU receives a report that concerns another member state, 'it shall promptly forward it to the FIU of that Member State'**.

Other recognised cooperation channels

Certain FIUs also use other channels – secure e-mails or even fax messages – to exchange information with the minority of their counterparts that are neither members of the Egmont Group nor FIU.NET.

2.2. Financial intelligence cooperation in face of obstacles

> 'We try to organise ourselves to better understand how exchanges work with each FIU and to understand how another FIU is organised. Because when, after a request, we are told "I don't know !", we have to determine is there no information because the other FIU has looked for it and did not find anything, or because it did not look for it, or because it could not have looked for it, or because it looked for it but did not have the resources to really look for it ?'.[183]

Cooperation practices between FIUs regularly come under fire in relation to a series of obstacles, including some that are particularly problematic in tax-related cases. This is due either to a lack of capacity to respond to a request, to the low level of spontaneous dissemination, or ultimately to abusive restrictions on the use of information.

[182] European Commission, 26th Meeting of the EU FIUs Platform, 16 October 2015.
[183] Interview FIU, 2016.

(Lack of) capacity to respond to FIU requests

First, a number of FIUs have been criticised for their inability to obtain information from 'obliged entities' (mainly financial institutions) following requests from foreign counterparts:

General inability to request information from reporting entities: Some FIUs cannot request and obtain additional information from reporting entities, even after the submission of one or several related suspicious transactions reports (STRs). For example, the 2016 FATF evaluation of Canada notes that 'Fintrac may request the person or entity that filed an STR to correct or complete its report when there are quality issues such as errors or missing information, but not in other instances where this would be needed to perform its functions properly. According to the authorities, Canada's constitutional framework prohibits Fintrac from requesting additional information from reporting entities'.[184]

Conditional (in)ability to obtain information from reporting entities: Other FIUs cannot request information from reporting entities on behalf of foreign FIUs without related suspicious transactions in their database. In other words, a prior report on client or transaction 'X' from bank 'Y' in the database of FIU 'A' is a pre-condition for cooperation with FIU 'B' that requests information on client or transaction 'X' from bank 'Y'. FIU 'A' will not contact bank 'Y' for further details without such a prior report. The recent FATF evaluation of Switzerland notes that 'an important limitation in the effectiveness of international co-operation results from MROS not having the power, in the case of a foreign request, to request information from a financial intermediary unless the latter has previously submitted a suspicious transactions report or has a link with a suspicious transaction report received by MROS. This limitation, which was also raised by numerous delegations who shared their experience in co-operating with Switzerland, appears particularly important in the Swiss context'.[185] By contrast, there are also concerns that FIUs' request for information from obliged entities on behalf of a foreign counterpart may compromise the confidentiality of the foreign investigation. 'Information security is sometimes a cause for concern when our counterparts (foreign FIUs) need to contact a reporting entity to obtain information. They contact the reporting entity and say: 'we are looking for the bank accounts of Mr X'. And the banker or the accountant or the lawyer might contact Mr. X. From experience, there is no guarantee that this will not happen'.[186]

Inability to get access to beneficial ownership information. The lack of useful information about beneficial ownership by legal persons and arrangements established in another country is widely recognised as a critical issue. In accordance

[184] Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, 2016, op.cit., p. 184.
[185] Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016, op.cit., p. 150.
[186] Interview FIU, 2016.

with the international standards against money laundering and terrorist financing, the notion of 'beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person'.[187] The fourth EU Directive draws on the FATF definition, with further details about the meaning of beneficial owner in the case of corporate entities and trusts. In light of transnational financial operations, especially for tax-related requests, FIUs often depend on beneficial ownership information available in another country. Parties involved in targeted transactions often cannot be identified without access to accurate and reliable information because of the lack of transparency in legal arrangements.

> 'This is at the heart of the Panama Papers! What do I see as the core issue of the Panama Papers? Yes there are suspicious financial flows but the main issue is to show that shell companies are used to conceal these financial flows … Because the financial flows – we see them! We can see them! But we cannot see who is the benefical owner and what is the economic reason behind the legal arrangement. There are structures of opacity that do not permit us to know who the operator really is'.[188]

Without access to information on beneficial owners and control of legal persons, it is not possible to match financial traces to an identity. The misuse of corporate entities for illicit activities was largely acknowledged before the Panama Papers[189], and frequently recalled in the aftermath of the scandal, but **the identification of beneficial owners through FIU-to-FIU cooperation is still a predominant concern among practitioners**. Along these lines, law enforcement agencies in Canada recently stated that 'they encounter difficulties in identifying beneficial owners of Canadian companies owned by entities established abroad, particularly in the Caribbean, Middle East, and Asia. […] Also, in a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for law enforcement agencies to identify the beneficial owners'.[190]

Lack of (access to) databases: According to the FIUs we examined, one of the main issues is related to the ability to get access to police databases in order to respond to foreign FIUs requests. The lack of access to such databases is presented as an 'international handicap'. However, the issue of direct or indirect access to national databases is not limited to police information, particularly for tax-related money laundering. In this regard, FATF's mutual evaluation of Canada suggests that it should 'consider granting Fintrac access to information collected by the CRA [Canada Revenu Agency] for the purposes of its analysis of STRs'.[191] **Current discussions in the EU are not restricted to access to existing national databases but also focus on the systematic creation of new**

[187] Financial Action Task Force (FATF), Recommendations, 2012, op.cit.
[188] Interview FIU, 2016.
[189] Riccardi M., and Savona E. U., *The identification of beneficial owners in the fight against money laundering*, Trento, Transcrime - Universitàdegli Studi di Trento, 2013.
[190] Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, 2016, op.cit., p. 103.
[191] Ibid., p. 36.

databases, such as the central registers for all holders of bank accounts – registeries that exist in some member states, including in France, which has FICOBA (*fichier national des comptes bancaires et assimilés*). Every bank account, savings account, and trading account opened in France is listed in FICOBA. The register contains information on the account's opening, modification, and closing. This includes: 1) the account owner's name, date and place of birth, and address (in the case of natural persons, the related code, names, legal form and address are registered); 2) the name and address of the financial institution holding the account; and 3) further details about the type and nature of the account as well as the account number. Financial institutions must provide and update this information, which is stored in the national register throughout the entire life cyle of an account and for ten years after the account is closed. In 2016, 80,000,000 individuals were registered in FICOBA, which processes 100 million account reports (opening, modification, closing) annually.[192] FICOBA is directly accessible to officials from financial administrations (tax administration, customs, Tracfin, and so on), the securities regulator, social security agencies, banks, judges, and criminal investigation officers, the 'huissiers de justice', and notaries in charge of a succession. In relation to financial intelligence, the promoted added-value relies on the ability to determine if a person related to a suspicious transaction report (STR) has more than one account in more than one bank. FIUs without such central registers are criticised for 'insufficient capacity' to map the possible multiple accounts held by an individual in various financial institutions. In this respect, the fourth EU Directive mentions that 'in accordance with Union and national law, Member States **could, for instance, consider putting in place systems of banking registries** or electronic data retrieval systems which would provide FIUs with access to information on bank accounts without prejudice to judicial authorisation where applicable'.[193] The creation of such national registers is thus not mandatory in the fourth directive.

Timeliness issues and lack of reciprocity: While responsivess to FIU requests may vary from one country to another, it may also vary from one type of illicit flow to another:

> 'Of course there have been some improvements but the fact remains that there are problems with some countries, including the largest ones such as the US, if we do not talk about terrorism. Most of the time, the answer is limited to 'known /unkown''.[194]

In the transnational field of financial intelligence, as elsewhere, national prioritisation matters and the focus on counter-terrorism has not necessarily had a positive impact on the fight against financial crime in general. **Moreover, response time is still a concern for all the FIUs we examined, which sometimes receive the requested information but several months too late to be relevant. Response time and number of responses from an FIU, however, deserve very careful assessment. An FIU may have good statistics on timing and number of exchanges but these results may include a wide range of quick**

[192] Commission Nationales de l'Informatique et des Libertés (CNIL), FICOBA : Fichier national des comptes bancaires et assimilés, 2016.
[193] Directive 2015/849, op.cit.
[194] Interview FIU, 2017.

responses such as, 'we are not in a position to reply'. It can also mask a lack of reciprocity that is a shared concern among FIUs:

> 'There is an issue of real importance in international cooperation: reciprocity. We have a problem in terms of reciprocity. Most of the time we do not succeed to obtain the same thing as what we provide'.[195]

(Lack of) spontaneous dissemination and 'abusive' restriction

> 'I have had some clashes with my analysts who used to tell me: 'Suspicious Transactions Reports - STRs not relevant, no link with our country' while for me it was critical to spontaneously send these STRs to foreign FIUs'.[196]

This quote illustrates current discussions regarding spontaneous dissemination. **Spontaneous dissemination is encouraged in international standards but is far from being the norm in practice.** While some FIU officials would like to see increased dissemination, others support an automatic information exchange every time an STR has an 'international' element. This support is especially explicit in the EU, where the internal market facilitates opening a bank account in another member state than the country of residence.

Finally, the ways in which the exchanged information can be used can also be a matter of significant tension between the FIU making the request and the FIU receiving the request, in particular on tax issues:

> 'Actually, when we make a request for information to this European FIU on tax-related money laundering, there is no problem with getting the information, they are doing their job. They reply in a timely manner but … They always write at the end: 'You cannot use this information for tax purposes'. It is too bad because it is exactly for tax purposes that we made the request! How do you want to exchange information post–Panama Papers? All the difficulties involved in getting access to the information and then at the end you receive the information with this kind of restriction!'.[197]

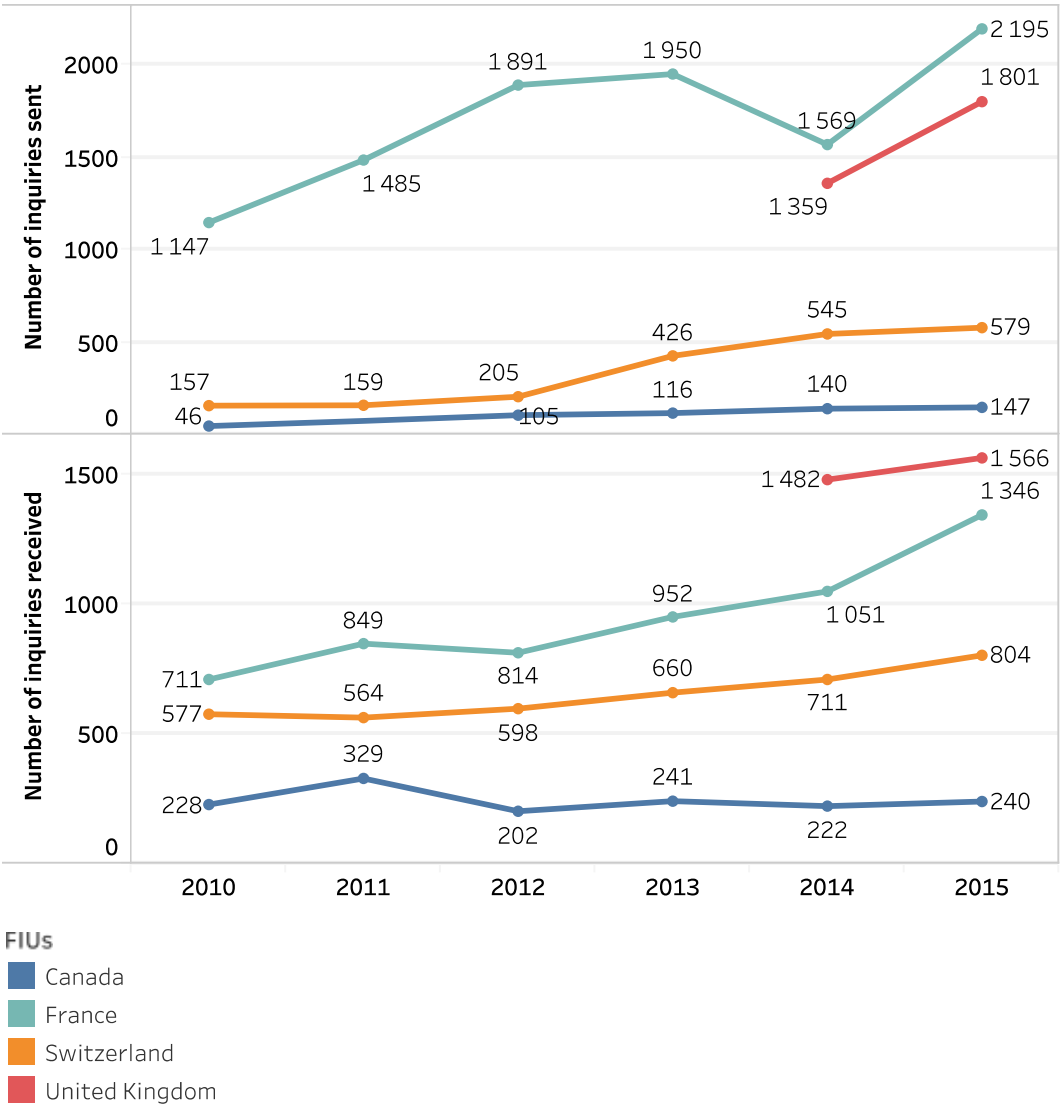
As already mentioned, **international standards of information exchange require that any further use of information must be authorised by the FIU providing the information** (Cf. 2.1. the rules for information dissemination include three main options or thresholds)**. The argument of abusive use of this basic principle in tax-related issues is debated on a daily basis in the field of financial intelligence, in the EU, and abroad.**

[195] Interview FIU, 2016.
[196] Interview FIU, 2017.
[197] Interview FIU, 2016.

2.3. Information sharing in numbers

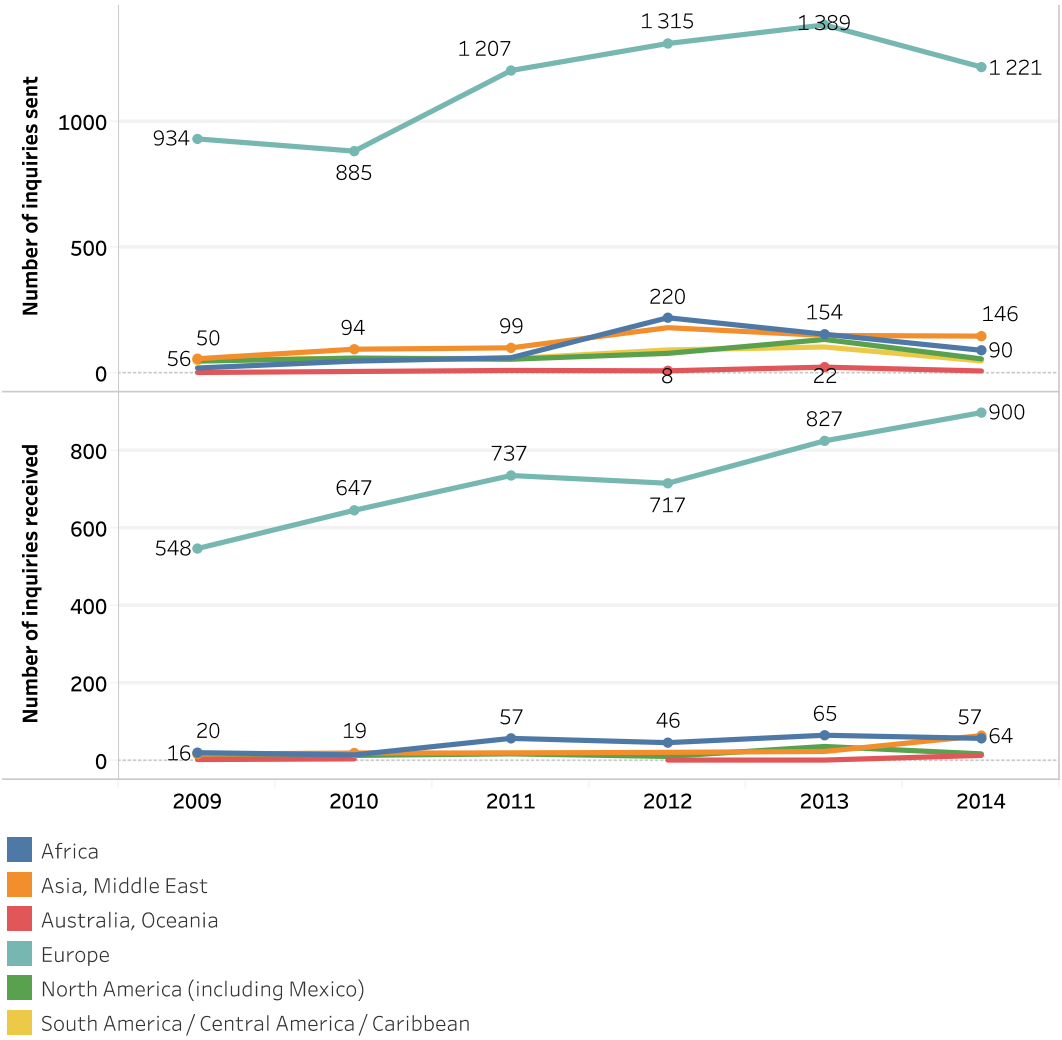
Chart 10 FIUs in Canada, France, Switzerland and the UK: Inquiries received/sent

		2010	2011	2012	2013	2014	2015
Canada's Fintrac	Inquiries received	228	329	202	241	222	240
	Inquiries sent	46	74	105	116	140	147
France's Tracfin	Inquiries received	711	849	814	952	1 051	1 346
	Inquiries sent	1 147	1 485	1 891	1 950	1 569	2 195
Switzerland's MROS	Inquiries received	577	564	598	660	711	804
	Inquiries sent	157	159	205	426	545	579
United Kingdom's NCA	Inquiries received					1 482	1 566
	Inquiries sent					1 359	1 801



- Both UK and France's FIUs receive and send more inquiries than MROS (Swiss FIU) and Fintrac (in Canada) even if the number of inquiries sent to MROS is high, especially regarding the inquiries sent compared to the number of STRs received by the Swiss FIU annually (In 2015, 579 inquiries compared to 2,367 STRs). The ratio can be largely explained by MROS's dependence on foreign information in relation to Switzerland's position as a major financial centre. The relatively low number of inquiries to Fintrac can be partly explained by the collection of monetary threshold-based reports such as tens of millions of electronic funds transfer reports annually.

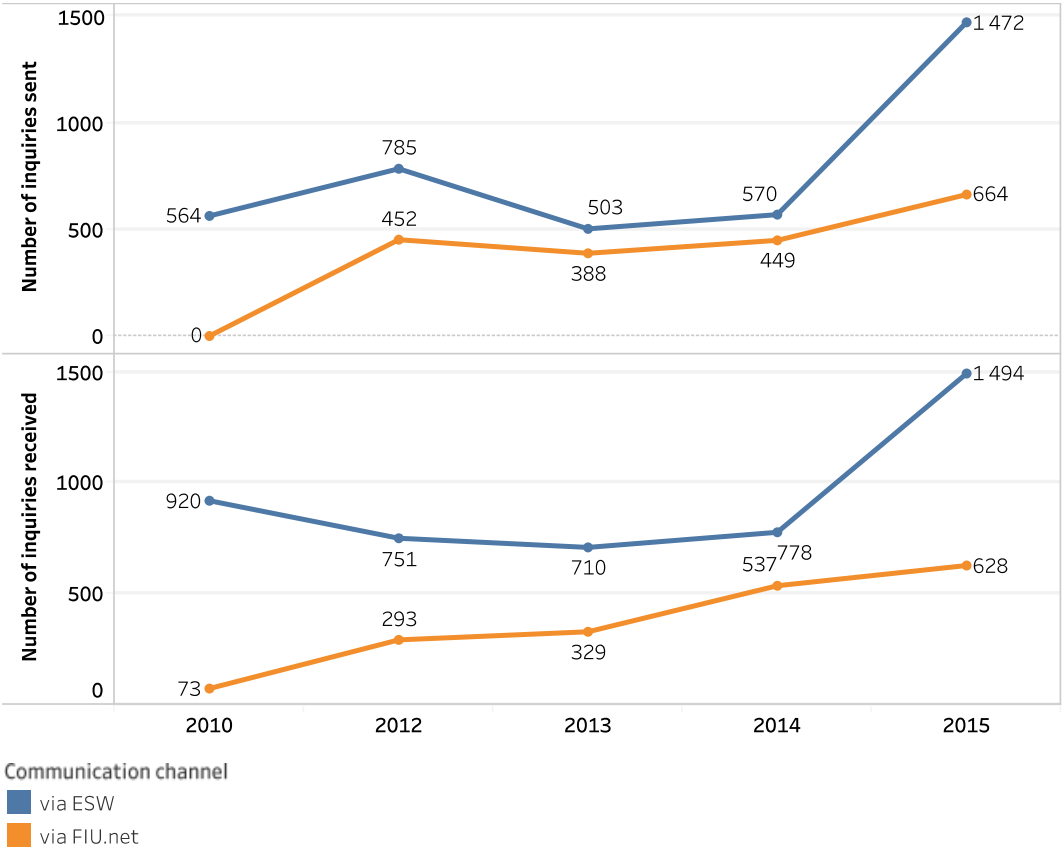
Chart 11 France's FIU: information exchanged



		2009	2010	2011	2012	2013	2014	Total
Europe	Inquiries received	548	647	737	717	827	900	4'376
	Inquiries sent	934	885	1 207	1 315	1 389	1 221	6 951
Asia, Middle East	Inquiries received	16	19	19	21	23	64	162
	Inquiries sent	56	94	99	180	149	146	724
Africa	Inquiries received	20	14	57	46	65	57	259
	Inquiries sent	19	46	60	220	154	90	589
North America (including Mexico)	Inquiries received	8	13	17	10	36	17	101
	Inquiries sent	46	58	54	77	133	55	423
South America / Central America / Caribbean	Inquiries received	15	14	19	19			67
	Inquiries sent	50	59	56	91	103	47	406
Australia, Oceania	Inquiries received	2	4		1	1	13	21
	Inquiries sent	1	5	9	8	22	7	52

- The vast majority of inquiries received by Tracfin (France's FIU) are from European Partners (both EU and non EU). Those from the EU are received largely via FIU.NET; around 60 percent of all inquiries received by Tracfin come from EU member states. There is almost no overlap between this cooperation channel and Egmont Secure Web (ESW). In other words, these channels of cooperation are complementary/compatible.

Chart 12 UK FIU: information exchanged



		2010	2012	2013	2014	2015	Total
via ESW	Inquiries received	920	751	710	778	1 494	4 653
	Inquiries sent	564	785	503	570	1 472	3 894
via FIU.net	Inquiries received	73	293	329	537	628	1 860
	Inquiries sent	0	452	388	449	664	1 953

- In contrast to Tracfin (France's FIU), the UK FIU seems to either receive and send a majority of extra-European Union inquiries or facing a problem of complementarity between the FIU.NET and the Egmont Secure Web (ESW).

Conclusion

Throughout our fieldwork on FIUs in Canada, France, Switzerland, and UK, we have traced the current dynamic in the fight against dirty money, the varying characteristics of financial intelligence and FIUs, and the state of play and problems in relation to transnational cooperation channels. Rather than attempt to summarise all the results of this study, we conclude with a discussion of two critical issues in the field of financial intelligence.

First, 'money laundering is the process of making illegally gained proceeds ('dirty money') appear legal ('clean')'.[198] This clear and straightforward definition of money laundering is now available on the website of the US FIU but could have been written, published, and widely accepted in 1990. Meanwhile, the scope of the concept of 'dirty money' has been radically extended from the proceeds of drug trafficking to illicit flows of money in general, including, after years of explicit exclusion, tax evasion. The striking definitional malleability of 'dirty money' has largely transformed financial intelligence practices, starting with a focus on both the origin and destination of money. Reporting entities' obligations and FIUs' powers have continued to increase significantly in the period considered here. The tremendous development of financial intelligence capabilities has been justified largely in the name of counter-terrorism, particularly in the EU following the adoption of the second Directive in December 2001. This prioritisation of terrorist financing is very often associated with an increased effort in the fight against financial crime as a whole. However, our fieldwork found much more mitigated results with regard to 'mutual benefits'. More generally, while international norms and EU legislation now officially cover all forms of financial flows, the differential management of predicate offences deserves further analysis.

Second, as the meaning of 'dirty money' has changed since the early 1990s, what an FIU is and what it does has evolved over time but still varies from one country to another, including between EU Member States. In other words, the expression 'dirty money' now tends to be increasingly understood in the same way in countries such as Canada, France, Switzerland, and the UK but this is far from being the case for 'financial intelligence unit'. Given the many differences between national agencies and their impact on international cooperation, critical discussions of FIUs should go beyond a focus on the four traditional models (administrative, hybrid, judicial, law-enforcement): this classic distinction between FIUs remains important for identifying and understanding a number of national variations and international tensions but these are certainly not the only issues at stake. **Other typologies are very useful in understanding the daily practices of FIUs, such as the distinction between the data-repository model (as in the UK, for instance) and the analytic model (France, Canada and Switzerland)**. Focusing only on the traditional models reifies differences between models and masks numerous differences in degree – amounting almost to differences in kind – between FIUs in the same model.

[198] FinCEN, History of Anti-Money Laundering Laws, 2017.

With regard to information collection, the first core function of an FIU according to the traditional model, financial transaction reports may vary from an exclusive collection of disclosures based on suspicion (as in Switzerland and UK) to monetary threshold-based disclosures (Canada and France). Furthermore, the core definition of suspicion and reports based on suspicion also varies from one country to another: 'well-founded suspicion' (Switzerland), 'unqualified suspicion' (France and UK), and 'reasonable suspicion' (Canada, France, and UK also) as well as 'suspicious transaction report' (Canada) and 'suspicious activity report' (France, Switzerland, and UK). **Those semantic variations have practical effects that deserve further attention**. With regard to information analysis, the second core function, **both the ability to obtain additional information from reporting entities and to access national databases or central registers varies from FIU to FIU**, regardless of the category of the FIU within the model, with large differences between Canada, France, and Switzerland, for instance.

Finally, with regard to information dissemination, the third core function, **both the rationale for dissemination (proactive disclosure vs reactive disclosure) as well as the range and nature of national partners changes significantly changes according to country**. National differences in information collection, analysis, and dissemination reflect a variety of financial intelligence uses and purposes as well as the roles, powers, and responsibilities associated with FIUs.

References

EU DOCUMENTS

Mapping exercise and gap analysis on FIUs powers and obstacles for obtaining and exchanging information, Report prepared for the EU FIUs Platform, December 2016 (led by FIU Italy - *Unità di Informazione Finanziaria per l'Italia* - UIF)

Proposal for a Directive on countering money laundering by criminal law, Brussels, 21.12.2016 COM(2016) 826 final

Proposal for a Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Strasbourg, 5.7.2016, COM(2016) 450 final

European Commission, 26th Meeting of the EU FIUs Platform, 16 October 2015

European Commission, 25th Meeting of the EU FIUs Platform, 1st June 2015

Europol, Financial Intelligence Units – FIU.NET

Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

EU Regulation (EC) 1889/2005 on controls on cash entering or leaving the Community

Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information

Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

INTERNATIONAL ORGANISATION SOURCES

Egmont Group of FIUs, Financial Intelligence Units, 2017

Egmont Group of FIUs, Benefits of Egmont Group Membership, 2017

Egmont Group of FIUs, Principles for information exchange between FIUs, June 2013

Egmont Group of FIUs, Charter, July 2013

Egmont Group of FIUs, Operational Guidance for FIU Activities and the Exchange of Information, July 2013 (revised June 2014)

Financial Action Task Force (FATF), Mutual Evaluation Report of Switzerland, 2016

Financial Action Task Force (FATF), Mutual Evaluation Report of Canada, 2016

Financial Action Task Force (FATF), Recommendations, 2012

Financial Action Task Force (FATF), Recommendations, 2003

Financial Action Task Force (FATF), Recommendations, 1996

Financial Action Task Force (FATF), Annual Report, 1994

Financial Action Task Force (FATF), Annual Report, 1992

Financial Action Task Force (FATF), Recommendations, 1990

International Monetary Fund, *Financial Intelligence Units: An Overview*, 2004

Organisation for Economic Co-operation and Development (OECD), *Improving co-operation between tax and anti-money laundering authorities. Access by tax administrations to information held by financial intelligence units for criminal and civil purposes*, September 2015

OTHER OFFICIAL SOURCES

Bamford, J., *Privacy and data protection: Are they casualties in the fight against crime?* London, Information Commissioner's Office, 2012.

Canada Revenue Agency (CRA), Cracking down on tax evasion and avoidance, 2016

CNIL, FICOBA : Fichier national des comptes bancaires et assimilés, 2016

Collovà C., *Prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, EPRS, PE 587.354, 2016

Department of Justice and Equality of Ireland, Anti-Money Laundering Compliance Unit, Statistics Report, 2012

Fedpol, Blanchiment d'argent - Jugements prononcés en Suisse en matière de blanchiment d'argent, Bern, Publication de la Police judiciaire fédérale PJF, fedpol, 2014

Financial Conduct Authority (FCA), De-risking: Managing Money-Laundering Risk, 2016

FinCEN, History of Anti-Money Laundering Laws, 2017

House of Lords. European Union Committee. *Money Laundering: Data protection for suspicious activity reports*, London, United Kingdom Parliament, 2011

House of Lords. European Union Committee. 19th Report of Session 2008-09: Money laundering and the financing of terrorism. Volume II : Evidence, London, The Stationery Office, 2009

Kroon U., 'Ma3tch: Privacy AND Knowledge. Dynamic Networked Collective Intelligence', IEEE International Conference on Big Data, 2013

Fintrac, Annual Report, 2016

MROS, Annual Report, 2016

MROS, Annual Report, 2014

MROS, Annual Report, 2013

MROS, Annual Report, 2012

NCA, SARs Annual Report, 2015

Tracfin, Annual Report, 2016

Tracfin, Press Release: Tracfin présente son rapport annuel - Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2015, 2016

Tracfin, Annual Report, 2015, p. 8

Tracfin, Annual Report, 2011

Tracfin, Annual Report, 2008

United State General Accounting Office - GAO, Statement submitted to the Subcommittee on General Oversight and Investigations, Committee on Banking and Financial Services, House of Representatives, *FinCen's Law enforcement Support, Regulatory, and International Roles*, 1998, GAO/T-GDD-98-83

Van Ballegooij W. and Zandstra T., *The Cost of Non-Europe in the area of Organised Crime and Corruption*, PE 579.318, 2016

ACADEMIC SOURCES

Amicelle A., *Suspicion in the Making: Everyday Policing against Money Laundering and Terrorist Financing in Canada*, TSAS report, forthcoming.

Amicelle A. and Jacobsen K.U., E., 'The Cross-Colonization of Finance and Security through Lists: Banking Policing in the UK and India', *Environment and Planning D: Society and Space*, Vol 34, No 1, pp. 89-106.

Amicelle A., 'Management of Tax Transgressions in France: a Foucauldian perspective', In J. van Herp, W. Huisman and G. Vande Walle (eds.), *The Routledge Handbook of White-Collar and Corporate Crime in Europe*, London, Routledge, 2015, pp. 379-398.

Amicelle A., 'Differential Management of Economic and Financial Illegalisms: Anti-Money Laundering and Tax Issues', *Penal field*, Vol 10, 2014, pp. 1-23.

Amicelle A., 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism. From Criticism to Imitation of Dataveillance', *CEPS Liberty and Security Series*, No 56, 2013, pp. 1-19.

Amicelle A. and Favarel-Garrigues, G., 'Financial Surveillance: Who Cares?', *Journal of Cultural Economy*, Vol. 5, No 1, 2012, pp. 105-124.

Amicelle A., 'Towards a 'New' Political Anatomy of Financial Surveillance', *Security Dialogue*, Vol 42, No 2, 2011, pp. 161-178.

Blum J., Levi M., Naylor, R., Williams, P., *Financial Havens, Banking Secrecy and Money Laundering*, United Nations Office for Drug Control and Crime Prevention, New York, 1998.

Carlisle D., *Making Information Flow. Instruments and Innovations for Enhancing Financial Intelligence*, RUSI, occasional paper, 2016.

de Goede M., and Sullivan G., 'The Politics of Security Lists', *Environment and Planning D - Society & Space*, Vol. 34, No. 1, 2016, pp. 67-88.

Favarel-Garrigues G., 'Domestic reformulation of the moral issues at stake in the drive against money laundering: the case of Russia', International Social Science Journal, Vol 57, No 185, 2005, pp. 529-540.

Favarel-Garrigues G., Godefroy T. & Lascoumes P., 'Reluctant partners? Banks in the fight against money laundering and terrorism financing in France', *Security Dialogue*, Vol 42, No 2, pp. 179-196.

Gold M., and Levi M., *Money laundering in the UK: An appraisal of suspicion-based reporting*, London, The Police Foundation and University of Wales, 1994, p. 89.

Helleiner E., 'State Power and the Regulation of Illicit Activity in Global Finance', In Andreas P., Friman R. (eds.), *The Illicit Global Economy and State Power*, Lanham Md, Rowman and Littlefield, 1999, pp. 53-89.

Helgesson K. S. and Mörth U., 'Involuntary Public Policy-making by For-Profit Professionals: European Lawyers on Anti-Money Laundering and Terrorism Financing', *Journal of Common Market Studies*, Vol. 54 (5), 2016, pp. 2216-2232.

Hibou B., *The Bureaucratization of the world in the neoliberal era: An international and comparative perspective*, New York, Palgrave Macmillan, 2015.

Mitsilegas V., 'New Forms of Transnational Policing : The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights', *Journal of Money Laundering Control*, Vol 3, No 2, 1999, pp.147-160 and Vol 3, No 3, 2000, pp. 250-259.

Palmieri R. and Rigotti E., 'Suspicion as an argumentative move. Semantic analysis of a pivotal concept in banks' *anti-money laundering* argumentative activities', *Journal of Argumentation in Context*, Vol. 3(3), 2014, pp. 287–321.

Project 'Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy - ECOLEF' (funded by the European Commission - DG Home Affairs, JLS/2009/ISEC/AG/087), Final Report, February 2013

Riccardi M. and Savona E. U., *The identification of beneficial owners in the fight against money laundering*, Trento, Transcrime - Universitàdegli Studi di Trento, 2013.

Scherrer A., G8 against transnational organised crime, Ashgate, 2009

Strange S., *Mad Money*, Manchester, Manchester University Press, 1998.

Woodiwiss M., 'Transnational organized crime: The strange career of an American concept', in Beare M. (ed.), *Transnational Organized Crime*, Ashgate, 2003;

MEDIA SOURCES

Boder W., 'La Finma veut changer la culture de la lutte contre le blanchiment d'argent', *Le Temps*, 2016

Financial intelligence units (FIUs) are the national structures responsible for the receipt, analysis and dissemination of financial information to combat money laundering and terrorist financing. Given the strong cross-border dimensions of money laundering, the exchange of information across FIUs is key to ensure illicit flows of money are properly detected and subsequently investigated by law enforcement authorities. This study aims to provide a better understanding of the current state of play in relation to the role, powers and activities of FIUs in fighting financial crime in general and tax crimes in particular, both at European and International level.

This is a publication of the Ex-Post Impact Assessment Unit
EPRS | European Parliamentary Research Service
European Parliament

PE 598.603
ISBN 978-92-846-0701-3
doi:10.2861/2427
QA-02-17-248-EN-N