ANNUAL ANALYSIS AND ACTIVITY REPORT 2013

TRACFIN

UNIT FOR INTELLIGENCE PROCESSING AND ACTION AGAINST ILLICIT FINANCIAL NETWORKS

CONTENTS

FOREWORD

In 2013, the combating of money laundering, terrorist financing and the fraudulent use of public funds were core priorities for the public authorities. Tracfin, which plays a central role in this fight, was directly affected by the changes made to the institutional framework in 2013.

Firstly, the law of 26 July 2013 on the separation and regulation of banking activities introduced major changes that have had a direct impact on the entities who are subject to the anti-money laundering and counter-terrorist financing system and report to Tracfin. The introduction of Systematic Information Disclosures (COSIs), alongside suspicious transaction reports, will result in some reporting entities systematically reporting certain transactions to Tracfin, based on objective criteria and thresholds. This measure, which covers fund transfers taking place when a payment is made in cash or a digital currency, will have its scope expanded to large cash transactions and some international transfers following an ongoing sector consultation process.

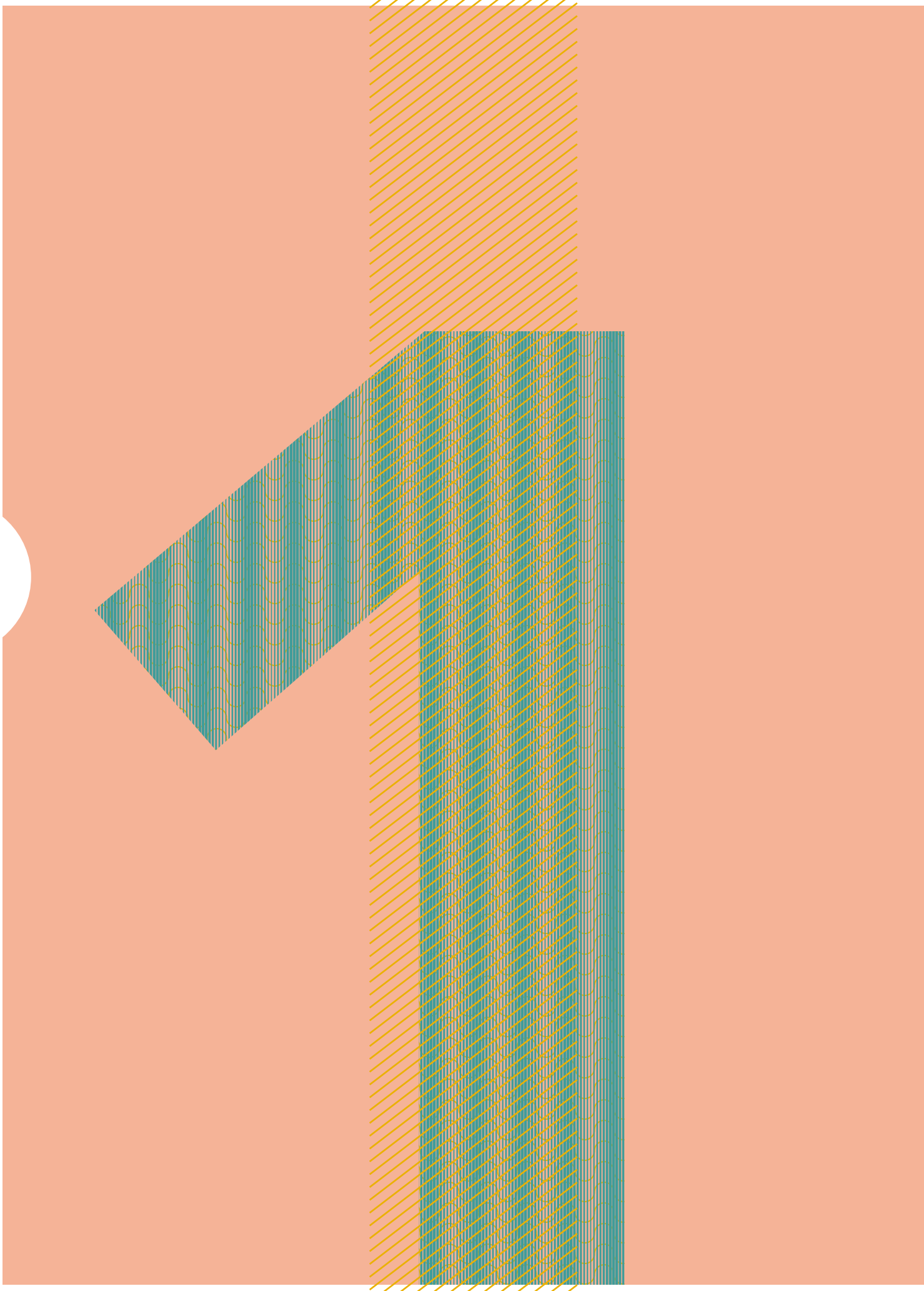
Secondly, law No. 2013-1117 of 6 December 2013 relating to the combating of tax fraud and serious economic and financial crime will have many consequences for Tracfin's activity. Aside from the provisions that it contains, which include a new definition of the offence of money laundering that should make it easier for the judicial authorities to process the reports sent to it by Tracfin, the passing of this law shows the public authorities' determination to ensure that they are able to combat any form of financial fraud more effectively, raising the standards for vigilance measures and reporting practices of entities subject to reporting obligations.

In addition to these changes, 2013 was a turning point for international cooperation. In keeping with the major changes underway regarding the lifting of banking secrecy and the cross-border traceability of financial flows, the number of reports shared between Tracfin and foreign FIUs has risen by more than 7%, as a result of the initiatives taken by France and the European Community to combat financial fraud. These initiatives are of course being extended within the framework of the negotiations on the fourth Anti-Money Laundering Directive and the revising of the Egmont Group's standards, in line with the new FATF rules.

Against this busy backdrop, Tracfin's workload grew considerably in 2013, with a 5% increase in the number of suspicious transaction reports received, a 25% rise in the analyses conducted by the team, and 10% growth in the ensuing referrals made based on these analyses. The different areas of Tracfin's activity have all at least doubled in volume over a five-year period.

These results could not have been achieved without the full confidence of our ministers, thanks to whom Tracfin's staffing levels and resources were increased despite strained public finances, and should be increased again in 2014. Most of all, however, I would like to offer my sincere thanks to all of the Unit's staff for their dedication, which has made this exceptional growth in activity possible, and for their loyalty, which has enabled the Unit to stay true to the French Republic's values in its work. The results of their efforts are presented below.

Jean-Baptiste Carpentier
Director of Tracfin



THE EFFECTIVENESS OF THE FRENCH ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING SYSTEM

It is vital that Tracfin receives high quality financial information to ensure the effectiveness of the anti-money laundering and counter-terrorist financing system. Analysing this information reveals new or evolving phenomena and any increase in the volume of suspicious transaction reports for a sector of activity, geographic zone or type of transaction.

In 2013, an example of this phenomenon is the increase of significant money laundering through the internet. Suspicious transaction reports (STRs) concerning individuals or legal entities in the IT sector rose. This rise is due to the growth in the digital economy and the development of cybercrime, as well as the use of new payment methods. A section is devoted to virtual currencies which, although they are a source of innovation, may also be contributing to the growth of electronic, disintermediated money-laundering techniques or be used for the informal transferring of money from one country to another. In 2013, Tracfin also noted the increased sophistication of money-laundering schemes relying on the use of collection accounts. In an international environment marked by the combating of tax evasion at the highest level, Tracfin also identified an increase in financial flows to tax havens. Many money-laundering schemes use legal entities with registered offices in countries with low taxes and limited transparency requirements to conceal the identity of the effective beneficiary or beneficiaries controlling financial flows. Given this state of affairs, the third consecutive annual fall in STRs concerning legal entities is a cause for concern.

RISK ANALYSIS TO INCREASE THE EFFECTIVENESS OF THE AML/CTF SYSTEM

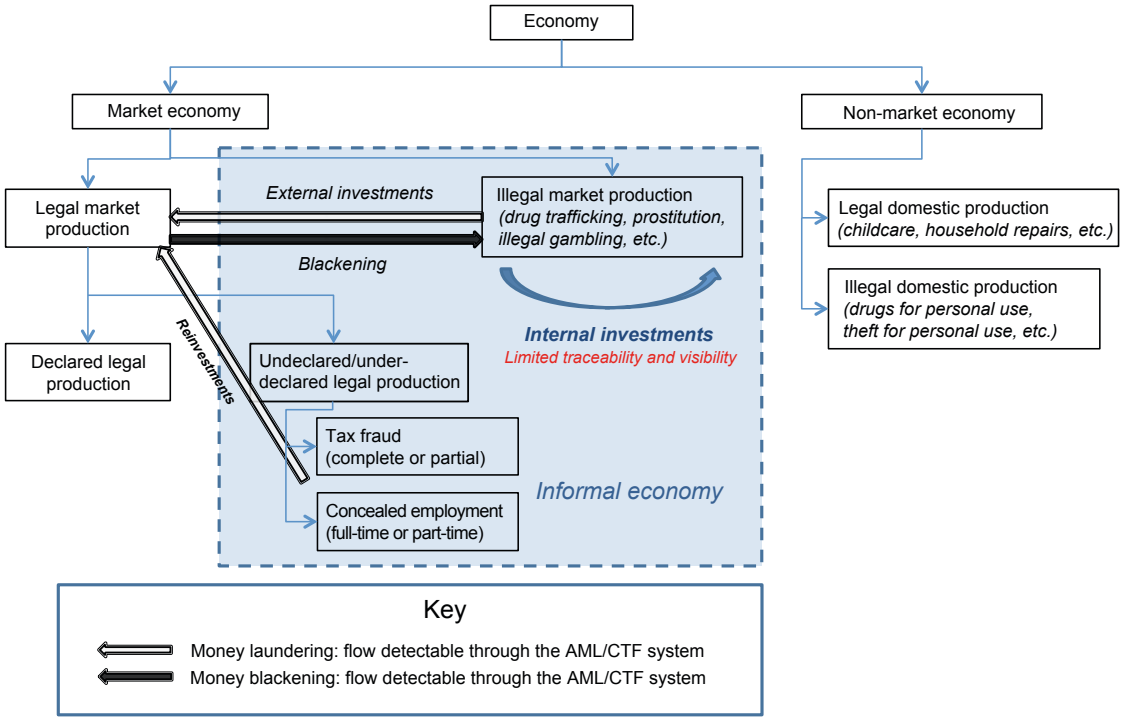
THE DETECTION OF ILLICIT FINANCIAL FLOWS

The informal economy consists of goods- and service-stemming from undeclared legal activities and illegal activities. Many methods have been developed to estimate the share of the informal economy in the GDP. These may be direct where they are based on surveys or tax audits, or indirect where they use various macroeconomic aggregates in a roundabout way. The results that these methods produce vary widely, however, and although the informal economy seems to account for a large percentage of the GDP, the precise figure is disputed.

The information received by a financial information unit, and particularly the STRs that account for 95% of the reports received by Tracfin, cannot be used as a basis for assessing the size of the informal economy.

The information received by a financial information unit, and particularly the STRs that account for 95% of the reports received by Tracfin, cannot be used as a basis for assessing the size of the informal economy. Although the data received by Tracfin cover an extremely broad scope, they cannot provide an overview and quantitative estimate of the informal economy in every sector of activity because of the disparities between the practices of reporting entities and their levels of vigilance. With a constant reporting scope, information can, however, be gathered about how the informal economy is structured and evolving by analysing STRs. Part of the transactions linked to the informal economy are in fact covered by suspicious transaction reports, but the proportion of the flows revealed this way cannot be quantified. When STRs are analysed, the possibility that the reports received may be affected by reporting biases that make them less representative must also be considered. The diagram below shows the boundaries of the informal economy along with the financial flows detectable through the French anti-money laundering and counter-terrorist financing system.

Diagram: The possibilities for the detection of financial flows linked to the informal economy



The flows shown above may exist at different levels, from local to international (moving of money from the informal economy of one country to the formal economy of another country).

As part of an active programme to combat fraud against publicfunds, in 2009 the scope of Tracfin's activities was extended to tax fraud, with the possibility of sharing information with the General Directorate of Public Finances (DGFiP). In 2012, a new law was passed authorising Tracfin to share information with social security bodies. An agreement governing information sharing between Tracfin, social entitlements bodies and the National Directorate for the Combating of Fraud (DNLF) has been signed as a result. STRs reporting tax and social security fraud are constantly increasing, consequently strengthening the Unit's close collaboration with the tax authorities and social entitlements bodies. A search for the STRs received since 2009 that expressly refer to tax fraud reveals a steady rise in the number of these reports. Since Tracfin's investigative scope was extended to tax fraud in accordance with the special conditions of the order of 30 January 2009, the proportion of tax-related STRs has increased four-fold in five years. Tracfin thus sends reports used by the tax authorities, which validate the information in tax terms and redirect the case as appropriate, for example proposing an external tax audit, proposing the opening of judicial proceedings or referring it to the inspection departments. From an anti-money laundering viewpoint, the consideration of tax fraud-related risks may also bring other predicate offences to light during the investigation process. In 2012, the Financial Action Task Force (FATF) therefore adopted new standards adding criminal tax offences to the list of the offences considered for anti-money laundering and counter-terrorist financing purposes. In France, law No. 2013-1117 of 6 December 2013 relating to the combating of tax fraud and serious economic and financial crime, published in the Journal Officiel of 7 December 2013, introduced new im-

plements in the fight against tax fraud and serious financial crime. Article 8 of this law (324-1-1 of the criminal code) introduces a presumption of money-laundering that can only be overturned if the person under suspicion proves the legal origin of the money or the transaction in question.

Internal investments within an illegal market production setup (see diagram) may come from organised criminal groups that wish to diversify their activities. The financial flows mainly take the form of cash and are therefore difficult to trace. Investments in legal market production originating from the informal economy are used to launder dirty money. On this basis, the French anti-money laundering and counter-terrorist financing system uncovers attempts to launder the financial flows generated by illegal market production.

Drug trafficking is the main source of revenue in the French informal economy. Narcotics are imported and sold in France by criminal groups of varying sizes, ranging from networks of dealers controlled by a local trafficker to transnational criminal networks. This trafficking generates cash that must be recycled in the legal economy. Tracfin exposes attempts to recycle this cash, whose complexity increases with the sophistication of the criminal network's structure. The case below shows the effectiveness of the AML/CTF system in its task of combating the infiltration of dirty money into the legal economy. Adding new types of reporting entities over time diversifies the sources of the STRs sent to Tracfin which, by cross-referencing them, recreates the different stages in the money-laundering process used.

Case study 1

Laundering gambling activities through the illicit proceeds of the sale of narcotics and attempt to integrate the funds through a life insurance policy

The following case illustrates a scheme to launder money from possible drug trafficking.

Profile of the participants:

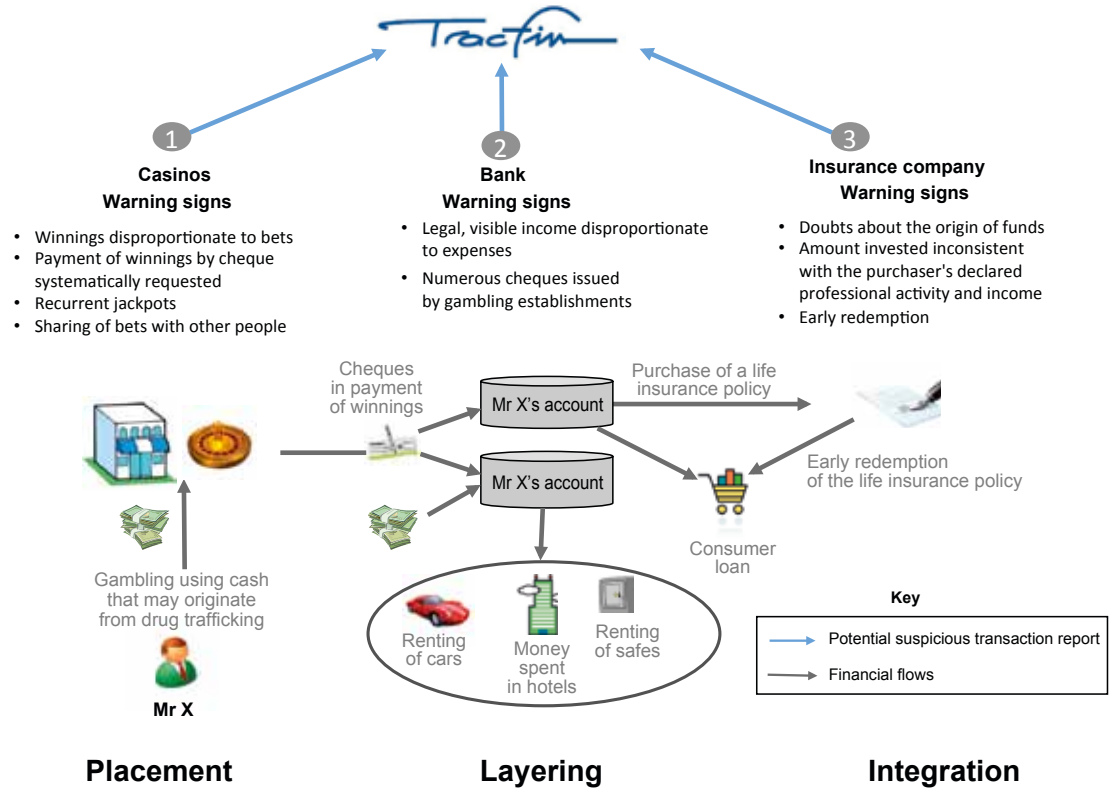
Individual: :

Mr X, who was known to the police

Flows leading to the suspicion of wrongdoing

Mr X, who was known to the police for his suspected involvement in a case of drug trafficking, visited casinos on multiple occasions. He was recorded on camera several times playing at table games and roulette, gambling cash sums amounting to several hundreds of thousands of euros in the space of a few months, which was at odds with his relatively modest official income. Mr X asked for his winnings to be paid by cheque. His winnings were slightly less than the amounts gambled. Even if Mr X were to regamble all of his winnings, the sums in question therefore appeared to be excessive given his declared financial position. Mr X's lifestyle also seemed to be extravagant in view of his apparent income. He bought many consumer goods, stayed at multiple hotels and leased a number of cars, while the amounts credited to his bank accounts mainly came from winnings paid by cheque and a few cash deposits. He also took out a consumer loan. Finally, he purchased a life insurance policy to try to integrate these funds, whose origin remains unknown, within the financial system. The policy was pledged and an early redemption request was made soon afterwards so as to pay back his consumer loan, before its due date.

Laundering diagram



A RISE IN SUSPICIOUS TRANSACTION REPORTS INVOLVING NEW PAYMENT METHODS

Tracfin assesses risks based on the information received from reporting entities and the cases investigated in 2013. Various criteria such as the transaction type, sector of activity or geographical zone of the flow form the basis for this analysis. The sectors of activity considered to be high risk by reporting entities, which are labour intensive sectors with a high business turnover rate, continue to account for a large share of STRs. Reports concerning the telecommunications sector grew in 2013, with many underlying types of schemes for laundering funds from undeclared work and tax fraud offences. In terms of B-to-B services, the number of reports concerning the IT sector rose sharply in 2013. This rise in suspicious transaction reports concerning IT entities reveals, amongst other things, the increase in the risks of the laundering of money generated from cybercrimes. Lastly, 2013 confirmed the growth in STRs, already seen in 2012, in the logistics, transport, medical and paramedical sectors (abuse of weakness by entities in this sector, scams linked to personal development training and training in alternative medicines, misuse of massage parlours and beauty salons, and so on).

The average amount per STR, in which several transactions may be consolidated over a wide range of time periods, is less than € 500,000 in 90% of cases, with a median amount of € 50,000. The anti-money laundering system's monitoring indicators suggest that these figures are fairly stable.

The growth, reported in 2012, in the share of the STRs received by Tracfin accounted for by financial flows in digital currencies, is continuing and gathering pace.

These reported amounts should not be taken at face value as the reporting entity is rarely aware of the entire scope of the financial transaction. Experience also shows that some activities, such as terrorist financing or drug trafficking, may be detected starting from very low, but repeated amounts. Cash transactions, cheques and transfers remain the most commonly reported payment methods.

The growth in suspicious transaction reports relating to financial flows in digital currencies

Reported in 2012, the growth, in the share of the STRs received by Tracfin accounted for by financial flows in digital currencies is continuing and gathering pace. This phenomenon is connected to the rise in the use of digital currencies in France. According to the Banque de France, more than 50 million payments were made in digital currencies in 2012, making France the fourth largest user of this new payment method, behind Luxembourg, Italy and the Netherlands. Many factors, such as the growth in on-line sales or the wider array of mobile services explain this change in payment habits. An analysis of the payment methods reported in STRs shows an increase of more than 20% in digital currency flows between 2012 and 2013. Prepaid cards (which can be purchased without the holder disclosing their identity up to an amount of € 250 for non-rechargeable cards and € 2,500 for cards rechargeable annually[1] offer a substitute for liquid cash, and particularly large denomination bills, due to their anonymity, portability and acceptance networks. Prepaid cards may be distributed either by credit or payment institutions, by market participants from the economic sphere, or on the internet. This last category, to which the growth in the market is largely attributable, is the most sensitive in terms of laundering. These cards, whose value is stored on the issuer's servers – which in most cases are located abroad – allow anonymous transactions to be performed through the acceptance network proposed by the card payment system with linked to the card. The funds prepaid into the digital currency account may be reimbursed to the card's holder or another holder of the

1.Under the conditions defined by article R561-16 of the Monetary and Financial Code

Case study 2

Use of prepaid cards to repatriate the proceeds of prostitution

This case describes a mechanism for the transferring of the proceeds of prostitution, whose level of organisation suggests that pimping is involved

Profile of the participants

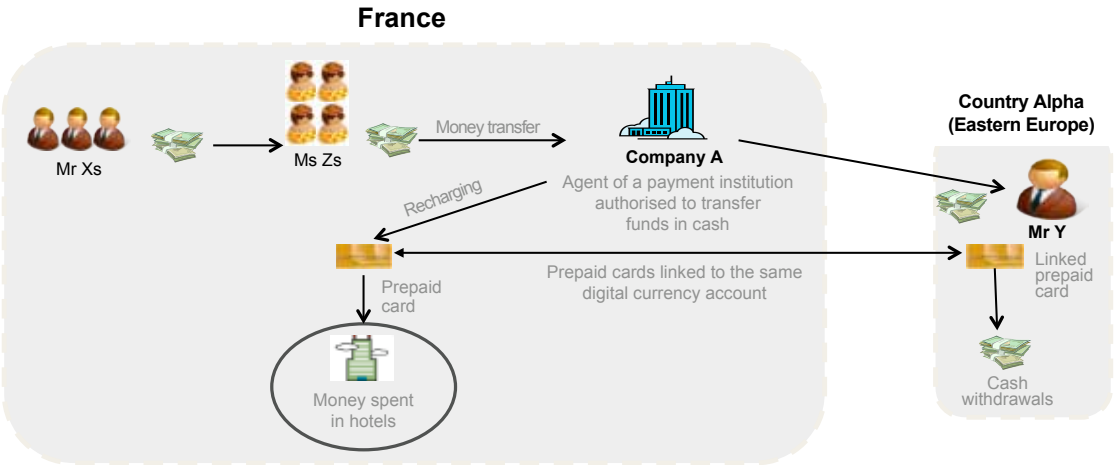
Individuals (the number of participants has been limited to make the diagram easier to understand)

- Mr Xs, the prostitutes' clients;
- Ms Zs, the prostitutes, originating from country Alpha (Eastern Europe)
- Mr Y, the presumed pimp.

Flows leading to the suspicion of wrongdoing

Tracfin's investigations uncovered a fund transfer mechanism based both on fund transfer transactions carried out by payment institution agents and the use of prepaid cards linked to the same digital currency account. Spread over several years, these transactions amounted to €€2.4 million. The Unit analysed more than a thousand transactions, carried out by over 400 senders, who were mainly young women from country Alpha (Eastern Europe) who made fund transfers over short periods of two weeks or so. There were sometimes multiple sending periods in the space of a year, apparently depending on the women's presence in the country. The main senders transferred total sums of between € 30,000 and € 50,000, mostly from Paris and a few large regional cities, and mainly to 3 people. The addresses given by the senders were in country Alpha or were high-end hotels in France, which seems to points to high-class prostitution using the internet as a means of contact. The senders therefore all seem to be directly or indirectly connected to each other by common addresses and/or beneficiaries, which again points to an organised operation. As well as the fund transfer transactions carried out through cash transfers, the prostitutes also recharged prepaid cards used to pay for the expenses relating to their activities. Using a linked prepaid card, the recipient of the cash transfers also made cash withdrawals from cash machines in country Alpha.

Laundering diagram



Warning signs

- Conditions of use and recharging of prepaid cards
- Hotels given as the senders' addresses
- Multiple senders making fund transfers to the same beneficiaries

Reporting entities most likely to detect the fraud

- Payment institutions

digital currency account. The possibility of transferring money in digital currencies therefore calls for special vigilance in both anti-money laundering and counter-terrorist financing terms. Given this situation, article 13 of law No. 2013-100 of 28 January 2013 provides, amongst other things, for the transmitting to Tracfin of information about transactions involving the transfer of money using digital currencies.

Increasing attention paid to financial flows involving virtual currencies

The use of virtual currencies is growing. They are used in a variety of ways, ranging from the settlement of transactions to their use as an investment vehicle. The volatile price of some virtual currencies, and particularly the price of Bitcoin, also fuels speculation. Such currencies are a way of avoiding the danger of personal data theft on the internet, while reducing transaction costs, so that micro-payments can be made. Although they are a source of opportunities, virtual currencies are not without risks. In its 2011 annual report, Tracfin highlighted the specific anti-money laundering and counter-terrorist financing risks arising from the use of virtual currencies given their characteristics. As a consequence of the digital economy's growth, money-laundering methods that use the internet as a channel have since developed. For instance, virtual currencies are contributing to the rise of electronic, disintermediated money-laundering techniques. The *Banque de France* has also issued a warning on the dangers posed to users by virtual currencies[2]. To prevent these risks and in the wake of the thought-process begun in 2011, in December 2013 Tracfin gave renewed consideration to virtual currencies.

2. Banque de France, Focus No. 10, 5 December 2013

How are the anti-money laundering and counter-terrorist financing risks linked to virtual currencies assessed?

While the potential development of the contribution of virtual currencies to internet trading and transactions should not be underestimated, the potential risks and threats linked to their use should also not be overlooked. The indictment by the US courts of the issuer of the virtual currency Liberty Reserve shows the anti-money laundering and counter-terrorist financing risks created by virtual currencies.

A virtual currency is traditionally defined as a unit of account exchangeable on the internet, which is currently unregulated, is created not by a State but by a group of people and is intended to recognise, on a virtual medium, multilateral exchanges of goods or services within this group. A virtual currency differs from a digital currency in that it has no legal tender counterpart.

There are many and varied virtual currencies. A risk assessment must in particular take into account the currency's issuing terms and conditions, conditions of use and particularly the transparency of the financial flows, liquidity, volatility and convertibility into legal tender. Virtual currencies may be based on a closed system (with no possibility of conversion into the official currency) or an open system (with the possibility of converting the virtual funds into the official currency). The flows may be unidirectional (the legal currency may be converted into the virtual currency) or bidirectional (the virtual currency and the legal currency may be converted in both directions). These crypto-currencies (such as Bitcoin and its many derivatives) operate using a technical and functional infrastructure that means that the use of a trustworthy third party to secure transactions can be avoided by using an encryption system. Although they are a source of opportunities, these innovative systems may also bear risks, particularly if their complementarity, interoperability and interconnection with the regulated financial networks are not supervised.

What types of money-laundering risks are virtual currencies exposed to?

In terms of money laundering, one of the main advantages of virtual currencies is that they ensure the complete anonymity of transactions. They may therefore be misused to act as the intermediary of choice in exchanges linked to the informal economy. The use of a virtual currency may also increase the opacity of internet-based money-laundering techniques, for example using on-line games, fraudulent e-commerce transactions or on-line auctions. Aside from these risks, the development of virtual currencies may lead to a loss of revenue for the public authorities (particularly the risk of VAT foregone) and result in unfair competition (payment of wages for undeclared work). This risk of tax and social security fraud is compounded by a risk of financial fraud. For instance, there are many websites designed for fraudulent purposes offering high-yield investment schemes relying on a virtual currency or offering loans in a virtual currency with no guarantee for the user.

Money launderers look for ways to launder dirty money quickly, discretely, securely and globally. Although virtual currencies meet the requirements of speed, discretion and globalisation sought by money launderers, funds held in virtual currencies may not be secure enough. As a result of the speculation on the prices of certain virtual currencies, cyberattacks on virtual currency wallets have increased. As virtual currencies are not issued by a central authority, they are also not legal tender. Their value is a simple value in use that depends on supply and demand. In a warning message issued in December 2013, the European Banking Authority stressed that there is no legal possibility of recovering funds if an exchange platform goes bankrupt[3].

Given the security limitations referred to above, the use of virtual currencies for money-laundering purposes seems more appropriate for micro-money laundering or the laundering of the proceeds of cybercrime. Virtual currency transactions may also be used to informally transfer sums of money from one country to another.

What measures should be taken to limit the risks?

Attention needs to be paid to the possibilities for converting virtual currencies into legal tender when it comes to combating money laundering. The Prudential Supervision and Resolution Authority (ACPR) stated in January 2014[4] that «when Bitcoins are bought/sold for a currency with legal tender status, the intermediation activity consisting of receiving funds from the Bitcoin buyer to then transfer them to the Bitcoin seller is classed as the providing of payment services and habitually carrying out this activity in France entails accreditation as a payment service provider (credit institution, digital currency institution or payment institution) by the ACPR». Particular attention must be paid to financial flows resulting from virtual currency buy/sell/conversion transactions originating from foreign, unregulated virtual money changers or exchange platforms.

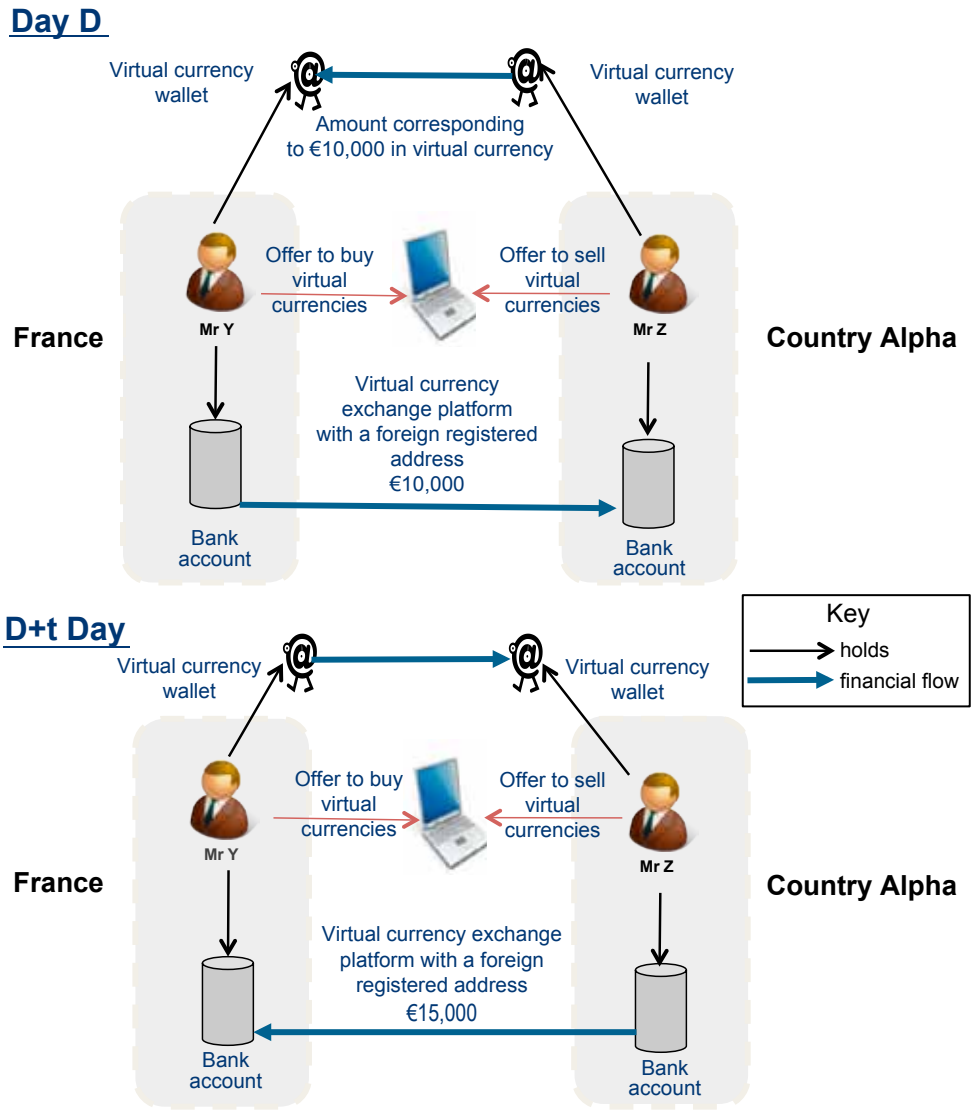
The increasing range of uses of virtual currencies in the economic and financial sphere also raises the issue of how these financial flows, which no longer need to be converted into legal currency beforehand, are to be monitored.

In 2013, Tracfin received reports relating to virtual currency buy-sell transactions by individuals and/or legal entities. The volatility of some virtual currencies prices also lends itself to two-way transactions disguising money transfers between two people as speculative transactions, as shown in the diagram below.

3. European Banking Authority, Warning to consumers on virtual currencies, 12 December 2013
4. Prudential Supervision and Resolution Authority, Position 2014-P-01, 29 January 2014

Diagram: Buying/selling of virtual currencies to transfer money between two people in collusion*

Over-the-counter transactions against a backdrop of high variability in the virtual currency's price



Balance of the transactions: €5,000 transfer from Mr Z to Mr Y disguised as virtual currency buying/selling transactions

⚠ This diagram does not include the transaction fees charged by the virtual money network, the virtual currency wallet management fees or any registration fees.

Particular attention must be paid by reporting entities to financial flows connected to virtual money changers or exchange platforms that are registered abroad and unregulated. These companies operate gateways from the virtual financial system to the State regulated and controlled financial system. They are often organised commercially, logistically and financially so as to take advantage of disparities in international regulations. They may also be used as a smoke-screen to conceal cross-border money transfers and financial movements between two people whose real counterparty is unknown. Reporting entities must therefore make sure that they have all of the necessary information about the origin and destination of the funds in question, and about the purpose of the transaction and the exact identity of the effective originators and beneficiaries.

* Transactions may be carried out in several instalments

THE ADAPTING OF THE RISK-BASED APPROACH TO REGIONAL CIRCUMSTANCES

The increasing of flows to certain tax havens

Tracfin analyses the geographical pattern behind the financial flows that are reported to it. Particular attention is paid to cross-border flows to identify any significant changes and analyse their consistency with the international context. For instance, the fall in the volume of information connected to Switzerland in the second half of 2013 (compared to the same period in 2012) led the Unit to conduct a situation analysis. In connection with the Foreign Account Tax Compliance Act's enforcement, Switzerland and the United States signed a joint statement in August 2013 that defines the framework for Swiss banks' cooperation with the US authorities. On 9 October, Switzerland also announced the approval of the OECD's multilateral convention on mutual administrative assistance in tax matters, which offers the possibility of automatically exchanging information, subject to the approval of the parties interested in this form of assistance. Following the changes to the FATF recommendations in 2012, Switzerland has undertaken to change its laws so as to establish criminal tax offences as money-laundering predicate offences. Against this backdrop, the Swiss banks have begun making strategic adjustments to their business models, pushing them to direct their clients to get their tax affairs in order or risk the termination of their business relationship.

So as to avoid tax regularisation proceedings, fraudsters will opt for a discrete way of transferring their funds, such as cash or precious metals. The fall in the flow of information in the second half of 2013, from Switzerland to France, may therefore be correlated with bank flow avoidance strategies used by Swiss bank clients who wish to illicitly repatriate their assets and, from France to Switzerland, may indicate the transferring of assets to other tax havens.

Although Switzerland should remain the world's leading financial centre for private banking, according to the Boston Consulting Group's global wealth report[5], with around 25% of wealth management assets, financial flows towards Asian tax havens should increase. The number of reports connected with Singapore, Hong Kong and Malaysia received by Tracfin in 2013 in fact grew by 20%. This observation is all the more worrying as the share of STRs concerning legal entities is continuing to fall. Many money-laundering schemes, however, rely on legal entities with registered addresses in countries with low taxes and limited transparency requirements to conceal the identity of the effective beneficiary or beneficiaries controlling the financial flows. The G20, which has made combating tax havens a priority, made a commitment in 2013 in favour of the automatic exchanging of tax information based on an international model that will be defined in 2014 by the Organisation for Economic Cooperation and Development (OECD).

5.The Boston Consulting Group, 2013: Global Wealth 2013

A reporting flow from the overseas territories to be reinforced

The geographical analysis process also looks at the intensity of the information flow, adjusted for the population within the country. This analysis reveals a number of geographical disparities. Variables such as the level of economic activity or crime figures may affect the number of reports observed for each département. Comparing the results of the predictive model built by Tracfin against the actual number of reports allows the identification of the départements whereirregularities have been reported. An analysis of the reporting flow from the Overseas Departments and Territories shows a certain mismatch with the criminal, economic and tax context. The information flow would benefit from being increased and from considering a broader typological scope, for example: i the suspected laundering of the illicit proceeds of drug trafficking, the illicit trafficking of protected species or illicit gold mining. A tax-exempt investment case study is presented below. The exempting of productive investments from tax lowers the profitability threshold of investments, in this way partly offsetting the additional costs that an overseas company may face in investment terms. However, these tax schemes are exposed to various types of fraudulent manipulation. They may also be a potential channel for money laundering. The boosting of the phenomenon by the appeal of French Overseas Departments for real estate investments, which are often used during the money integration phase, may result in an increase in the risk of undeclared labour being used in the construction sector, stimulated by these incentive schemes.

Case study 3

Simplified diagram of potential fraud using schemes to encourage overseas investment

The diagram below summarises a set of suspicions taken from various suspicious transaction reports transmitted to Tracfin regarding «industrial Girardin» type tax-exemption schemes.

Profile of the participants

Individuals:

- Overseas operators who need to develop their business;
- Mainland taxpayers who invest for the tax benefits.

Legal entities:

- An investment company (limited liability company) in a French Overseas Department that raises funds from investors interested in the tax-exemption scheme;
- One or more general partnerships created by the limited liability company to manage the acquisition and rental of the tax-exempt properties.

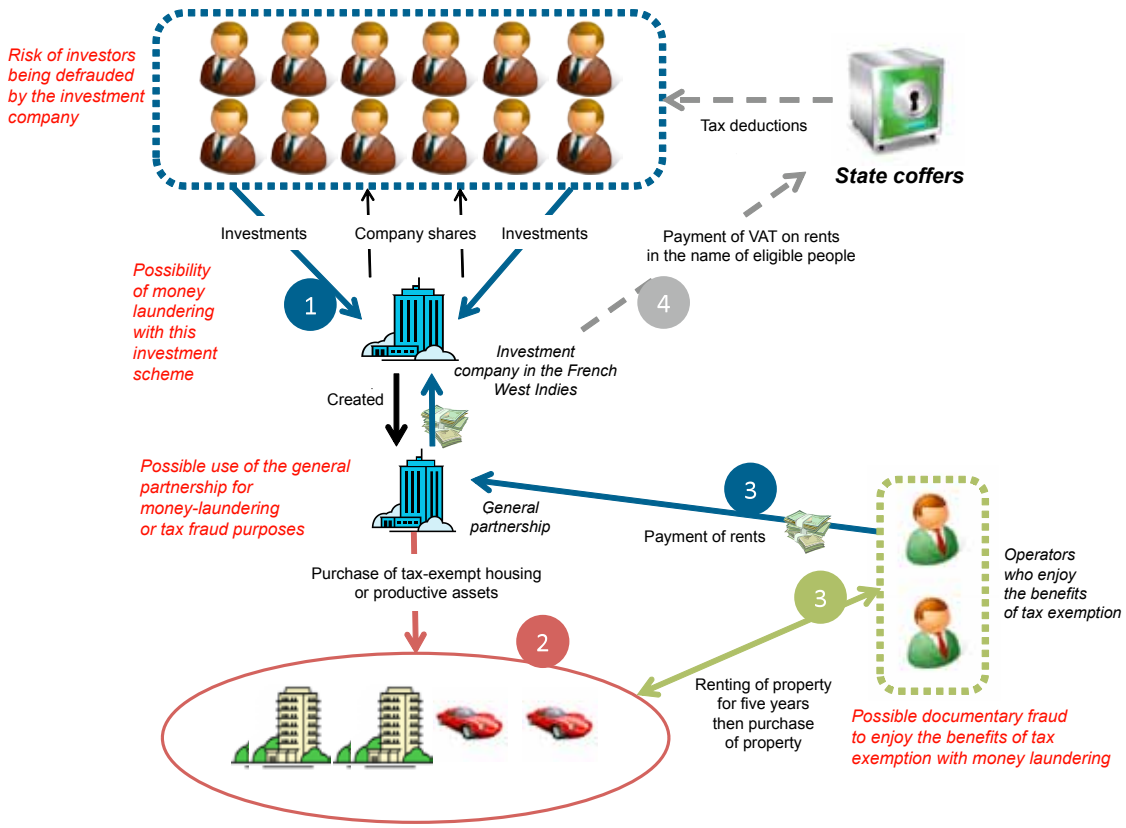
Flows leading to the suspicion of wrongdoing

Productive investments made as part of an «industrial Girardin» type tax-exemption scheme are initially partly financed by the overseas operator (guarantee deposit) through a bank loan and contributions from mainland investors. The operator then pays rent, which is used to pay back the loan, while the mainland investors enjoy tax benefits. The companies involved in setting up the mechanisms are remunerated for services rendered.

In many of the STRs received by Tracfin, some of the properties' operators were not eligible for the scheme and used other people's identities without their consent. This type of fraud may be combined with money laundering depending on the origin of the money that the operators use to rent and purchase the tax-exempt properties. Note that fraudulent structures, fictitious structures and lawful structures may co-exist within the same umbrella company, which complicates detection and calls for a high degree of vigilance.

Where the project is financed by a bank loan (taken out by the general partnership on behalf of the operator), there is an additional risk of the umbrella company playing the role of a credit institution by habitually financing the share of the investments that should be financed by bank loan

using its own capital, which is a practice tantamount to the illicit practice of banking and may be used to launder money. This unlawful behaviour also implies an increased risk for the French treasury as banks, who act as guarantor, usually check the investments' eligibility for the scheme and their compliance. This practice enables the umbrella company to benefit from the payment of interest on the loans instead of banking institutions. A complex setup partly based on foreign structures and bank accounts located in tax havens may also be created to launder the profits generated, and in this way concealed from the tax authorities.



Warning signs

- Financial flows in the investment company's accounts that originate from a person who is not eligible for the scheme.
- Withdrawal of cash from the general partnership's accounts with no economic justification.
- Unknown origin of the money invested in the scheme.
- Purchase of a property not eligible for the scheme.

Reporting entities that are the most likely to detect the fraud

- Banks and credit institutions.
- Financial investment advisors and portfolio management companies.
- Auditors and accountants.

THE ADAPTING OF THE AML/CTF SYSTEM TO GROWING VULNERABILITIES AND EMERGING THREATS

SOPHISTICATED MONEY-LAUNDERING METHODS USING COLLECTION ACCOUNTS

The investigations led by Tracfin have revealed complex illicit financial networks for the financing of undeclared work, the laundering of the proceeds of various predicate offences and the transferring of funds abroad. Within this context, Tracfin has conducted in-depth investigations allowing the reconstruction of the financial networks and the offsetting structures set up. In 2013, for instance, Tracfin exposed a large financial network using the collection account technique. In its 2010 annual report, Tracfin reported the existence of money-laundering networks involving a hundred or so collection accounts held by individuals, as part of a retirement benefit fraud against the CNAV (National Retirement Insurance Fund), whose amount was estimated at more than € 30 million at the time. The fraud mechanism in this type of case was already more complex than in the cases initially described in Tracfin 2008 annual report. Based on the financial networks detected and analysed in 2013, money-laundering structures are becoming more sophisticated and are now based on several levels of collection accounts and the interposing of shell companies.

Based on the financial networks detected and analysed in 2013, money-laundering structures are becoming more sophisticated and are now based on several levels of collection accounts and the interposing of shell companies.

The network uncovered involved more than 600 companies and allowed the recycling of money from sources such as undeclared work and tax fraud in amounts of more than € 90 million. These companies participated in the scheme in successive layers with varying degrees of involvement. The first layer of companies was composed of multiple businesses operating in labour-intensive sectors that in this way considerably reduced the volume of their activities liable for various commercial taxes and made use of undeclared work. These were mainly short-lived businesses with a high turnover from the start of their activity, which were managed by people from the same community and often acted as sub-contractors. The outgoing flows were in the form of either cheques made out to a very large number of individuals, which were possibly salary payments to staff, or payments to second-tier companies. These companies also operated in labour-intensive sectors and recorded bank flows of several millions of euros per year, but did not appear to have any real activity other than acting as financial intermediaries. The third-tier companies operated within the formal economy in highly diverse sectors. These companies were used to launder the illicit proceeds of undeclared work or tax fraud by reincorporating them within the formal economy through international trade transactions. They accepted funds from French entities with which they had no commercial ties as payment from foreign companies.

Case study 4

Complex money-laundering networks using collection accounts

The following case describes a complex, large scale money-laundering scheme based on the collection account technique. This case is also notable for the assignment of receivables agreements used to try to give legitimacy to fraudulent transactions.

Profile of the participants

Individuals:

- Mr X, Mr Y and M Z, directors of security and cleaning companies who belong to the same community.

Legal entities:

- Security and cleaning companies located in France.
- Import-export company A, located in France.
- Numerous companies located in a non-European State, operating in various sectors (agri-food, textile, etc.).

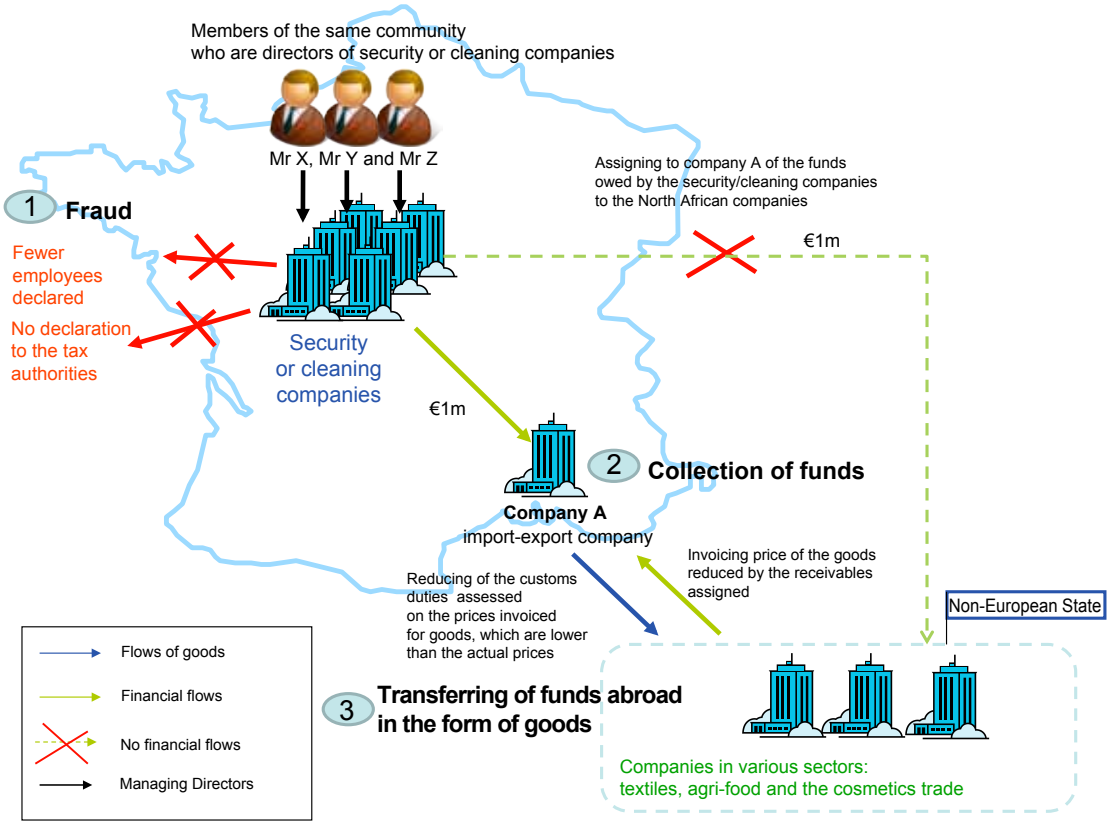
Flows leading to the suspicion of wrongdoing

Company A is an import-export business. In financial terms, and only for its atypical flows, it receives numerous payments from companies located in the Paris region, operating in the security and cleaning sectors. These atypical financial flows amount to nearly € 1 million per year. These companies, which trade in sectors considered to be prone to the use of undeclared work and issue a lot of cheques, are often managed by people from within the same community with ties to a non-European country. After analysis, the accounts of company A reveal a link between these cheques and its clients' accounts. These clients are located in the country of origin of the cheques' issuers. Company A has set up assignment of receivables agreements with its clients to trace these funds. These agreements refer to the existence of a debt between a company located in the non-European country in question and the French cheque issuer. As company A simultaneously holds a claim on the company located in this non-European State, it assigns its claim on the security or cleaning company to company A, which can then collect the cheques of the security or cleaning companies. However, there is no economic justification for this arrangement.

After analysis, the bank accounts of company A show the existence of financial movements originating from this non-European country. The security and cleaning companies' cheques may supplement these payments for the purchase of goods. These funds from the security and cleaning companies may be left out of customs declarations and so allow the value of the goods declared to be reduced when they are imported into the foreign country in question.

These facts taken together suggest that company A is being used to launder the illicit proceeds of undeclared work or tax fraud by reincorporating them within the formal economy through international trade transactions.

Laundering diagram



Warning signs

- With regard to the security and cleaning companies:
  - Recent creation, registered address;
  - Large incoming flows from the first months of activity.
- With regard to the import-export company:
  - Incoming flows from companies operating in an unusual sector;
  - Collection of numerous cheques;
  - Assignment of receivables agreement with no economic justification.

Reporting entities most likely to detect the fraud

- Banks and credit institutions.
- Auditors and accountants.

INCREASED VIGILANCE REGARDING THE RISK OF THE MISUSE OF FUNDS BY CREATING NEW COMPANIES

In 2012, Tracfin highlighted the increased vulnerability to fraudulent practices of companies which, in the current sluggish economic environment, are struggling to find funding. In 2013, a number of reforms were introduced to make it easier for SMEs and mid-tier firms to get appropriate financing. In the 2012 annual report, several types of case illustrated the risk that some companies may fall under the control of criminal networks to be used as «legal shop windows» for the recycling of illicit activities or enter into business relationships with companies controlled by organised crime. In 2013, company failures remained at a high level and also affected companies more than five years old, putting many jobs in jeopardy. When analysed, the failed companies were found to have both operating weaknesses and weak balance sheet structures[6] with very high levels of debt. Given the considerable potential impact that company failures may have on suppliers and financial lenders in these conditions, increased vigilance is needed when new companies are set up to prevent the risk of fraudulent practices.

6. Altares «Analyse 3ème trimestre 2013 : défaillances et sauvegardes d'entreprises en France» (Q3 2013 analysis: company failures and rescues in France)

Case study 5

Creation of companies for the misuse of funds lent by credit institutions and a public business financing and investment group

The following case is an example of the misuse, for personal ends, of funds lent by credit institutions and a public business financing and investment group, by individuals using false identities and various falsified documents. The financial transactions identified as suspicious and the investigations conducted by Tracfin point to a financial scheme involving the misuse of company assets, forgery and the use of forgeries, fraud and the laundering of the proceeds of said misdemeanours.

Profile of the participants

Individuals

- Mr X, the director of companies A and B.
- Mrs X, the wife of Mr X and partner in companies A and B.

Legal entities

- Company A, a supposed supplier of equipment to company B.
- Company B, which has several bank accounts.
- Company D, a company removed from the commercial register many years ago, which is in no way connected to Mr and Mrs X and whose name is almost identical to that of company A.

Flows leading to the suspicion of wrongdoing

Mr X is the minority director of company A and his wife, Mrs X, is his partner. After this first company had been set up, Mr X falsified his name, his date of birth and his national identity card to create a second structure, company B, of which he was also the minority director. His partner, Mrs X, also used a false date of birth and national identity card, for the same reasons.

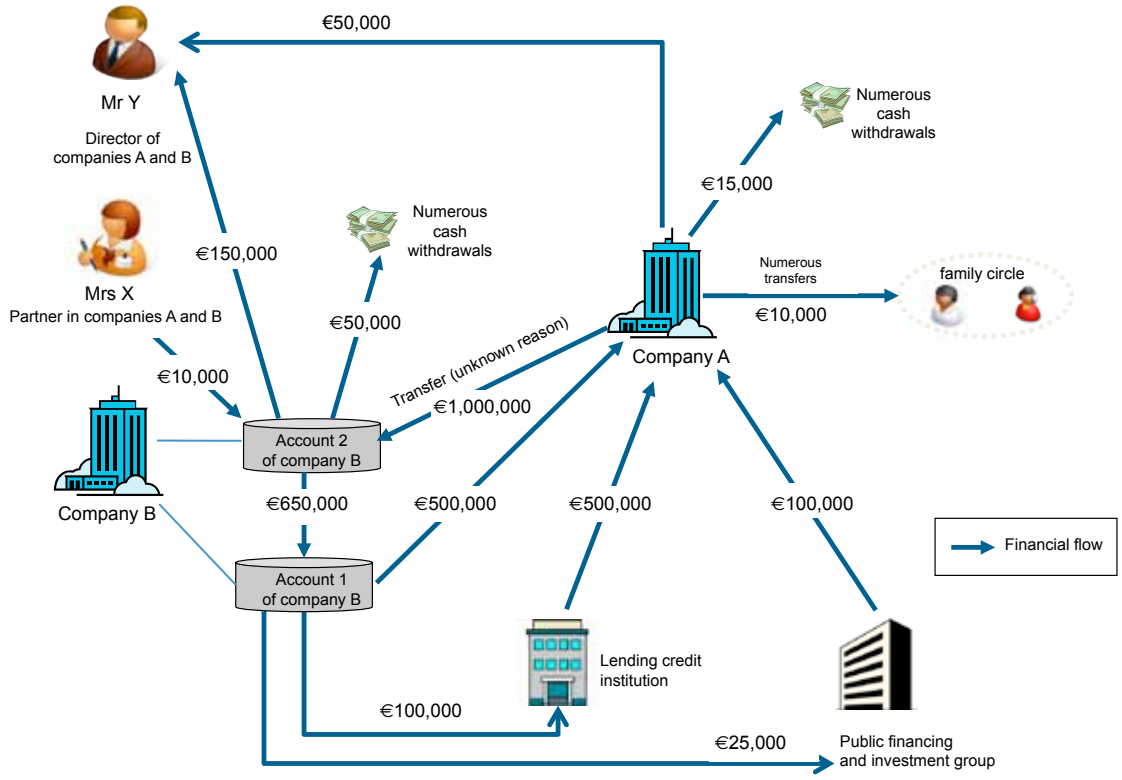
Company B took out several leases, covered by contracts that also contained false information. In order to receive funds from the credit institution without arousing suspicion, on each contract Mr and Mrs X:

- designated as a supplier of company B the company D, which had been removed from the commercial register and which they were in no way linked to;
- signed these contracts in the name of their other company, company A, of which they were the minority director and partner respectively, but using the commercial registration number of Company D.

By using the fact that the names of companies D and A were almost identical, and by using the commercial registration

number of the second company in connection with the first company, Mr and Mrs X managed to hoodwink the credit institution, which did not realise, when the contracts were signed, that the information produced was partially incorrect and that company B, the borrowing company, and company A, the signatory company, belonged to the same two people. Once the contracts had been concluded, company A, which was a supposed supplier of equipment to company B, received more than € 500,000 from the lending institution. At the same time as it submitted its loan application to the credit institution, company B, wishing to extend and develop its activity, sent a second application to a public business financing and investment group. Like the application submitted by company B to the credit institution, the application submitted to the public financing and investment group contained anomalies (falsified information). Under the terms of this contract, nearly € € 100,000 was transferred by the public group to company A. Note that, during the period analysed, company B was company A's only client. Nearly half of the funds credited to company A's bank account therefore came from company B, while, at the same time, company A transferred more than € 1 million to company B for an unknown reason. Both company A and company B also issued cheques and transfers to Mr X and his children. Many withdrawals were also made from the two companies' accounts. It is possible that the invoices presented by company A to these two lending organisations were fictitious and were not connected to any actual equipment. It is also likely that companies A and B were set up by Mr X and his wife solely to misappropriate funds and enrich themselves by putting them to personal use.

Laundering diagram



Warning signs

- Reciprocal financial flows with no apparent justification between companies with the same director.
- Noting of anomalies in invoices.
- Use of forged documents.
- Numerous cash withdrawals and numerous transfers and cheques issued to the director and his loved ones.
- Doubts about the company's real activity.

Reporting entities most likely to detect the fraud

- Banks and credit institutions.
- Public business financing and investment group.

NEW FINANCING METHODS REVIVING TRADITIONAL LAUNDERING SCHEMES

According to the *Banque de France*[7], although SMEs still have wide access to investment loans, the supply of cash loans is tightening. These tougher credit conditions have been all the more harmful due to the lack of a real alternative to external bank financing. This is why many initiatives were launched to diversify sources of funding for SMEs and mid-tier firms in 2013. These included the reforming of the insurance code, which extended the list of assets eligible to cover insurance companies' regulated commitments, thus allowing them to diversify their investments by financing SMEs and mid-tier firms. This is the backdrop to the strong enthusiasm shown for crowdfunding in France, with close to «€ 40 million invested in 60,000 projects in 2012»[(8)]. This participative financing method offers an alternative means of project financing, which allows funds to be raised from the public to finance a project through an internet platform. It combines several different banking and financial techniques whose common feature is mainly the non-professional background of the participants, or even, sometimes, the disinterested nature of their contribution, made over the internet. It means that projects unable to obtain financing through traditional channels can still get funding. The Prudential Supervision and Resolution Authority (ACPR) has identified three types of crowdfunding platforms:

- platforms used to collect donations or contributions that may be used for various purposes;

- platforms used for project financing through loans;

- platforms used to finance an entrepreneurial project through the subscription of shares.

As part of the think-tank led in 2013 by the French authorities on the reforming of the legal framework applicable to participative financing, Tracfin has analysed the risks associated with this new financing method in terms of money-laundering and counter-terrorist financing.

Crowdfunding platforms have a number of features that lend themselves to various fraudulent schemes, as the use of the internet enables traditional channels for money-laundering and fraud to take electronic form and proliferate.

The credit transactions and investment services that may be offered by some crowdfunding platforms are indeed likely to be of interest to launderers, as useful «tools» for the integration of funds within the formal economy. As the nature of the funds is changed it becomes more difficult to detect their dubious origin.

Crowdfunding platforms may be a way to modernise the tontine operating principle, through the use of the internet, and to consolidate sums from different sources. A crowdfunding platform may be used as a «collection account», for example for a drug-trafficking operation or any other form of informal economy. Crowdfunding platforms are useful for obscuring financial flows, which can then be obscured still further by the use of digital and virtual currencies. In terms of terrorist financing, the risk posed by such platforms is that a tool may be developed that could be used to accumulate financial flows and make international fund transfers while avoiding the regulated financial channels. Crowdfunding is also a tool that may be misused for cybercrime such as internet fraud disguised as pseudo-cultural or humanitarian projects. A scheme whereby canvassers contact a large number of internet users to request small contributions towards a fictitious project is a perfectly plausible scenario. The client would be less likely to be wary given the small amount involved and also less likely to file a complaint.

7. Quarterly survey of SMEs and mid-tier firms on their access to credit in France, Q4 2013.

8. Les Echos, 15 March 2013. Financement participatif des PME : le « crowd-funding » francais donne de la voix (Participative financing of SMEs: crowdfunding provides support in France).

Tracfin was part of the think-tank led by the French authorities in 2013 on the reforming of the legal framework applicable to participative financing so as to promote the development of this new financing method while limiting the risks, given that it is particularly suited to the financing of SMEs and innovative young companies. The reform will come into effect in the first half of 2014. The regulatory disparities between countries also need to be smoothed out, or else there is a risk of arbitrage between legal systems in favour of the least restrictive in terms of money laundering and terrorist financing. Another risk is that of certain countries that are money-laundering hubs and also have expertise in the hosting of IT servers specialised in payment services developing a crowdfunding platform hosting activity. The alignment of national regulatory frameworks, particularly with regard to platforms or project sponsors operating in several European countries, is a priority being tackled by the European Commission.

Case study 6
Use of a crowdfunding platform by drug dealers to pay their wholesaler

The following diagram presents the misuse of a crowdfunding platform as part of a drug trafficking operation. The drug traffickers use the platform to pay their wholesaler, thus disguising payment transactions as investment transactions. This setup may be used for any type of illicit economy (such as counterfeiting, undeclared work, weapons and prostitution).

Profile of the participants

Individuals:

- Investors 1, 2, 3 and so on: drug dealers in France.
- Project sponsor: drug wholesaler, located in country A.

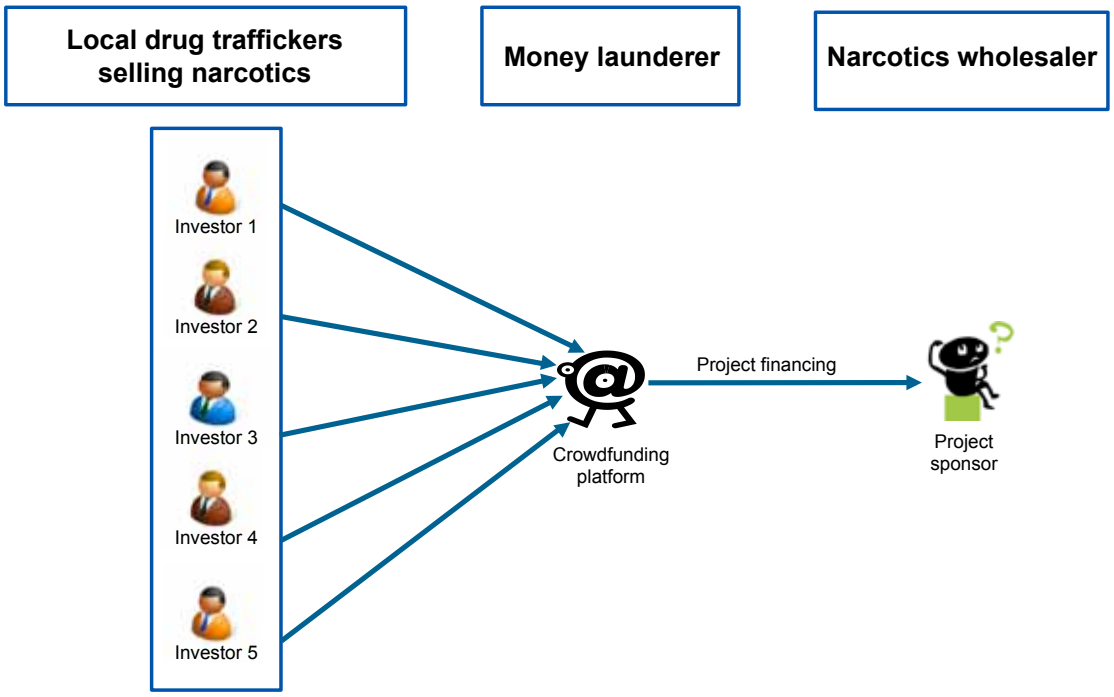
Legal entities:

- Crowdfunding platform: commercial registered address in country A, IT hosting in country B, banking registered address in country C.

Risk analysis

A crowdfunding platform may be used by a criminal network to facilitate the transferring of funds between a group of «feeders» and a collection account. The platform gives an appearance of legitimacy to a money-laundering operation, behind a commercial or humanitarian smokescreen, by allowing the consolidation of financial flows in a collection account registered abroad. This setup, which is designed to obscure financial flows, and particularly cross-border flows, may be made more complex by combining it with the use of a digital and/or virtual currency.

Laundering diagram



Warning signs

- Amounts given/lent/invested and conditions of payment of these amounts (origin of funds, bank details, etc.).
- Doubts about the identity of the effective beneficiary of the sums collected.
- Profile of investors.
- Nature of the project financed.

Some examples of good practices for the internal monitoring of a crowdfunding platform

- Reasonable knowledge of contributors and project sponsors: platforms put project sponsors into contact with contributors. They have access to information enabling them to check their contributors and project sponsors and to put into place vigilance procedures. Whatever the activity carried out by the platform, the contributor and project sponsor databases must be regularly cross-checked to detect any anomalies pointing to the misuse of the platform for money-laundering purposes (e.g. the contributor and the project sponsor are the same person).
- Detection of suspicious behaviour: the platforms apply a filter between project sponsors and contributors, which provides them with feedback that allows them to identify atypical behaviour (e.g. an atypical flow amount and/or frequency or an abnormally low or high number of contributors). The platforms have access to information enabling them to conduct consistency checks (e.g. one IP address – one contributor, foreseeable amount collected estimated based on the number of the project sponsor's contacts on social networks) and detect anomalies.
- An appropriate risk classification, for example: specific vigilance procedures may be applied above a given contribution threshold,regardless of the methods of payment of the contribution (one or multiple instalments).

THE COMBATING OF TERRORIST FINANCING

For the combating of terrorist financing, the detection of high-risk profiles by using financial intelligence is a very discrete way of adding to the information collected by the field units responsible for identifying and combating radical movements. Whether its intelligence comes from suspicious transaction reports sent by reporting entities subject to AML/CTF obligations or other channels such as information notes transmitted by intelligence units, the counter-terrorist financing (CTF) unit is able to promptly collect and analyse the large quantity of financial and environmental information at its disposal thanks to the powers devolved to Tracfin under the monetary and financial code.

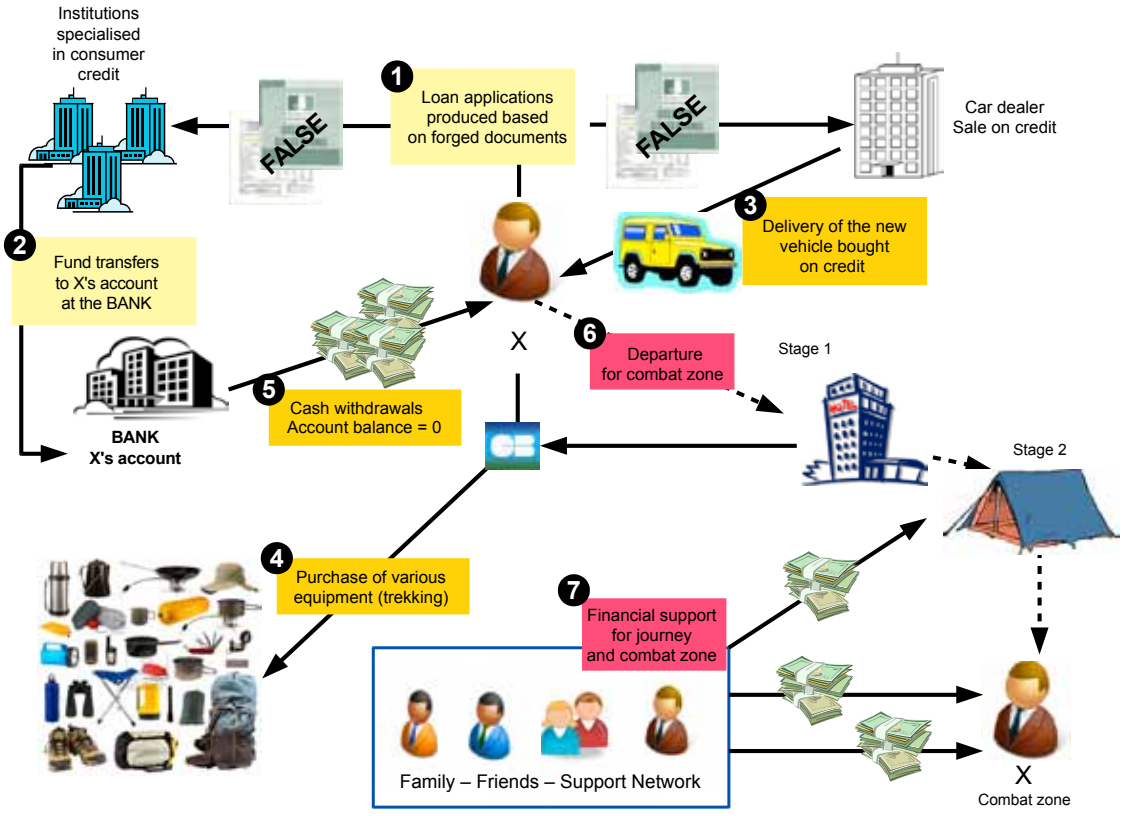
For this type of investigation, the aim is to detect weak signals and find the connection between them by identifying the links between the various participants. Tracfin investigators collect information that can be used firstly to characterise the financial behaviour of these targets, and secondly to situate the people or entities with which they have established relationships in time and space.

In a very factual way and based on the financial intelligence collected, the investigators profile these individuals, describing their habits, their acquaintances, the relationships or friendships they have forged and where they trave. To complete this process, the investigators have access to multiple financial sources and a relatively broad scope of information. Banking information is particularly useful as it can be used to produce a «financial» composite sketch of individuals suspected of belonging to a terrorist organisation. This approach can reveal details on their resources, such as: wage income, welfare benefits and donations or remuneration paid by cheque or through cash deposits.

The collecting of this type of information provides a better picture of suspects' immediate environments. The various financial transactions detected and analysed sometimes lead to the identification of individuals who support a cause and have decided to make a financial contribution to it. These people are then likely to be included in the scope of the unit's investigations and to have their finances examined in their turn. At this particular stage of the inquiry, it is vital to define the scope of the investigations with the specialist units focusing the research on relevant targets.

CASE STUDY
AN INDIVIDUAL GOES TO A COMBAT ZONE

In terms of financial behaviour, there may be many warning signs indicating that an individual has decided to take action by leaving the country for a combat zone abroad. In the case below, the individual's main objective is to raise a maximum amount of funds in a short time. Initially, the rapid collection of funds is a core element of his activity. To achieve his goal, the individual applies for credit to several consumer loan institutions using false documents (pay slips, certificate from his employer, etc.). These organisations are in fact able to provide funds very quickly, providing that the amount requested does not exceed a few thousand euros. During this preparatory phase, operating on these same principles, the applicant may also purchase a vehicle on credit. Shortly before his departure, once the funds have been paid by the credit organisations, the money is completely withdrawn in cash in one or more instalments. The account is rarely closed but its balance is close to zero and there are no further transactions. During this last stage of their preparations, the individual will also acquire the equipment they need, such as trekking equipment from a specialty shop. After the person has left the country, it is sometimes possible to follow their itinerary through expenses paid for by bank card and. Once they have reached their destination,it is followed through cash transfers sent to them by support networks (family, friends and accomplices). In this last phase, it is particularly important for the unit to have already identified as many targets as possible in the suspect's entourage so as to detect any sources of financial support.



OVERVIEW OF NOTEWORTHY CASES IN 2013

CASE 1
TAX AND VAT FRAUD

Tracfin was informed about some atypical financial transactions, carried out in November 2013, in several accounts opened in the name of Mr X and numerous entities managed by the latter and his spouse.

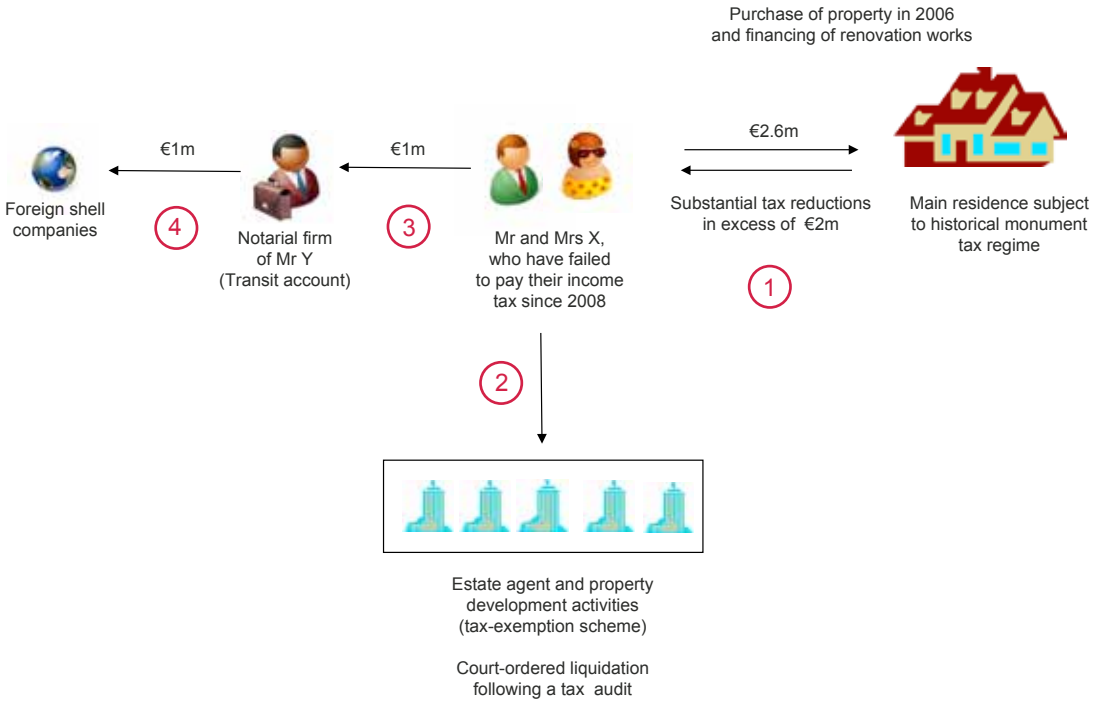
Mr X and his spouse developed a real estate activity and had more recently invested in «senior residence» type property development schemes offering tax benefits for investors. As part of these activities, the couple set up around twenty companies between 2012 and 2013, including property investment companies, construction-sale companies and various commercial consultancy or architecture companies.

Most of the companies owned by Mr and Mrs X had not submitted any income tax or VAT returns since they were set up. Mr and Mrs X had also not filed any tax returns since 2008. Up to this date they had benefited from substantial tax reductions (more than € 2 million in respect of their 2007 income) particularly in connection with expenditure on buildings designated as historical monuments. They failed to file a wealth tax return.

The main residence of Mr and Mrs X was an outstanding property, purchased in 2006 and designed by a well-known early 20th century architect, it had a 1000 m2 living floor space. Extensive restoration works were carried out on this property, which was listed as a historical monument and was purchased for € 2.6 million.

Mr and Mrs X, and many entities managed by them, underwent several tax inspections that resulted in substantial back-tax requests. To avoid paying the tax that they owed, the interested parties employed various strategies to evade precautionary recovery measures. Several companies that had been audited were declared bankrupt. Mr X also deposited part of his disposable cash in an account opened in his name with a notarial firm (which was unlikely to be subject to a third-party notification) which was a business acquaintance. Using the sale of shares to two foreign companies based in the Middle East as cover, Mr X ordered several transfers from the account held with his notary to these shell companies, totalling € 1 million with the intent to leave the country.

In accordance with Article L561-25 of the monetary and financial code, the Unit used its power to put a stop on these transactions. The freezing of these transactions



enabled the exposing of the part played by the notary involved in them. The latter had, in fact, ordered the transferring of the sums initially frozen to a third-party account that had a commercial relationship with Mr X.

This information was referred to the competent public prosecutor's office. An investigation is underway based on evidence of conspiracy to launder the proceeds of tax and VAT fraud and complicity.

Warning signs

- repeated failure to meet tax obligations;
- ordering of international money transfers.

Case 2
PONZI SCHEME

Following reports of suspicious transfers by individuals to two companies X and L based in a free zone of a Mediterranean country, Tracfin identified around forty individuals, residents of the same region, who had transferred in excess of € 4 million to these companies.

These transactions, in the form of share subscriptions or management mandates, were presented as financial investments with particularly high returns, in the 20% to 200% range per annum. They were presented as likely to be of interest to savers looking for a discrete way to earn high yields. These rates seemed all the more unrealistic as the activity of the two companies involved remains entirely obscure (no website, not listed in professional directories, no commercial testimonials, and so on). The projects they presented were as varied as as shellfish farming, wine and nappies. All of these facts seemed to point to fraud.

Thanks to the help of the financial intelligence units of the relevant countries, the Unit identified Mr A as the founder of companies X and L and became convinced that these were largely fictitious structures as the funds merely passed through bank accounts opened abroad.

It was also found that more than € 5 million from these companies had been credited to several accounts in France. Although part of this money was earmarked for financial intermediaries (asset management advisers, brokers, etc.), the lion's share of the funds was used to finance five companies, which were all controlled by Mr A.

When these entities and their accounts were analysed in depth, it was discovered that structures with unclear boundaries were simultaneously set up and large sums of money passed through them very quickly. This network-based structure and the corresponding reciprocal flows offered the advantage of concealing the overall volume of the funds received and their final destination.

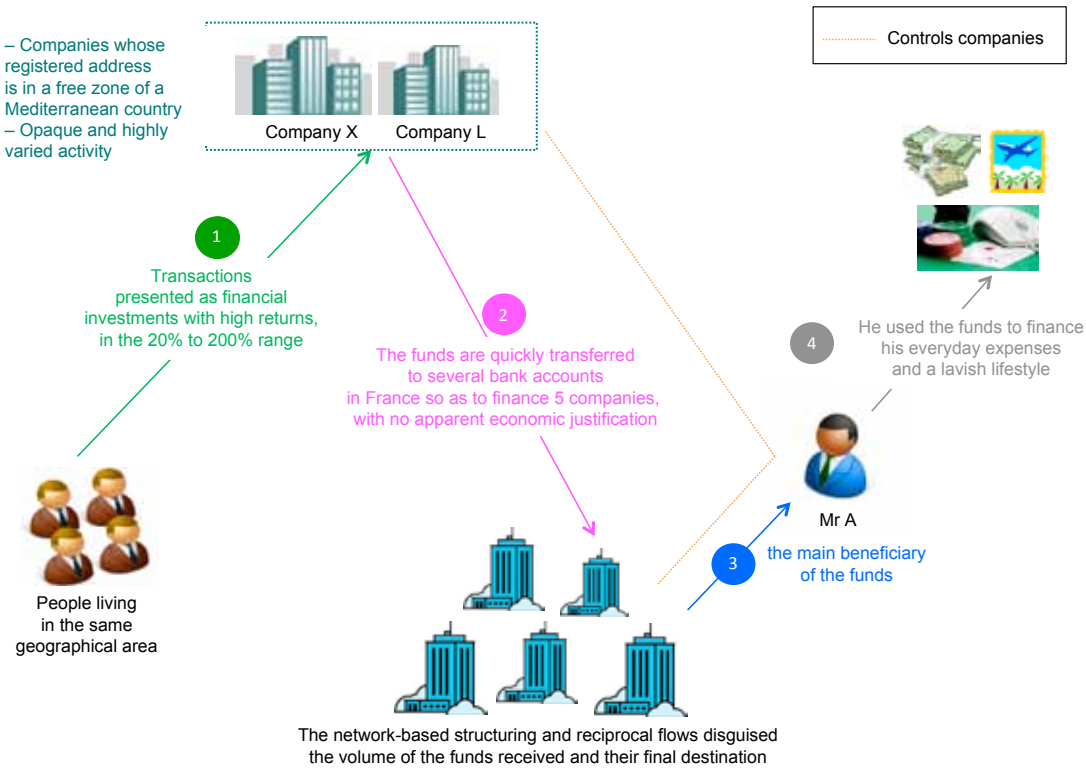
It was in fact Mr A who proved, in a personal capacity, to be the main beneficiary of the funds received from the free zone of the Mediterranean country. Aside from a few related investments, in various sectors, these sums enabled him to pay for his everyday expenses. The funds

he collected from gullible individuals enabled him to lead a particularly extravagant lifestyle.

The police investigation conducted following the referral from Tracfin resulted in the uncovering of a scam involving more than a hundred victims and an estimated sum of € 15 million. The Criminal Asset Identification Platform (PIAC) also went to work to identify any property purchased using the proceeds of this fraud. The main protagonist was charged with conspiracy to defraud, conspiracy to commit a crime and money laundering.

Warning signs

- foreign investments promising an unrealistic return;
- wish of interested parties to ensure the confidentiality of these investments;
- simultaneous creation of several companies and reciprocal flows between them, associated with no clear economic justification;
- atypical operation of company accounts: receiving of foreign transfers, lack of the expenses usually expected (wages, suppliers, etc.), private expenses;
- clear inconsistency between the client's known situation and their lifestyle.



Case 3

FRAUD INVOLVING GRANTS FOR IMPROVEMENTS TO SOCIAL HOUSING

The Unit was informed of atypical bank transactions by individuals who applied for State, regional and departmental grants to make improvements to rented social housing.

These grants are subject to the meeting of strict conditions which, according to the bank statements examined, appear to have been breached, and particularly the requirement to use private contractors to carry out the work.

The beneficiaries, who were labourers in the construction sector, appear to have overestimated the cost of the work, which they then carried out themselves at a lower cost, pocketing most of the grant money.

Whereas these grants were introduced to help ensure that the poorest people have access to decent housing, associates X and Y may have applied for these grants unduly for their own personal gain, using fraudulent practices and particularly false documents.

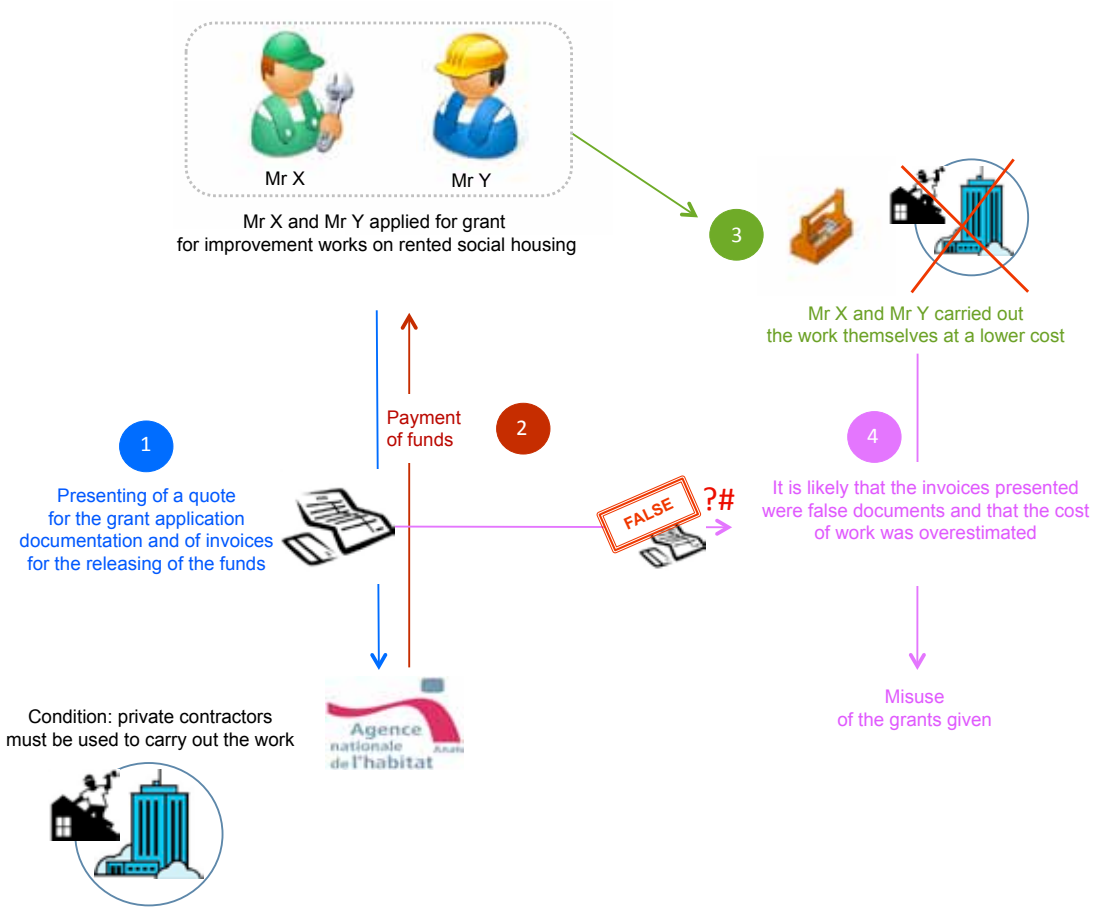
The grants awarded could only be released on the presentation of original invoices from the private contractors that carried out the work in accordance with the estimates produced for the grant application documentation. Mr X and Mr Y therefore probably produced false documents to gain access to the funds.

An estimated € 132,000 of public funds were misappropriated between 2009 and 2012. There is also a real risk of this practice quickly spreading within the family and professional circle of the interested parties. Note that the individuals under suspicion are related.

The evidence uncovered led Tracfin to suspect Mr X and Mr Y of breach of trust (misuse of grants), forgery and use of forgeries.

Warning sign

- Use of grants that is unconnected to their initial purpose.



Case 4

LAUNDERING OF THE PROCEEDS OF ILLICIT ACTIVITIES THROUGH SPORTS BETTING AND DUBIOUS PROPERTY FINANCING TRANSACTIONS

As part of its duty to monitor gambling activities, Tracfin's attention was drawn to the abnormally high number of cheques received by Mr X and his wife. Over a period of 24 months, the couple won more than 900 times at the Parions-Sport betting games offered by Française des Jeux (FDJ), collecting winnings of more than € 150,000. A large share of the winnings were notably paid into the accounts of the couple's children, who were minors.

The tax returns of Mr and Ms X showed that their only, modest income came from rental activities. For these activities, the couple took out real estate loans exceeding € 1.5 million from various banks to buy a large housing stock. Although the amount of the loan application very much exceeded usual requirements, the bank nevertheless gave its approval, transferring the risk to Crédit Logement (a mutual guarantee fund).

As the tenants were low income, rents were mainly paid by the Caisse d'Allocations Familiales (Family Allowance Fund) and the couple willingly requested housing benefits for themselves as well.

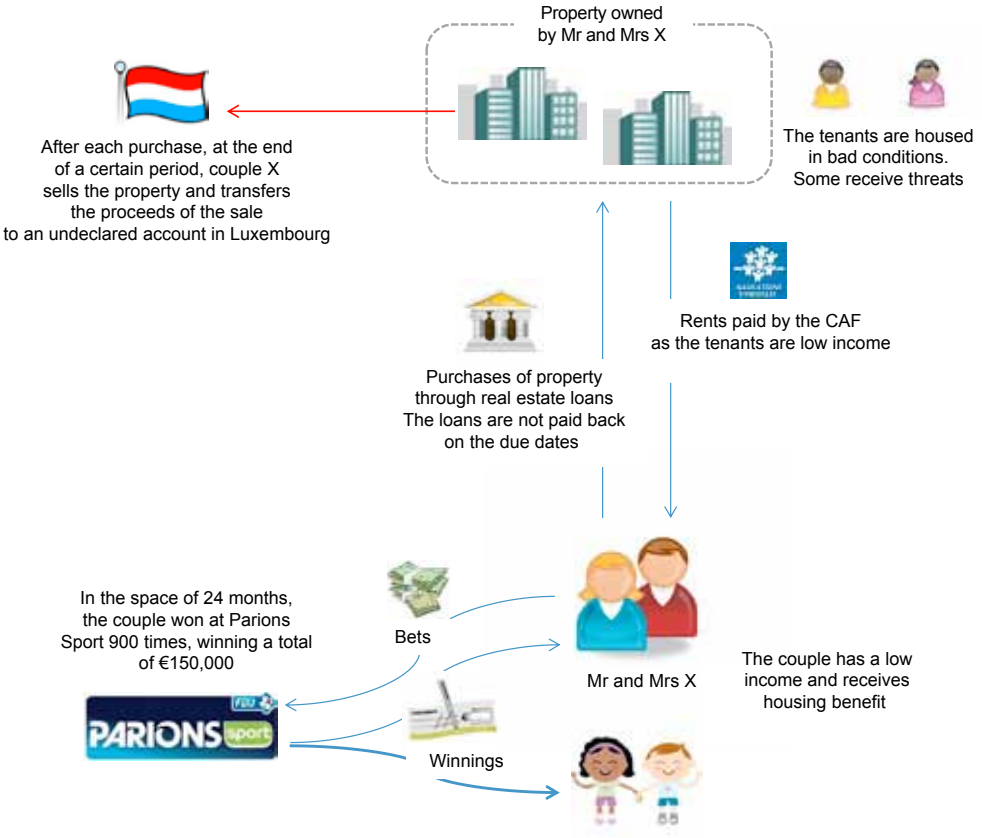
The tenants were apparently housed in bad conditions, with some living in cramped conditions. Others received threats.

After each purchase, at the end of a certain period, the couple resold the property and transferred the proceeds of the transaction to an undeclared account in Luxembourg. They also failed to make repayments on their loans by the due dates.

One of the possible explanations for the large, repeated winnings paid out by the Française des Jeux was that Mr and Ms X had a lot of undeclared cash, probably as a result of their rental activity, and they used it to place sports bets.

Warning signs

- The large number of cheques for betting winnings collected.
- International transfers.
- Hundreds of transfers from the CAF.



Case 5

MISUSE OF PUBLIC FUNDS AND COMPANY ASSETS

Mr X worked for limited liability company A, a family construction company managed by Mr Y, his brother-in-law. His wife was an employee of an inter-municipal structure. In the space of 15 months, Mr X received nearly € 280,000 in his personal account in the form of transfers issued by a municipal treasury on behalf of a public institution. The incoming flows showed, when analysed, that these sums were paid for supposed services invoiced by company A.

These facts all suggested the misuse of public funds backed by a system of false invoices. These suspicions were confirmed during the judicial investigation, which revealed that Ms X, as general secretary of the public institution where she worked, had misappropriated more than € 800,000 over an 8-year period so that she could lead the high life and pay back loans.

At the same time, Tracfin led investigations into atypical financial transactions carried out in the account held by Mr Y, the director of limited liability company A and brother of Mr X. Between 2008 and 2013, the latter received over € 710,000 from this company, which had recorded losses since 2010. When analysed, the flows debited from Mr Y's account showed that a little over half of these sums were later withdrawn in cash. This evidence caused the Unit to suspect the misuse of company assets and the laundering of the proceeds of this offence.

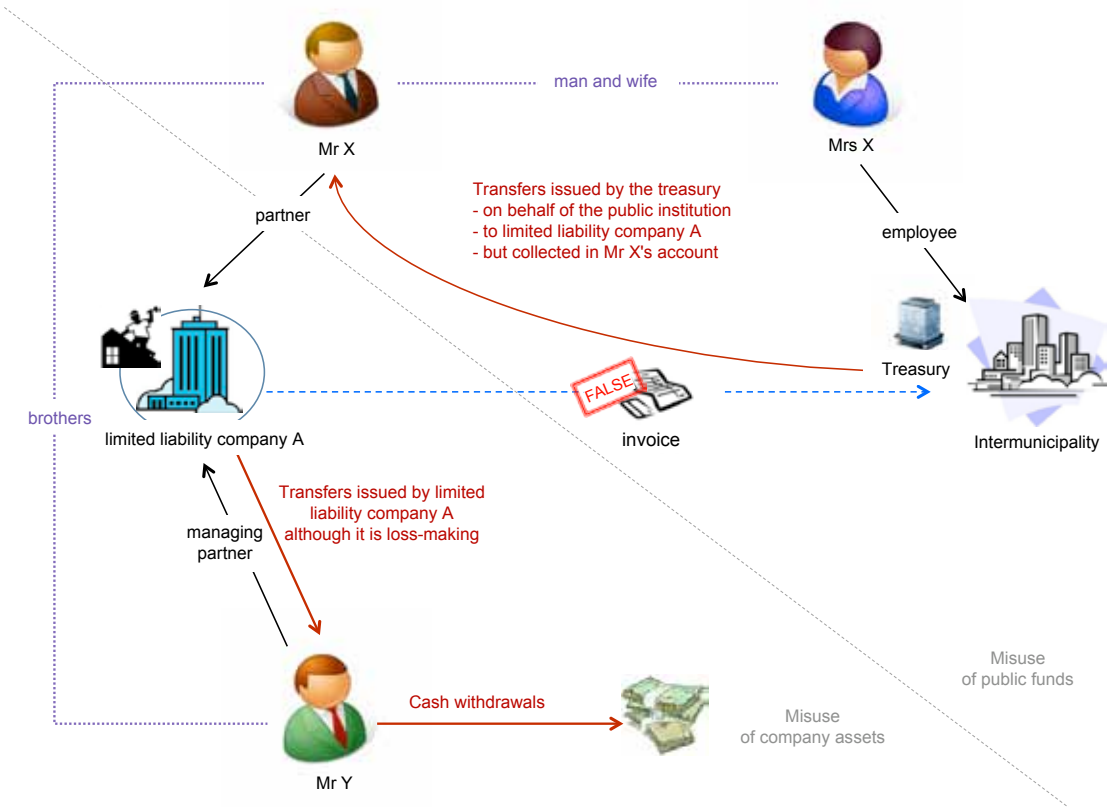
Warning signs

Regarding the misuse of public funds:

- receiving in an individual's account of large transfers from a municipal treasury;
- wife of this individual employed by the public institution issuing said flows;
- inconsistencies in the explanations given by the interested party.

Regarding the misuse of company assets:

- disproportionate amounts of the sums paid by a loss-making company to its director;
- frequent cash withdrawals;
- refusal by the interested party to explain the transactions in their account.



Case 6
MONEY-LAUNDERING SCHEME USING PREPAID TELEPHONE CARDS

Tracfin's attention was drawn to atypical financial transactions carried out by a company operating in the telephony field and hosted by a registered office provider. This structure received funds from companies whose sector of activity seemed to be unrelated to telecommunications.

The Unit uncovered incoming flows totalling over € 6 million over an 18-month period from textile merchants. The outgoing flows were in excess of € 6 million and comprised of transfers to prepaid card providers.

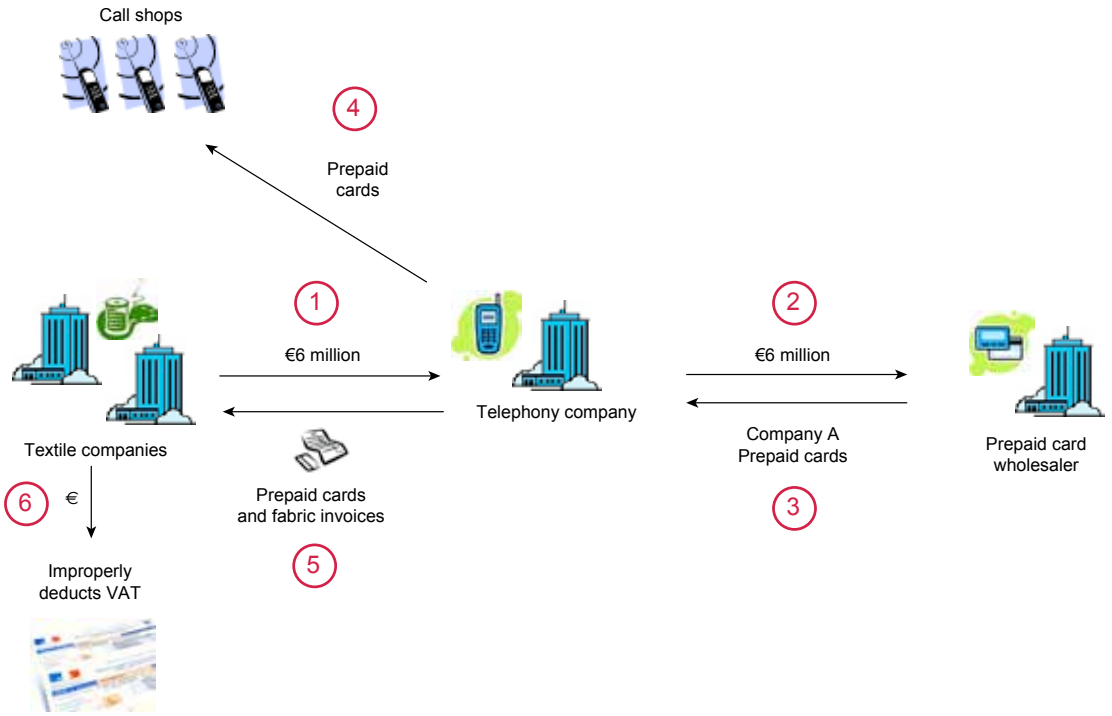
Tracfin's investigations showed that the company was buying prepaid cards from wholesalers. These cards were then being sold to textile companies.

This information was referred to the courts for suspected laundering of the proceeds of crime as the financial flows had no economic justification.

A false invoicing system was then exposed by a criminal investigation department unit. The invoices for the purchasing of telecommunication cards by these textile companies had been falsified and become invoices for fabric purchases. The client companies deducted more VAT than they were entitled to based on these false invoices. As a matter of fact, the textile companies were not the final recipients of the SIM cards, which were sold on the black market through call shops and small stores. In addition to the VAT fraud, the retail sale of the cards generated a large flow of cash that was not paid into a bank account and may have been channelled into money-laundering mechanisms based on offsetting. This money was probably shared by the various protagonists (telephony company, call shops, wholesaler and textile companies).

Warning signs

- telecommunication company whose main clients operate in other sectors of activity;
- telecommunication company with the status of a one-person limited liability company or limited liability company;
- company hosted by a registered office provider;
- tax returns not declaring any assets (real or movable property) or salary.



TRACFIN ABROAD: A STRATEGIC ACTIVITY

Tracfin's many proposals aimed at promoting information sharing with its partners have always focused on increasing the information shared as part of the combating of money laundering and terrorist financing. As an example, the substantial increase in information requests from foreign financial intelligence units (FIU) (952 requests from FIUs in 2013, representing a +17% increase), reflects the Unit's cooperation efforts designed to provide its counterparts with relevant information to develop the information that they have received from their own reporting entities at national level. It also demonstrates the FIUs' determination to improve the monitoring of atypical cross-border financial flows.

2013 was a turning point in Tracfin's international activity, as many projects begun in previous years took shape over the year.

Internationally, it has been agreed that the Egmont Group's standards need to be raised, in keeping with the revising of FATF's standards, particularly with regard to the recommendations for information analysis and increased information sharing.

At European level, the Unit is actively participating in negotiations on the proposed revising of directive No. 2005/60/EC of 26 October 2005 (known as the «third anti-money laundering directive»), which was transposed into French law by order No. 2009-104 of 30 January 2009. Tracfin's position is that FIUs' operating capacities should be increased by taking steps to ensure that every FIU has access to effective tools, such as a centralised bank account file or the power to exercise a right to information against reporting entities subject to anti-money laundering obligations.

At the bilateral level, the Unit is participating in projects related to current major issues, such as tax evasion. It is acting to strengthen its collaboration with countries known as tax havens. In 2013, for instance, Tracfin initiated meetings with these countries' anti-money laundering units, to identify the means required to improve information sharing and systematically disseminate these FIUs' information.

Finally, the Unit is working to bring FIUs within the French-speaking community together to discuss the operational capacities of each, particularly in the area of information analysis.

Tracfin has increased its resources to meet the needs of this work. The gradual streamlining, standardisation and formalisation of the procedures for processing information received from abroad, combined with an increase in the number of staff dedicated to international information sharing, who have complementary backgrounds and specialist expertise, have contributed greatly to the development of information sharing with foreign FIUs.

At the same time, the formalisation of operating procedures at international level has enabled Tracfin to more efficiently develop the evidence in ongoing judicial proceedings. Tracfin is also able to target the foreign disclosures that will subsequently allow the French authorities to usefully set up mutual judicial assistance. By streamlining this process and identifying it as a major focus for its cooperation with its counterparts, the Unit has become a key partner of the French judicial and police authorities in this field.

International information sharing is increasing in a way that is consistent and complementary with the expertise of the interested units.

PROCEDURES FOR INTERNATIONAL INFORMATION SHARING

THE DIFFERENT TYPES OF INFORMATION SHARING

The handling of requests through secure information-sharing networks is one of the key duties of the division responsible for managing Tracfin's international information sharing.

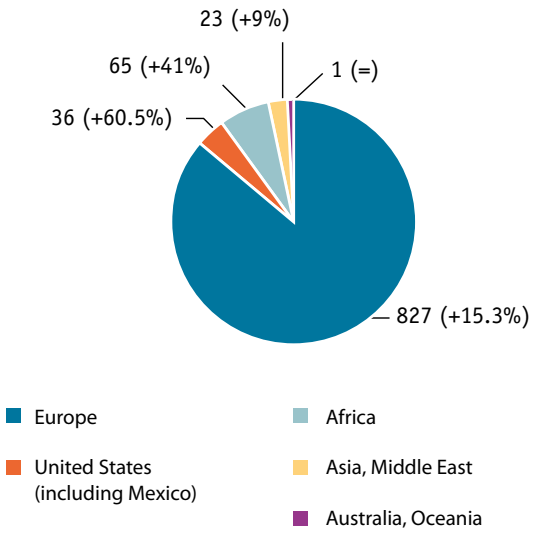
952 requests sent to Tracfin by foreign FIUs (incoming requests in 2013)

Tracfin plays a two-fold role in the information-sharing process. It is firstly obliged to respond to requests from other FIUs. In fulfilling this role Tracfin conducts general investigations aimed at responding to foreign requests. The questions asked are usually about Tracfin's knowledge of the individual or legal entity referred to by the foreign FIU or the existence of ongoing judicial proceedings in France. Secondly, Tracfin may also carry out in-depth investigations if these incoming requests reveal a potential for prosecution in France.

Requests from European FIUs have increased by 15.3%, which is a result of the clear determination of all of the European FIUs to promote international cooperation.

Also note an increase in the volume of requests from FIUs on the African continent which, for several of these FIUs, shows a trend towards operational «maturity».

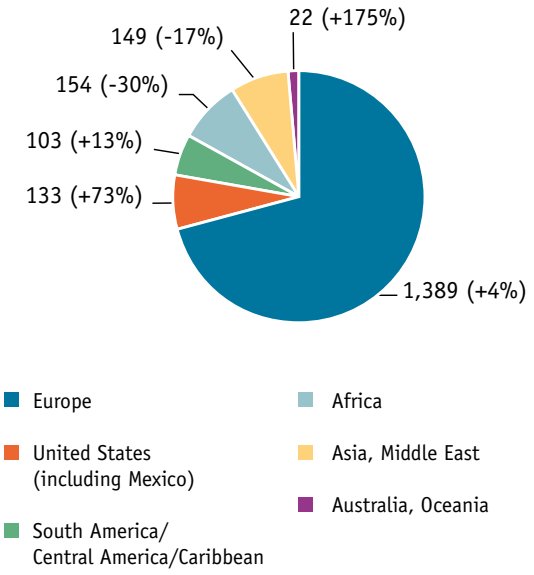
Incoming requests in 2013. Percentage change from 2012 to 2013



1,950 requests sent to foreign FIUs by Tracfin (outgoing requests in 2013)

The rise in the number of information requests sent to foreign FIUs continued in 2013. This increase reflects the growth in international cases. Tracfin's main partners are traditionally in Europe (1,372 outgoing requests). There was also a sharp rise in the number of requests sent by Tracfin to North America, however.

Outgoing requests in 2013. Percentage change from 2012 to 2013.



Spontaneous disclosures to foreign counterparts

Independently of the information sharing with foreign FIUs, Tracfin may spontaneously disclose some information to its counterparts. These disclosures result from analyses made based on domestic suspicious transaction reports received by the Unit. This means that some information may not only be disclosed to the national authorities, but may also be used internationally for the benefit of the relevant foreign FIUs. The number of these disclosures increased considerably in 2013, from 52 in 2012 to 90. The main recipients of these disclosures are still the FIUs of France's neighbours and some FIUs on the African continent.

Spontaneous disclosures to foreign FIUs may also provide them with information about facts that would not necessarily be analysed at national level but may be of interest to recipient FIUs.

EXAMPLE

A suspicious transaction report referring to the holding of funds by a foreign resident in an account opened in France.

The reporting entity's analysis reveals that all of these funds were repatriated to the foreign resident's country of origin. The foreign resident left France and closed his account. After investigations led by the Unit, the criminal record of the person involved suggested that this financial operation might be of interest to the public authorities of the relevant country. In this particular case, the Unit included permission for the foreign FIU to disseminate this information to its country's criminal justice system in its disclosure (see «Permission to disseminate», page 43).

TOOLS FOR INTERNATIONAL OPERATIONAL COOPERATION

The unit shares operational information with foreign FIUs through two secure networks: «Egmont Secure Web» and «FIU.NET».

FIU.NET is the secure, remote network for information sharing between the European Union's FIUs. In operational terms, it enables the exchanging of data between FIUs in even faster times than those recommended by the Egmont Group's good practices, including a «known/unknown»[1] ("hit"/"no hit")initial exchange. FIU.NET is funded by the European Union and by contributions from European FIUs and is currently used by 26 countries.

The «Egmont Secure Web» is a centralised exchange network used by the 139 FIUs that belong to the Egmont Group. This international division of Tracfin plays a centralising role in the management of the Unit's information exchanges with its foreign partners, due to its in-depth knowledge of the foreign FIUs. Its expertise allows it to manage both information requests from abroad and responses to the Unit's requests, which it is tasked with entering in Tracfin's IT system.

LEGAL PRINCIPLES

The legal value of a request sent by a foreign FIU

Information requests from foreign FIUs have the same legal value as suspicious transaction reports. Tracfin therefore has the same powers to respond to them, including exercising a power to obtain information against the relevant French reporting entities and requesting additional information from foreign counterparts other than the requesting counterpart. Since the introduction of the law on the separation and regulation of banking activities of 26 July 2013, suspicious transactions reported in an incoming request and not yet carried out can also now be stopped (see the 3rd part of this report in this regard)

The principle of reciprocity

Tracfin may share information with its foreign counterparts, particularly if the analysis conducted uncovers the existence of financial ties with third-party countries or any other information pointing to financial activity abroad. Similarly, a foreign FIU can question Tracfin if it has been informed in its own country about a suspicious financial transaction linked to France. **This information sharing is governed by the principle of reciprocity, which means that an FIU cannot request more information from a counterpart (or even disclose more) than the national legislation permits it to receive or disclose in its own country.**

CMF art. L.561-31

In practice, applying the principle of reciprocity can sometimes be complex and require detailed knowledge of the legal operational capacities of each foreign FIU, whose articles of association, prerogatives and working methods vary greatly.

For instance, the operating scope of some FIUs may be restricted by the legal foundations of their anti-money laundering system. While Tracfin has jurisdiction over the laundering of the proceeds of offences punishable with a custodial sentence of more than one year, some FIUs exercise their prerogatives within a more limited scope of crimes and offences. Some

1. «known» or «unknown» to the Tracfin database.

FIUs do not have jurisdiction over tax offences or the money laundering relating to them.

As a result, according to the principle of reciprocity defined above, although Tracfin is able to exercise a power toobtain information based on an incoming request, it will not be able to disclose the results of its analysis to its counterpart if it does not have the same powers.

Permission to disseminate

The information shared between Tracfin and its foreign partners is confidential. This principle of confidentiality implies that any dissemination of the information shared between FIUs to a third-party authority (judicial or police authority, tax authorities, customs, etc.) is subject to the prior approval of the FIU which transmitted the information. This requirement helps boost the information sharing between FIUs in both quantitative and qualitative terms. An express, written request must be made. This provides the FIU that discloses the information with a guarantee that the use of the information will be monitored.

Tracfin has defined **three levels of permission to disseminate information** depending on how it will be used abroad:

- the information shared between FIUs may only be used by these FIUs and cannot be disseminated without prior consent;
- Tracfin authorises the dissemination of its information to a foreign enforcement authority, which may use it under its own responsibility, as it sees fit, but without disclosing the origin of this information or including documents issued by Tracfin in any formal proceedings;
- the Unit exceptionally authorises the FIU to disseminate its information note and mention Tracfin's name.

There are some limits to the dissemination of information by Tracfin, however. Article L.561-31 of the CMF in fact prevents the Unit from disclosing financial information to a foreign FIU if judicial proceedings based on the same evidence are underway in France, as the goal of international administrative cooperation should not be to circumvent the rules of judicial mutual assistance between countries.

Tracfin may, however, transmit information about an ongoing judicial investigation to a foreign FIU to facilitate judicial mutual assistance if it does not relate to substantive aspects of the case and is limited to general information (such as the competent court, case number and name of the magistrate in charge of the investigation). In addition, if a foreign FIU discloses information likely to be used in judicial proceedings in France to Tracfin, if the FIU that disclosed this information gives its permission to disseminate it, the Unit may then forward this information to the competent court to add evidence to the proceedings in progress.

THE MAIN MONEY-LAUNDERING SCHEMES REPORTED IN 2013

A large proportion of the reports received by the Unit related to the offence of laundering the proceeds of the misuse of company assets or the fraudulent organisation of insolvency. These reports, which may also be analysed for concealment of part of the suspects' activity, often reveal the same fraud mechanism. The Unit receives information from a foreign FIU about a company X operating in France. It is mentioned that the company opened a bank account abroad. The information transmitted draws Tracfin's attention to the flows observed in this account (in the name of a director acting as the company's chief executive officer). Transfers by French clients are credited to the account, and these funds are then either withdrawn in cash or transferred to a personal account opened in the name of the director (or in the name of a member of their family) in the same foreign country, in a third-party country or sometimes even in France.

The number of reports of «false transfer orders» has also been rising in recent months. French companies are falling victim to computer hackers, who issue false transfer orders in the company's name to transfer funds to an account abroad. Most commonly, people visit the company claiming to be from the IT department of the bank with which the company has its account and ask the company for its access codes so as to test the IT migration of transfer orders to SEPA format. The funds are then fraudulently transferred to accounts opened in other European countries, usually in the name of individuals originating from these countries or bogus companies. These countries'FIUS then informthe Unit of ongoing judicial proceedings in their jurisdictions.

MONEY LAUNDERING CARRIED OUT IN FRANCE WHOSE PREDICATE OFFENCE HAS BEEN COMMITTED ABROAD

Tracfin receives a report of suspicious transactions relating to the purchase of property in France. The buyer does not provide any proof on the origin of thefunds used to acquire the property.. The investigations conducted reveal that the buyer represents a company registered in a European Union country. After the relevant European FIU was questioned, it was shown that the company involved is a shell company whose manager is a resident of a non-EU third-party country. After Tracfin questioned this second FIU, it appeared that the manager was a known active member of a criminal organisation. He has been charged in his own country with participation in the large-scale misappropriation of public funds.

THE INTERPLAY BETWEEN THE RULES GOVERNING INTERNATIONAL INFORMATION SHARING BETWEEN FIUS AND L MUTUALJUDICIAL ASSISTANCE

The dissemination of information by Tracfin is restricted if there are ongoing judicial proceedings in France. This restriction only covers information requested by a foreign FIU relating to the same people and the same evidence as those involved in the judicial proceedings. It is intended to prevent any risk of interference with the organisation of any mutual judicial assistance. However, it doesn't prevent Tracfin from disclosing information to its counterpart that would enable the French judicial authorities and the authorities of the requesting country to contact each other to start cooperating faster (competent court in France, contact details of the magistrate responsible for the case, proceedings registration number, investigating unit referred to, and so on).

TRACFIN'S STANDING WITHIN THE INTERNATIONAL COMMUNITY

TRACFIN'S CONTRIBUTION TO FATF AND MONEYVAL

The Financial Action Task Force (FATF) now has 34 member countries. Its current mandate (2012-2020) forcefully reiterates the objectives of this international organisation, which are to:

- define standards;
- promote the effective application of legislative, regulatory and operational measures to combat money laundering, terrorist financing and related threats to ensure the integrity of the international financial system.

FATF assesses the implementation of its standards by its members and the countries belonging to the 9 regional FATF-type groups. Tracfin's role within the French delegation is to manage the work led by the typology working group.

The Unit also participates in Moneyval's work and meetings. France is a full member of Moneyval, which is the Council of Europe's regional FATF-type group. France's special status, awarded by the Chairman of FATF to two of its member States, allows it to directly participate in Moneyval's work. This status was granted to France for the first time from August 2011 to August 2013 and has been renewed for two years. In 2013, France was therefore an ad hoc reviewer of the Moneyval report evaluating Israel. France is particularly concerned about consistency in the evaluations of different countries and was able to flag political or cross-cutting issues to the team of assessors for further examination, and inconsistencies with the evaluation reports previously adopted. A Tracfin employee also participated in the evaluation of the Romanian AML/CTF system in 2013 in an expert capacity. This evaluation report was discussed and adopted in a plenary meeting in spring 2014.

FATF's new evaluation methodology

After its 40 recommendations were adopted in February 2012, in February 2013 FATF published a new methodology for the evaluation of national AML/CTF systems. This now has two parts:

- evaluation of technical compliance, which relates to the country's legal and institutional framework, and the competent authorities' powers and procedures;
- evaluation of effectiveness, an innovation introduced by this methodology, which is designed to assess how well FATF's recommendations are applied and measure the effectiveness of the legal and institutional framework.

To ensure compliance with the terms of the ministerial mandate, the French delegation wanted the two parts to be closely aligned.

The first evaluations based on this new methodology began at the end of 2013. For money laundering and terrorist financing to be combated effectively, the standards must be met by as many countries as possible. To help to achieve this aim, Tracfin may second one of its experts to FATF to participate in one of the evaluations carried out using the new methodology.

TRACFIN'S CONTRIBUTION TO THE EGMONT GROUP: THE PROGRESS MADE AT THE PLENARY MEETING OF JUNE 2013

Following the revising of FATF's standards in 2012, the Egmont international group, which is responsible for the operational sharing of information between financial intelligence units, began revising its own standards. There were two opposing approaches. The first was to consider a limited raising of Egmont's standards, based on the argument put forward by certain countries whose intelligence-sharing laws are more restrictive. The second approach, which was supported by Tracfin, was to extend the powers of financial intelligence units and increase international cooperation.

This second approach was adopted at the Egmont Group's plenary meeting, held in South Africa in June 2013, after several months of negotiations.

This Egmont summit also resulted in significant progress in the sharing of information with the Swiss FIU. Given the need to comply with the Egmont Group's standards, Switzerland has in fact changed its laws. The federal law on the combating of money laundering now enables the Swiss FIU to exercise power to request further information and to disseminate information obtained in this way to its foreign counterparts. Tracfin will conduct a review of its information sharing with its Swiss counterpart in 2014.

THE CREATION OF THE CIRCLE OF FRENCH-SPEAKING FIUS

At a meeting of the Egmont Group in July 2012 in Saint Petersburg, the Canadian, Senegalese, Belgian, Luxembourg, Moroccan and French FIUs met to discuss common issues, particularly in the area of cooperation. Cross-border financial flows were found to reflect the historical and linguistic ties between these States.

Based on this finding, it seemed appropriate to create a structure that would bring together FIUs that share the same language (French) and common anti-money laundering and counter-terrorist financing issues.

The idea of an association or «Circle» therefore emerged, whose aims quickly took shape:

- improving mutual knowledge of people and investigative capacities between French FIUs and therefore sharpening up operational cooperation;
- exchanging good practices for dealing with shared anti-money laundering and counter-terrorist financing issues;
- facilitating the accession of French-speaking candidate FIUs to the Egmont Group by setting up dedicated training.

Given the real success of this project with French-speaking FIUs, the association was officially launched at the Egmont Group's meeting in January 2013 in Ostend. This resulted in the holding of a seminar in French on international cooperation during the plenary meeting of the Egmont Group in South Africa in 2013. The association also created a positive framework for the sponsoring of the FIUs of Algeria, Burkina Faso and Togo as future members of the Egmont Group. These three FIUs officially joined the group in July 2013.

In 2014, the circle plans to take steps to facilitate the exchanging of good practices to allow Chad's FIU to join the Egmont Group. The Crcle is also planning a seminar on information analysis and sharing for spring 2014..

TRACFIN'S PARTICIPATION IN THE WORK CARRIED OUT BY THE EUROPEAN UNION

In 2013, Europe saw the launching of negotiations on the proposed revision of Directive No. 2005/60/EC of 26 October 2005 (known as the «third money-laundering directive»), which was transposed into French law by order No. 2009-104 of 30 January 2009.

This proposal is aimed at revising the current European legal framework by notably supplementing it with the new obligations resulting from the recommendations issued at international level by the Financial Action Task Force (FATF). It is designed particularly to take into account certain specific requirements of the internal market that call for the defining of a common position for all of the member States and a more harmonised operation of the EU's FIUs. These specific requirements above all stem from the carrying out of cross-border transactions and the consideration of the need to analyse risks at supranational level and to introduce a minimum common base of applicable penalties.

Against this backdrop, Tracfin is participating in an expert capacity, as part of the French delegation, which includes the General Directorate of the Treasury and the Prudential Supervision and Resolution Authority (ACPR), in all of the working groups on the future 4th directive, organised both within the Council of Europe and within the Committee on the Prevention of Money Laundering and Terrorist Financing (CPMLTF), which became the EGMLTF (Expert Group on Money Laundering and Terrorist Financing) in June 2013.

The EGMLTF is tasked with assisting the European Commission with the defining of legal standards and policies and coordinating the exchanging of member States' positions. This group met 3 times in 2013, particularly to discuss the current negotiations on the 4th directive and the amendments made to the text by the various member States. Tracfin attended each of these meetings. The presidency of the Council of Europe, held by Ireland and then Lithuania, also called the members States' experts to Brussels for a dozen or so working meetings on the draft text of the 4th directive. At these meetings, Tracfin was able to defend the amendments suggested by France relating to the operation and cooperation of the EU's FIUs, which were in line with the proposals supported by the FIU-Platform to which the Unit belongs.

The provisions relating to the procedures for cooperation and information sharing between member States' FIUs were therefore debated at length. This debate was held particularly in the wake of the «Jyske Bank Gibraltar» Court of Justice of the European Union (CJEU) order, rendered on 25 April 2013, which declared that Spanish law was compatible with European law. Spanish law demands that credit institutions operating in Spain in keeping with the free provision of services regulations, disclose the information required for anti-money laundering and counter-terrorist financing purposes directly to the Spanish FIU, without going through the FIU of the State hosting the credit institution in question.

The conclusions of this order, based particularly on the lack of an adequate system of cooperation between FIUs, led the member States to take the CJEU's observations into account in the negotiations on the 4th directive to reinforce the mechanisms for information sharing between FIUs. The French delegation was able to suggest amendments to the draft text and so include new requirements. The very nature of cross-border operations, which are increasingly common due to the globalisation of financial flows, argues for clear, relevant provisions for the FIUs that are destined to receive information about transactions carried out in part or in whole in their country. FIUs must also be able to exercise their power to obtain information effectively in these situations. The goal is to ensure that the information effectively reaches the FIU of the Member State where it will be of most use, without filtering and without delay.

Other provisions should establish the operating independence and autonomy of FIUs, clarify the definition of a politically exposed person and of the effective beneficiary of legal structures such as trusts, strengthen the rules for the supervision of financial institutions within the European Union and consider special vigilance measures for the use of digital currencies, in accordance with FATF's recommendations.

BILATERAL COOPERATION

In furtherance of its strategy of reinforcing operational information sharing with its counterparts, Tracfin has received representatives from the UIF (the Italian FIU) to launch a joint project to introduce more systematic information sharing between the two units.

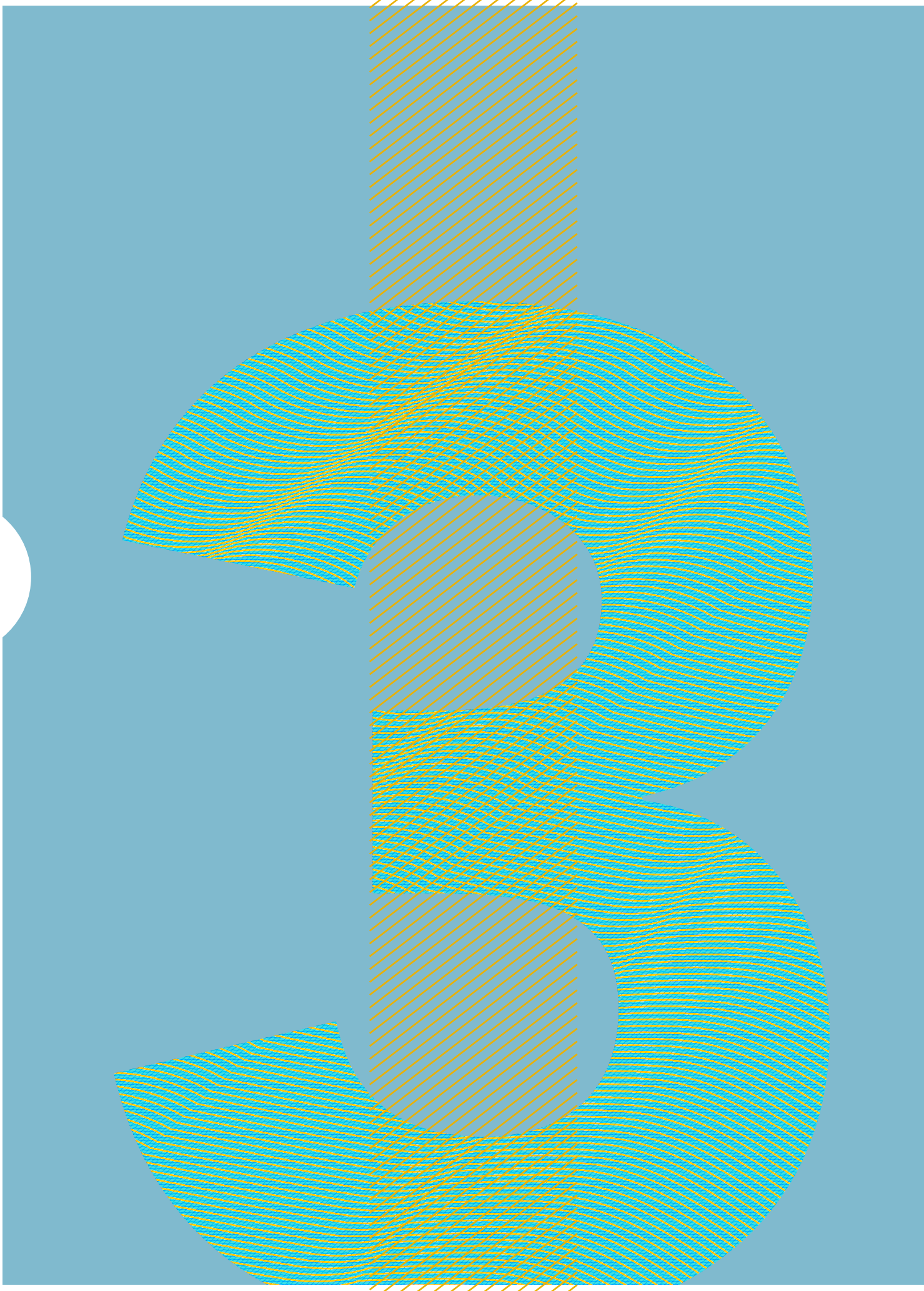
The Unit has also received the heads of the FIUs of Jersey (JFCU) and Guernsey (FIS) to develop information sharing with these partners and facilitate reciprocal arrangements for information dissemination.

Tracfin has continued its work to strengthen its cooperation with French-speaking FIUs, particularly by sponsoring Chad's FIU. Access to the Egmont Group depends on a procedure that requires an in-depth analysis of the candidate FIU's operation, from both a legal and operational viewpoint.

The Unit also welcomed its Vietnamese counterparts. This meeting enabled discussion about respective working methods and the defining of the terms for a closer collaboration between the two units.

As part of the cooperation between France and Albania, Tracfin was invited by the current security attaché in Tirana to train around twenty magistrates and judicial police officers in the combating of money laundering and corruption.

As a result of the increase in cross-border transactions, money-laundering techniques are becoming more complex and globalised and greater international cooperation has become a major requirement that all FIUs must now meet.



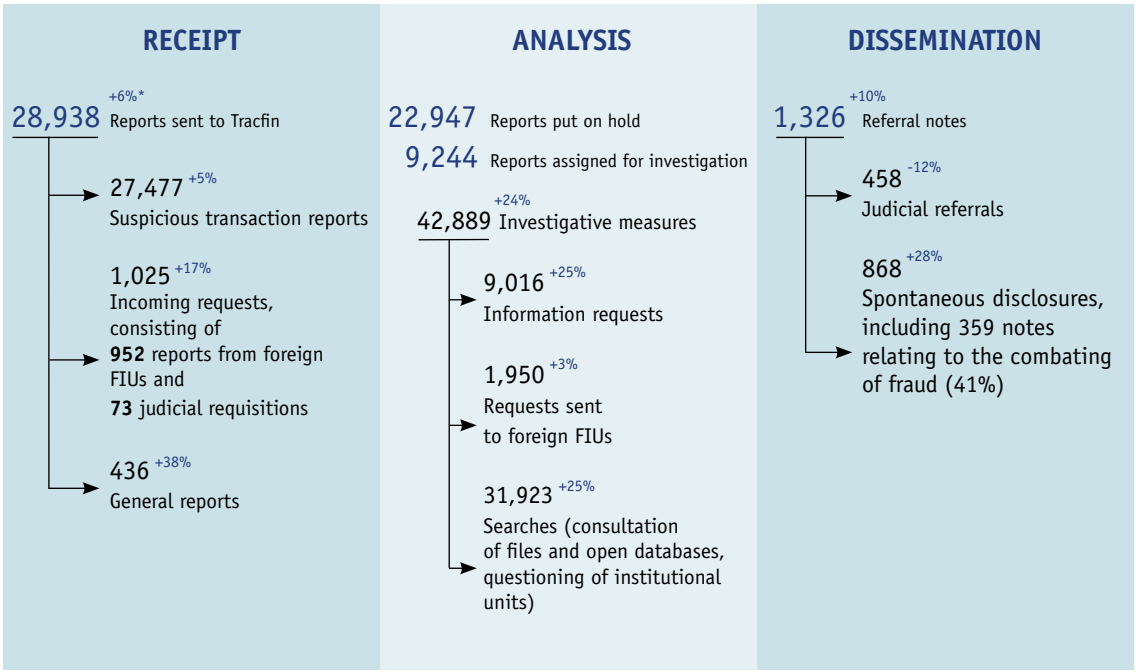
TRACFIN: FIGURES FOR 2013 AND ORGANISATIONAL STRUCTURE

TRACFIN'S ACTIVITY IN 2013

Tracfin's activity has grown considerably over the past five years as a direct consequence of its increased workload. Between 2008 and 2013, the number of reports received rose by 85% and the number of reports analysed by 155%. Over the same period, the Unit's budget was increased by 3% and its staff numbers by 40%, bringing the Unit's headcount to 89 employees.

REPORTS RECEIVED BY TRACFIN: A STEADY RISE IN 2013

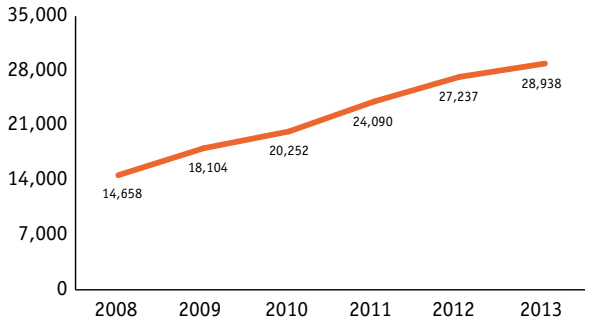
The growth seen in previous years has continued: the number of reports received by Tracfin increased by 6% in 2013 with 28,938 reports sent to the Unit (27,237 in 2012).



* Comparison with the figures for 2012

Three types of reports may be sent to Tracfin:

- **suspicious transaction reports** sent by entities subject to reporting obligations;
- **reports** sent by State departments and people entrusted with a public service mission;
- **reports sent by foreign FIUs** (see part 2).



Reports received by Tracfin between 2008 and 2013.

THE TRANSMISSION OF SUSPICIOUS TRANSACTION REPORTS

Since the second half of 2013, reports have been transmitted to Tracfin by reporting entities using the following two methods:

- the Ermes e-reporting system, which is mandatory **for financial entities**;
- the mandatory electronic form (www.economie.gouv.fr/Tracfin)

or sent by fax or post, **for non-financial entities** opting not to use Ermes.

Suspicious transaction reports

Entities subject to reporting obligations must report all sums recorded in their books or transactions relating to sums that they know, suspect or have good reason to suspect are of fraudulent origin to Tracfin.

CMF* art. L.561-15 à L.561-27

In 2013, 95% of the reports received by Tracfin were sent by reporting entities, in other words 27,477 suspicious transaction reports (+5% versus 2012).

The Unit may receive tax reports in addition to «traditional» STRs.

*Code Monétaire et Financier (Monetary and Financial Code)

Reporting activity of reporting entities (2009-2013)

	2009	2010	2011	2012	2013
Banks, credit institutions	12,254	13,206	15,582	19,288	21,950
Money changers	2,249	3,002	3,251	2,104	1,199
Insurance companies	1,007	808	889	1,059	1,169
Payment institutions	N/A	0	290	1 218	831
Money-issuing institutions	675	608	779	436	259
Investment firms	67	134	133	52	46
Mutual insurance companies and benefits institutions	58	56	98	35	60
Financial investment advisers	46	78	92	20	20
Insurance intermediaries	2	3	40	38	25
Settlement system participants	0	0	1	1	0
Portfolio management companies	3	10	10	13	20
Total for all financial reporting entities	**16,361**	**17,905**	**21,165**	**24,264**	**25,579**
Notaries	370	674	1,069	995	970
Organisers of games of chance, and sports and horse-racing betting	361	269	73	120	127
Casinos	30	137	149	171	153
Court-appointed receivers and trustees	57	55	62	52	82
Accountants	55	98	135	145	195
Real estate entities	33	14	19	34	54
Auditors	22	46	57	54	72
Dealers in precious goods	12	2	13	3	12
Auctioneers, auction houses	5	8	16	7	25
Bailiffs	2	0	17	14	18
Lawyers	2	0	1	4	6
Commercial registered office providers	0	0	4	21	3
Online gambling operators	N/A	0	76	127	181
Sports agents	N/A	0	0	0	0
Total for all non-financial reporting entities	**949**	**1,303**	**1,691**	**1,747**	**1,898**
Total for all reporting entities	**17,310**	**19,208**	**22,856**	**26,011**	**27,477**

With 27,477 suspicious transaction reports received, the upwards trend (+5.6%) continued, but at a slower rate than in previous years. The number of STRs received from non-financial entities rose (+8.6%) due to a handful of reporting entities. The reporting activity of the different entities remains very uneven, however.

The majority of **suspicious transaction reports are still made by reporting entities from the financial sector** (25,579 in 2013 versus 24,264 in 2012), although this increase was less pronounced than in previous years (+5.4% in 2013 versus +14.6% in 2012 and +18.2% in 2011). Out of the reporting entities in this sector, the share of the STRs from banks and credit institutions rose particularly sharply, to 86% in 2013 from 79% in 2012.

With 21,950 suspicious transaction reports sent, banks and credit institutions remain the leading contributors to the anti-money laundering and counter-terrorist financing system.

The number of reports received from non-financial reporting entities rose slightly, from 1,747 in 2012

to 1,898 in 2013. Notaries, who accounted for 51% of the STRs, continue to be the largest contributors in the non-financial sector.

Tracfin believes that entities subject to reporting requirements need to set up warning systems using a risk-based approach. This means that vigilance measures must be constantly adapted. For example, vigilance criteria must be differentiated according to the socio-economic profiles of clients, the geographical zone where the transaction was completed, the opacity and complexity of the economic and/or legal structures, and so on. Reporting entities should also regularly revise their vigilance criteria. The detection criteria adopted must be updated, in fact, as money launderers very quickly learn to get around the measures and warnings introduced. Each reporting entity must therefore constantly adapt their vigilance system.

AWARENESS RAISING OF REPORTING ENTITIES

Throughout the year, Tracfin regularly organises meetings with each sector's representatives. They take place in the form of bilateral meetings or events that bring together the financial security heads of major groups. The introduction of advisers within Tracfin has also improved communication with reporting entities.

Main Tracfin events in 2013:

- 11 January: Tracfin and the ACPR organised a bank AML event
- 6 January: AML event for auditors
- 7 March: meeting with the SCCJ (also on 27 June)
- 29 May: meeting with the ARJEL (On-line Gaming Regulatory Authority) (also on 2 July and 9 September)
- 29 May: meeting with the Chambre Nationale des Commissaires-Priseurs Judiciaires (National Association of Auctioneers)
- 4 and 30 July: meetings with the IFPPC
- 3 October: review of the CSN's awareness-raising initiatives following the Tracfin/CSN working group
- 28 November: participation in the training day organised by the CNAJMJ
- 11 December: meeting with the FDJ (also on 4 July)
- 13 December: meeting with the AMF

Created on 10 December 2009, the CNS (National Supervisory Committee) defines the procedures for monitoring compliance with the obligations imposed on entities subject to AML/CTF system requirements.

These procedures govern so-called «orphan» reporting entities, which are in the non-financial sector and are not supervised by a professional association, namely estate agents, commercial registered office providers, casinos and online gambling operators. The CNS is chaired by Francis Lamy, who was appointed by decree on 22 November 2013.

The committee's creation therefore deals with one of the main criticisms made by the international Financial Action Task Force (FATF) of the oversight of non-financial reporting entities in France.

General reports

CMF art. L.561-27

Aside from suspicious transaction reports, Tracfin also receives information transmitted by various public bodies or bodies with a public service mission. This includes State authorities, local authorities, financial courts, public institutions or any other person with a public service mission.

The Unit also receives reports connected with money-laundering activities identified by supervisory authorities and professional associations as part of their duties. Reports transmitted in this way have the same legal value as suspicious transaction reports. They can be used as a basis for in-depth investigations by Tracfin.

CMF art. L.561-30-II

In 2013, 436 general reports were received by Tracfin (314 in 2012).

The State authorities that sent the most reports were our partners within the intelligence community and the Ministry of the Economy and Finance (DGFiP, DGDDI and DGTPE). They sent 367 reports.

There was a large increase in reports from the supervisory authorities, mainly from the Prudential Supervision and Resolution Authority (ACPR), which sent 51 reports. This trend is due in part to a provision of the law on the separation and regulation of banking activities of 26 July 2013, which expands the scope of the information that Tracfin may receive.

The following information must be included in a general report:

The reports received must contain at least the following information to allow their full use:

- the exact identification of the person(s) involved, if possible accompanied by proofs of identity and address;
- the description of their activities and the financial flows registered on their account(s);
- the details of the financial instruments used (bank account number, etc.);
- all the documents required to assess the situation described as thoroughly as possible.

CLARIFICATION OF THE REPORTING OBLIGATION OF SUPERVISORY AUTHORITIES

The scope of the information that may be reported to Tracfin by supervisory bodies (ACPR, AMF or any other supervisory authority) was expanded by **law No. 2013-627 of 26 July 2013 on the separation and regulation of banking activities** to any sum or transaction covered by article L.561-15, in accordance with the reporting obligations to which reporting entities are subject in line with article L.561-15 of the Monetary and Financial Code.

This information must now be transmitted «without delay» to Tracfin. **The adding of this provision confirms that it is mandatory for these authorities to send information uncovered through checks conducted by them** as soon as possible.

Conditions for the admissibility of suspicious transaction reports

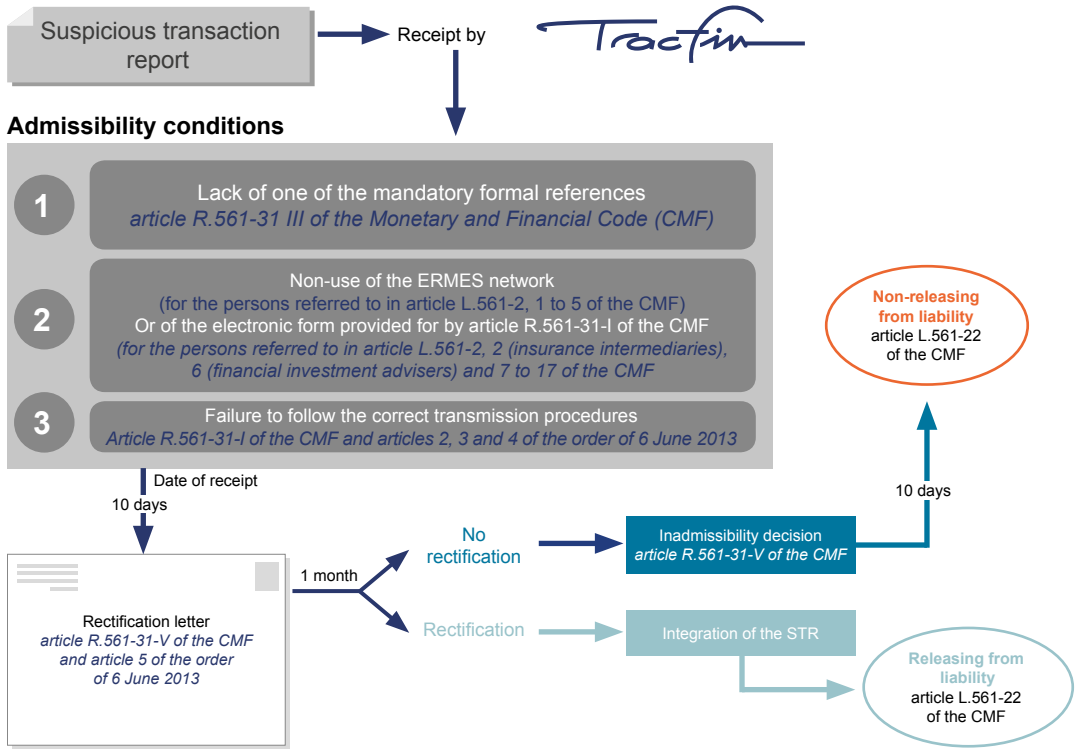
CMF art. L.561-15 et R.561-31

2013 saw some major regulatory changes. Two regulations relating to transmission procedures and the conditions for the admissibility of suspicious transaction reports were signed into law on 6 June 2013 (*Journal Officiel de la République Française* (JORF) of 8 June 2013)[1].

As a result, since 1 September 2013, STRs may be considered to be inadmissible if they don't include the following information:

- The profession practiced by the person who submitted the report by reference to the categories referred to in article L.561-2;
- Identifying information and professional contact details of the reporting entity designated in accordance with the provisions of article R.561-23;
- Reporting scenario by reference to the scenarios referred to in paragraphs I, II and V of article L.561-15;
- Information identifying the client and, where appropriate, the beneficial owners of the transaction reported and, if a business relationship has been entered into with the client, the purpose and nature of this relationship;
- Description of the transaction and analysis points that led to the report being made;
- Execution date if the transaction has not yet been executed.

Circuits and procedures for checking the admissibility of a suspicious transaction report.



1. **Decree** (No. 2013-480) amending article R.561-31 of the CMF, defining the conditions for the admissibility of suspicious transaction reports in accordance with article L.561-15 of the CMF; Order (known as the «Ermes» order) enacting the new provisions of article R.561-31 of the CMF, defining the procedures for the transmission of suspicious transaction reports made in accordance with article L.561-15 of the Monetary and Financial Code (CMF) and, for informing reporting entities about the inadmissibility of suspicious transaction reports.

In the first six months of these rules' implementation (July to December 2013), out of the **589 suspicious transaction reports received in paper format, the Unit recorded 276 inadmissible STRs. 10 reports came from the financial sector and 266 from the non-financial sector.**

Since 1 September 2013, when the rules governing the non-financial sector became effective:

171 letters have been sent declaring inadmissibility. 162 letters were sent to the non-financial sector and 9 to the financial sector;

540 phone contacts were made on the Unit's initiative.

In sum, 46 letters were sent declaring the inadmissibility of an initial suspicious transaction report, all to the non-financial sector.

The most frequent omissions were handwritten suspicious transaction reports, failure to use the dedicated form (available on the Tracfin website), failure by the reporting entity to sign the suspicious transaction report or the incomplete identification of the signatory and a lack of information identifying the client.

Find out more:

Questions-réponses : la recevabilité en 8 points (FAQ: admissibility in 8 points) (October 2013) (www.economie.gouv.fr/Tracfin/lettres-dinformation-aux-professionnels)

Information that must be systematically reported to Tracfin: «COSI», an innovation in 2013

Reporting practices changed in 2013 with the creation of systematic information disclosures (COSI).

CMF art. L.561-15-1 alinéa 1 et D.561-31-1

Credit, payment and digital currency institutions must now send Tracfin information relating to certain fund transfer transactions carried out through a cash transfer or using a digital currency.

Note that a COSI does not require any analysis by the reporting entities and is not used to report a suspicion. It cannot be used as grounds for the conducting of investigations by Tracfin and does not release the reporting entity from criminal, civil or professional liability. However, the information disclosed within this framework adds substance to ongoing investigations.

Since 1 October 2013, information about fund transfer transactions of a unit amount of greater than or equal to € 1,000 has been disclosed to Tracfin through the Ermes e-reporting system.

On 1 April 2014, it also became compulsory to report transactions totalling more than € 2,000 per client per calendar month using Ermes.

CMF art. L.561-15-1 alinéa 2

A Council of State decree that should be published in 2014 will also expand the scope of systematic information disclosures. Consultations and discussions with reporting entities on this issue began in December 2013.

REPORTS ANALYSED BY TRACFIN

Additional information that builds up and develops the context surrounding a reported suspicion is brought together so as to decide whether or not an information note should be sent to the public prosecutor's office, partner authorities or foreign financial intelligence units. Searches are carried out through «investigative measures» (see below). This first analysis stage is used by Tracfin to decide how it will move forward with the case.

All of the reports received by Tracfin are analysed and redirected by the Unit. 9,244 reports were examined in greater depth in this way in 2013.

Redirecting of the reports analysed by Tracfin

How a report is redirected determines how it will be handled. Redirecting may result in:

- An investigation: during this phase the investigators use their legal powers such as their power to obtain further information;
- Putting on hold: if the report appears to be potentially unusable or if any doubts are resolved after an investigation (in this case, the report will not be referred). The report may be reused, however, if new information is subsequently received by the Unit. Tracfin may in fact reactivate old reports received within the past ten years to add substance to a newly received report.

Out of the 9,244 reports analysed in depth in 2013, 7,624 reports were received in 2013 and 1,620 were already in the Unit's possession.

Developing of reports and the main investigative measures.

Investigative measures take the form of documentary searches to develop a suspicion reported by a reporting entity or contained in a report. They involve exercising the power to obtain further information, directly or indirectly consulting databases (bank accounts file – Ficoba -, tax authority or customs files, company data or gendarmerie or police files), mining open databases and questioning other intelligence units, foreign intelligence units or other State authorities.

Tracfin carried out 42,905 investigative measures in 2013.

The power to obtain further information

The Unit's investigative measures included the sending of 9,016 information requests, rising by 25% from 7,221 requests in 2012.

2013 saw a major IT development in 2013 with the use of the Ermes platform for secure document exchanges. **On 3 June 2013, Tracfin in fact launched a new functionality for e-reporting system users named «échange sécurisé de fichiers» or ESF (secure file exchange)**. Using the ESF Tracfin is able to send information requests in electronic form, thus enabling reporting entities to respond through the same channel. The aim is to ensure that the information transmitted is more secure and its confidentiality is increased. The system also improves the traceability and follow-up by reporting entities of the reports that they send*.

3,303 information requests were sent through Ermes between June and December 2013.

*New mandatory suspicious transaction report transmission procedures) (November 2012) on the Tracfin website (www.economie.gouv.fr/Tracfin/lettres-dinformation-aux-professionnels)

Power to suspend transactions

In 2013, the Unit exercised its power to oppose the execution of a transaction 16 times

The Unit uses this prerogative with caution as it effectively entails informing the client whose funds or transactions have been temporarily frozen. This power is exercised in close collaboration with the judicial authorities and only in cases where there is an immediate risk that the suspicious funds identified may be taken out of the account through cash withdrawals or transfers to uncooperative foreign countries.

CMF art. L.561-25

Since 2013, Tracfin has been able to exercise its power to suspend transactions based on any suspicious transaction reports or information received from reporting entities, the authorities or foreign FIUs, even without having previously received an STR from the entity responsible for the transaction. Thepower to suspend transactions may be exercised at any time before the transaction's execution. The period during which the transaction is suspended has been increased to 5 business days.

Tracfin requests sent to foreign FIUs

The number of requests sent by the Unit to foreign financial intelligence units (FIUs) has been steadily increasing for the past few years. A 2.2% rise was recorded in 2013 (1,933 requests versus 1,891 in 2012).

REFERRING OF THE REPORTS ANALYSED

In 2013, Tracfin produced 1,326 referral notes (+10% from 2012) including:

- **458 notes sent to the judicial authorities;**
- **868 notes sent to State authorities, including 237 sent to the tax authorities and 80 to social security bodies.**

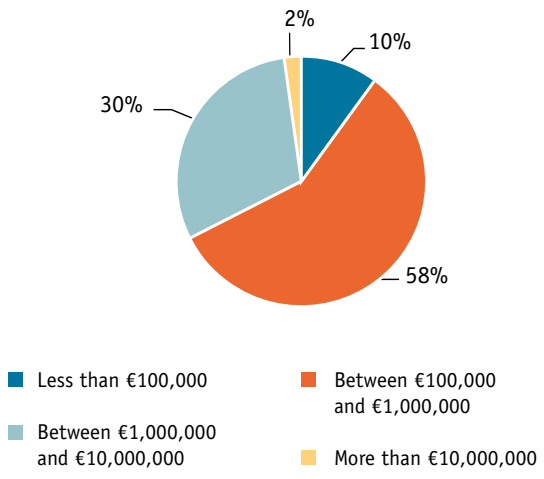
A fall in the number of court referrals

458 cases were referred by Tracfin to the courts in 2013 (versus 522 in 2012). Thisdecrease is particularly due to the referring this year of cases that were particularly complex or involved large sums that required the specific assistance of certain investigators from within the Unit. It can also be traced to the nature of the reports eligible for referral to other authorities.

According to the information available at the Unit's the financial amounts at stake in these referrals may be estimated at € 766 million in 2013.

Out of the 458 cases referred, 51 concerned an amount of less than € 100,000, 257 an amount of between € 100,000 and € 1 million, 139 an amount of between € 1 million and € 10 million and 11 in excess of € 10 million.

Estimated value of cases



ORIGIN OF REPORTS AND DEFINING OF THE OFFENCES GIVING RISE TO REFERRAL TO THE COURTS

A court referral may result from several reports received by the Unit. Many cases may be put together by combining reports from different reporting entities operating in different sectors. The number of reports received by Tracfin cannot therefore be compared against the number of cases referred by the Unit without taking this key fact into account.

Given the nature of the Unit, all the investigations that it conducts concern suspected money-laundering activities. Tracfin uncovers a body of reasonable evidence that suggests that offences have been committed and may suggest the category of offence that the activities fall under in its referral note. This categorisation is purely a suggestion and in no way commits the judicial authorities, which are alone authorised to decide what action to take in response to the Unit's reports. It merely reflects Tracfin's assessment based on the information at its disposal.

A court referral may also help to ultimately reveal other facts that could not have been detected by the reporting entity or by Tracfin, either at the STR stage or during the subsequent administrative investigation by the Unit.

When cases are referred to the courts, the judicial proceedings often bring to light much higher amounts than those initially reported by the Unit.

In 2013, the five categories of predicate offence that were the most frequently reported were tax offences, undeclared work, fraud, the misuse of company assets and breach of trust. There was also an increase in the number of cases of alleged abuse of weakness this year.

The Paris Court of Appeal once again received the most court referrals, receiving 182, including 101 for the Paris District Court alone

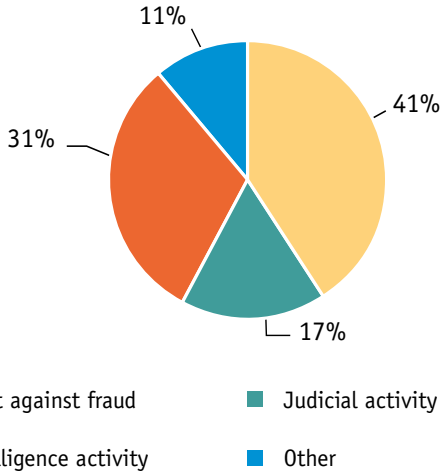
A significant increase in spontaneous disclosures

CMF art. L.561-29 et L.561-31

Tracfin is authorised to disclose financial intelligence to the judicial police, the customs authorities and specialist intelligence units (if the information «relates to activities that pose a threat to the fundamental interests of the Nation in matters of law and order and State security»), the tax authorities, social welfare bodies and foreign financial intelligence units.

Since 2012, the Unit has also been able to disclose information to the State departments in charge of setting up and implementing measures to freeze or prohibit fund movements or transfers, financial instruments and economic resources, providing that it is in connection with the performance of their duties.

Breakdown of spontaneous disclosures by sector in 2013



■ An innovation in 2013: disclosures to the judicial authorities

CMF art. L.561-29 II

Tracfin may now spontaneously disclose information that does not suggest that a criminal offence has been committed but may, however, usefully contribute to an ongoing court case. It makes these disclosures to the judicial authorities using the model of disclosures to to the customs authorities and the judicial police.

The relevant judicial authority may therefore receive information that it seems useful for it to know and that it is able to use and investigate further, either in connection with a criminal investigation or for other purposes.

While the information disclosed by Tracfin may not report a criminal offence, it must be connected with the activities referred to in paragraph I of article L.561-51 of the Monetary and Financial Code and the magistrate's duties.

For example, it may be:

- **information held by Tracfin** about a company subject to insolvency proceedings;
- **information about a company** that is the apparent purchaser of a company in court-ordered liquidation.

In these first two cases, the information may be sent either to the public prosecutor's office or the commercial court, based on a case-by-case appraisal according to the nature of the information;

- **information about the registered address or contact details of a person** for whom a search or arrest warrant has been issued, which may be sent directly to the magistrate who issued the warrant;
- **objective/descriptive information about financial flows or transactions** that do not constitute offences but may provide information about the related context or environment that usefully contributes to ongoing judicial proceedings, which may be directly sent to the magistrate in charge of the case, particularly prior to a hearing by an investigating judging or a sentencing hearing to give guidance to the court;
- **information about the alleged vulnerability of an isolated person** who is not subject to any protective measures, such as a trusteeship or guardianship, that may be sent to the public prosecutor's office, which may assign the case for criminal investigation and/or refer it to the guardianship judge;
- **financial information about a convicted person who has fines or damages and interest to pay,** which may be transmitted to the judge in charge of sentence enforcement or to the public prosecutor's office's in charge of sentence enforcement.

As with any disclosure by the Unit, the source of the information will be strictly protected. Tracfin's legal adviser, who is not obliged to issue an opinion in such cases, will also be consulted before information is sent to the judicial authorities to assess the advisability of such a disclosure.

Furthermore, the information note sent to the competent judicial authority on this basis will constitute a pleading that may be included in the case file.

Finally, note that information is spontaneously disclosed to magistrates on an exceptional basis and that Tracfin mainly sends information notes to the public prosecutor's office. These disclosures are also not intended to replace spontaneous disclosures to the judicial police, through which Tracfin is able to directly disclosure information of use in ongoing investigations.

In 2013, Tracfin made 6 spontaneous disclosures to the judicial authorities.

Disclosures to intelligence units

The number of disclosures to intelligence units rose by 28% in 2013 compared to 2012. This increase is the result of the shared determination of the six units that make up the intelligence community to improve the quality and quantity of the information shared.

Disclosures to the tax authorities

The rampup of Tracfin's anti-tax fraud activity continued in 2013 (+41% versus 2012) with a total of 237 notes sent to the DGFiP.

The amounts involved total € 285m, representing an average of € 1.2m per case. 5 cases exceeded the € 10m threshold, while € 29m was the highest amount for an individual case.

TRACFIN AND THE DGFIP

Tracfin has been closely collaborating with the General Directorate of Public Finances (DGFiP) since 2009, increasing the amount of information that they share. The results achieved to date are illustrated by the sharp growth in the number of information notes transmitted by Tracfin. This growth is due to:

- an increased number of suspicious transaction reports relating to tax matters from reporting entities;
- the tax issues involved in a large number of cases of different types;
- the creation of a division in 2012 specialised in the developing of information relating to tax and social security fraud and its detection.

The signing of an information-sharing agreement with the DGFiP has also facilitated the disclosure of tax-related intelligence.

The reports sent by Tracfin are all used by the tax authorities, which validate the information in tax terms and redirect cases as appropriate, for example proposing an external tax inspection or the starting of judicial proceedings or referring them to the DGFiP's inspection departments.

Since 2009, this collaboration has resulted in 561 tax inspection or personal tax assessment proposals, leading to the collection of €€508 million in duties and € 183 million in fines.

Disclosures to social security bodies

In 2013, Tracfin's involvement in social entitlements cases was consolidated by the signing of an information-sharing agreement in April 2012 with the social welfare bodies. 80 notes were sent in 2013, representing a 78% rise (45 notes in 2012), with an increase of more than 50% for the *Agence central des organismes de Sécurité sociale* or ACOSS (Central Agency for Social Security Bodies).

An estimated € 29m were at stake, with an average of € 0.4m per case (versus € 14m in 2012).

The different types of fraud identified are based on the following practices:

- **for social security contribution fraud:** undeclared work and use of undeclared labour, reducing by companies of the base for the calculation of their social security contributions by concealing a varying proportion of their professional activity, concealed activity and cases involving the employing in France of workers from other European Union countries by structures not registered with URSSAF (Social Security and Family Allowance Contribution Collection Offices) in France;
- **for social security benefit fraud:** carrying out regular undeclared work while at the same time collecting unemployment benefit, fraudulent collection of RSA (Earned Income Supplement) or any other benefits dependant on the recipient's income;
- **misappropriation of retirement benefits**

As in 2012, such cases were most commonly found in the construction sector. The main practices identified were the use of undeclared work and the failure to declare an activity. In the security and trade sectors, which are also sensitive to fraud, the cases brought to the Unit's attention were mainly based on concealed activity or the partial concealment of an activity.

EXAMPLES OF THE MISAPPROPRIATION OF PUBLIC FUNDS OR MONEY LAUNDERING INVOLVING RETIREMENT BENEFITS.

Tracfin, in partnership with the CNAV's anti-fraud department, investigated retirement benefits fraudulently paid to people known as «collectors» to the detriment of the real beneficiaries. This type of «collection account» case is based on the appropriation by a «collector», who may be an individual or legal entity, of flows from several accounts held by other people who are recipients of social security benefits.

As a result of this work collectors, including some trustees, were able to be identified. These collectors' accounts often collected sums from several dozens of accounts held by individuals. The financial flows linked to the use of this money were also able to be retraced. The aim was to ultimately prove that the pension payments were not being used for their initial purpose and only marginally benefited the pensioners registered with the CNAV.

Evidence of various schemes was found in the accounts involved:

- **Mechanism 1: collection followed by cash withdrawals.** A trustee completes transactions in several bank accounts receiving pension payments. The accounts are regularly emptied through cash withdrawals. The effective destination of the funds remains unknown.
- **Mechanism 2: collection followed by bank transfers abroad.** The bank account of a «collector» regularly receives transfers from several pensioners' accounts. The sums are then credited to a bank account held abroad by the collector.
- **Mechanism 3: collection followed by the purchasing in France of various consumer goods.** The bank account of a «collector» regularly receives transfers from several pensioners' accounts. Cheques or transfers issued to companies operating in various sectors of activity (production and trading of grains, wholesale trading of equipment and cars, trading of food products and textiles, etc.) are debited from the account.

■ Disclosures to the customs authorities

In 2013, 42 information notes were sent to the General Directorate of Customs and Excise (DGDDI – excluding the National Directorate of Customs Intelligence and Investigations – DNRED). This total is stable compared to 2012 (41 notes sent).

The notes mainly regarded suspicions of a failure to meet reporting obligations relating to cross-border transfers of cash or cheques (45% of the notes) and counterfeiting (21%).

The other alleged suspicions are highly diverse. They include customs irregularities in the form of non-existent or false import or export declarations (10%), as well as the trafficking of works of art, drugs, the laundering of the proceeds of customs offences, offences relating to indirect taxes and non-compliance with the Washington Convention on the protection of wild fauna and flora and endangered species.

Ten reports were also sent directly to the DNRED. These concerned commercial transactions involving dual-use goods or goods that breached the embargo on Iran, or transactions relating to weapons or warfare equipment.

Tracfin has also assisted with various requests from customs units, within both a judicial (SNDJ) and administrative (DNRED) framework.

THE SIGNING OF THE INFORMATION-SHARING AGREEMENT WITH THE DGDDI

An information-sharing agreement was also signed by the DGDDI and Tracfin in 2013. The purpose of this agreement was to increase the effectiveness of the anti-money laundering and counter-terrorist financing system and of the measures to identify criminal assets and illicit financial flows. The agreement also reinforces the coordination between the two units so as to ensure an optimum, effective complementarity in the performance of their respective duties. The agreement also provides for the seconding of a DGDDI liaison officer to Tracfin. He took up his post in April 2014.

■ Disclosures to the supervisory authorities

CMF art. L.561-30

Tracfin sent 7 information notes to the supervisory authorities. These notes were about cases where Tracfin believed, based on the information at its disposal, that a reporting entity had failed to meet its vigilance and/or reporting obligations.

Responses to institutional partners' requests

• Information received from foreign FIUs

Requests for information from foreign FIUs are handled by the Unit like suspicious transaction reports. Based on these requests, Tracfin may therefore exercise the same powers as when investigating STRs submitted by reporting entities. In 2013, Tracfin received 952 information requests from foreign FIUs (+17% versus 2012).

• Judicial requisitions

Magistrates and criminal investigation depart-ments may send two types of judicial requisitions to Tracfin's director as part of their investigations. The purpose of these requisitions may be to obtain:

– **any information held by Tracfin** that may shed light on an ongoing investigation. Tracfin received and processed 73 judicial requisitions in 2013 (versus 84 in 2012) issued by magistrates or judicial police officers. This slight fall in the number of judicial requisitions is largely due to the sharp increase in 2013 in the judicial authorities' prior contacts with the Unit's magistrates or liaison officers to assess whether or not a requisition should be issued based on the information held by the Unit;

THE COUNTER-TERRORIST FINANCING UNIT'S ACTIVITY IN FIGURES

In 2013, the unit worked on nearly 200 cases, around 40 of which were referred to the judicial authorities (4 judicial referrals) and/or intelligence units (34 spontaneous disclosures). In addition to the referrals, 280 reports were analysed, a two-fold increase from 2012.

A total of more than 3,300 investigative measures were carried out by the Unit's employees, including 1,233 information requests issued to entities subject to AML/CTF obligations. Nearly 1,200 requests were made to the judicial police and intelligence units, and 74 requests to foreign financial intelligence units.

– **the disclosing of a suspicious transaction report, solely in cases where a criminal investigation reveals that the reporting entity might be involved in the money-laundering or terrorist-financing scheme exposed.** In 2013, Tracfin received 8 judicial requisitions aimed at incriminating a reporting entity, 3 of which were financial sector entities and 5 non-financial sector entities.

CMF art. L.561-19 II

Note: the judicial authorities or judicial police officers cannot use a warrant or requisition to obtain the disclosing of a suspicious transaction report **directly from a reporting entity**. The principle of confidentiality in the reporting of suspicious transactions is in fact enforceable against the judicial authorities and judicial police officers, who may never request the disclosure of a suspicious transaction report. Reporting entities may, however, inform them that they have disclosed information to Tracfin.

TRACFIN'S ORGANISATIONAL STRUCTURE

Tracfin originally reported to the General Directorate of Customs and Excise before the Unit was given national jurisdiction in 2006, under the dual supervision of the Economy and Budget ministers. The Unit was reorganised in 2011 and 2012 in response to the expanding of its remit by the order of 30 January 2009. It is now under the exclusive authority of the Ministry of Finance and the Public Accounts.

The Unit's operations are now organised around two departments, two specialised units and an expanded legal division:

- **an analysis, intelligence and information department (DARI)** responsible for collecting and redirecting STRs, analysing financial intelligence and managing relations with reporting entities and international bodies;
- **an investigation department (DE)** that conducts the in-depth investigations needed to handle the cases that require them;
- a unit dedicated to the handling of terrorist-financing cases;
- **a strategic analysis unit;**
- **a legal and judicial division** staffed by the legal adviser and her deputy, who are judicial magistrates, and three liaison officers (from the General Directorate of the National Gendarmerie, the Central Office for the Prevention of Serious Financial Crime and the Central Office for the Combating of Corruption and Financial and Tax Offences).

The Unit is also supported by:

- **an Administrative and Financial Affairs Department (DAAF)**, which is responsible for the Unit's support functions, budget and human resources management;
- **an information system office** tasked with the operation and development of Tracfin's information system.

A YEAR OF CHANGES FOR THE UNIT

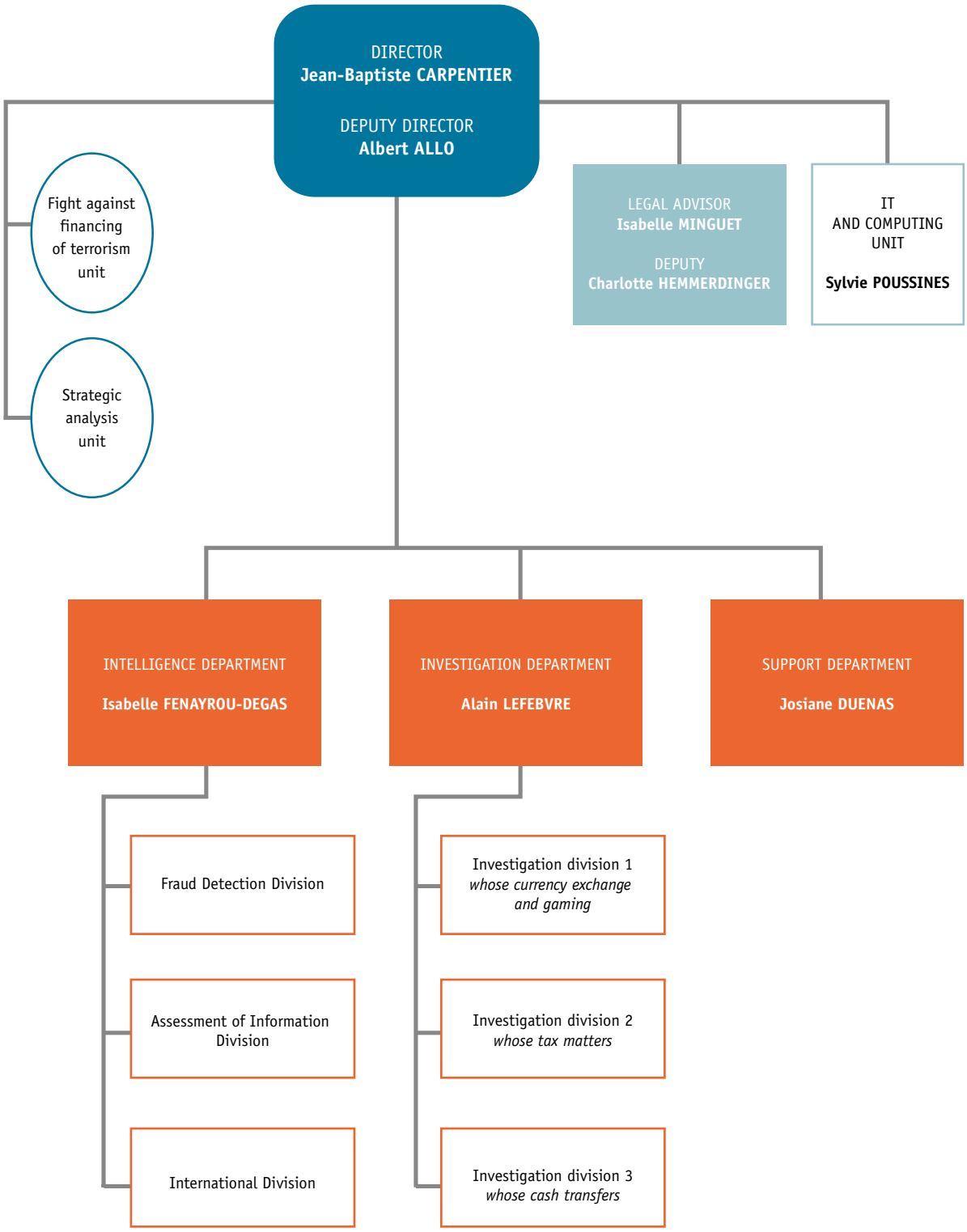
The development of the IT office

The Information System Office was set up on 1 October 2013 in response to the Unit's changing circumstances. Its two divisions are responsible for the operation and development of Tracfin's information system, according to strategic guidelines, users' expectations and current regulations.

It is also tasked with designing and introducing a new information system, by 2017, that will aggregate the different types of information sent by the Unit's national and international partners.

Tracfin will require an integrated system for this aggregation process, which must particularly include analysis and processing functionalities that are appropriate to the data's sensitivity and at the same time take into account the legal framework governing the Unit's activities.

The necessary development of Tracfin's information system. Tracfin's information system mainly consists of a professional application and an e-reporting system set up in 2012. More than 95% of STRs, which are the raw data on which Tracfin's employees work, are now received and processed electronically thanks to the Ermes e-reporting system, which also handles some inter-authority information-sharing procedures.


DIRECTOR
Jean-Baptiste CARPENTIER
DEPUTY DIRECTOR
Albert ALLO
Fight against financing of terrorism unit
Strategic analysis unit
LEGAL ADVISOR
Isabelle MINGUET
DEPUTY
Charlotte HEMMERDINGER
IT AND COMPUTING UNIT
Sylvie POUSSINES
INTELLIGENCE DEPARTMENT
Isabelle FENAYROU-DEGAS
INVESTIGATION DEPARTMENT
Alain LEFEBVRE
SUPPORT DEPARTMENT
Josiane DUENAS
Fraud Detection Division
Assessment of Information Division
International Division
Investigation division 1
whose currency exchange and gaming
Investigation division 2
whose tax matters
Investigation division 3
whose cash transfers

THE ROLE OF THE LIAISON OFFICERS

The liaison officer team, which was initially composed of a liaison officer from the Gendarmerie provided by the DGGN and a DGPN liaison officer seconded by the OCRGDF, has gained a new addition with the arrival of a Chief Inspector from the Central Office for the Combating of Corruption and Financial and Tax Offences (OCLCIFF). **Acquiring a new team member has enabled Tracfin to be more proactive and dynamic in the coordination and management of information sharing.**

The Unit is therefore organised so as to provide a single point of entry for judicial information, allow the differentiation of requests, ensure that information is exchanged more smoothly and improve the coordination and monitoring of any action taken.

These liaison officers now centralise, analyse and redirect the information received in order to develop it and share it with the relevant units. They look for links with ongoing criminal investigations or follow up cases referred to the courts through information transmitted by investigative units. They also check the presentation of the judicial requisitions sent to Tracfin by judicial police officers and follow them up.

The interfacing by the liaison officers with their original units has helped increase the flow of information from investigative units in the form of background notes, alerts or awareness-raising about criminal practices or organised criminal groups. These analyses are added to Tracfin's database.

The liaison officers work very closely with the investigative units and parties involved in the combating of money laundering and counter-terrorist financing (central offices, regional task forces, specialised brigades, the financial units of inter-regional or regional judicial police departments and Europol) to assess threats, identify new phenomena and emerging criminal practices and consider the possible joint action to be taken. Tracfin regularly meets with the «judicial» offices of the general directorates of the Police and the Gendarmerie to explore common issues (through inter-institutional strategic meetings, coordination of investigations, risk assessments, etc.).

The information system must also be adapted to cope with the expected volume of the new flow from the introduction of Systematic Information Disclosures (COSI), as a result of which some entities must now provide Tracfin with information about fund transfer transactions involving cash transfers or digital currencies.

In addition, information sharing with other State departments and foreign intelligence units requires flow automation and the inclusion of the flows' content in Tracfin's databases.

The expanding of the legal and judicial division

As a financial intelligence unit dedicated to the combating of money laundering and terrorist financing, Tracfin's primary objective is ensuring that its investigations result in criminal prosecutions. To achieve this aim, Tracfin has created a legal and judicial division overseen by the Unit's legal adviser, who is a judicial magistrate.

The legal adviser and her deputy, who is also a judicial magistrate, and the police and gendarmerie liaison officers, are thus responsible for:

- **Actively interfacing**

with magistrates and judicial police units to prepare, assist with and follow up on the cases transmitted to them, assess the usefulness of the information held by Tracfin for court-led investigations and assist it with the drafting of the requisitions or reports received by the Unit,

- **The Unit's legal activity.**

This division is now specifically in charge of:

- drafting all of the legal documents relating to the Unit's organisation and its operational and institutional activity (legal and regulatory provisions, orders and internal and external notes);
- preparing responses to written questions from members of parliament and questionnaires and surveys sent by national and international public organisations (such as the National Assembly, Senate, European Commission or the OECD);
- keeping track of the negotiations on the 4th AML/CTF directive. This has included the legal division's

participation, as part of the French delegation, in numerous meetings organised in Brussels by the European Commission and the presidency of the EU Council as part of the ongoing negotiations;

- any legal research required for the Unit's activities and the criminal justice training of Tracfin's employees.

■ the training and awareness-raising of participants from the criminal justice system and operational cooperation:

As in previous years, in 2013 Tracfin contributed to several training programmes on financial investigation, money laundering and corruption, directed to French and foreign magistrates, investigators and specialist magistrates from the Court of Auditors:

- given by the National School for Magistrates (ENM) as ongoing training, at the school or through local training sessions at courts of appeal;
- given by police and gendarmerie training schools (Officer Training Schools, the Gendarmerie's National Centre for the Training of the Judicial Police, the Gendarmerie's National Centre for Training in Operational Intelligence) as part of the ongoing training of investigators specialised in economic and financial crime or more specific anti-money laundering programmes;
- given by the Central Unit for the Prevention of Corruption (SCPC).

At the same time, the director, the seconded magistrates and the liaison officers, accompanied by investigators from the Unit, have visited various courts (Lyons Public Prosecutor's Office – Specialised Inter-regional Courts, Ajaccio District Court, Corsican Security Headquarters, Paris Public Prosecutor's Office – division S1 and S2), the Inter-regional Council for Criminal Justice Policy of the French West Indies and central and regional investigative units (Ajaccio Judicial Police, Lyons Inter-regional Directorate of the Judicial Police, Nantes Judicial Police Department, Toulon Judicial Police Department, Val-de-Marne Departmental Judicial Police Department, Seine-Saint-Denis and Seine-et-Marne Regional Task Forces, the Office for the National Coordination of Regional Task Forces, the Central Office for the Combating of Corruption and Financial and Tax Offences, the Central Office for the Combating of Harm to the Environment and Public Health, the Central Office for the Combating of Illicit Employment, the Paris Criminal Investigation Department, the Caen Criminal Investigation Department, the Maritime Gendarmerie's Criminal Investigation Department, the Criminal Affairs Bureau of the National Gendarmerie's Judicial Police Branch and the Headquarters of the Overseas Gendarmerie) to continue and develop operational information sharing with investigators and magistrates. It has been achieved through feedback on proceedings initiated following the referral of STRs to the judicial authorities, the types of cases encountered and the new risks identified.

The Legal Adviser and her deputy also travelled in 2013, after being invited to share the benefit of their experience, to Bulgaria (at the invitation of the MILDT (Inter-ministerial Office for the Combating of Drugs and Addictions) and the liaison magistrate in Belgrade) and Algeria (where they were invited by the Central Office for the Prevention of Corruption).

The strategic analysis unit

Tracfin wished to develop its strategic analysis capacities by creating a dedicated unit in January 2013. According to FATF[1], strategic analysis «uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns.» After this processing the information becomes strategic financial intelligence that «is then used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities».

The strategic analysis unit has two global tasks:

- detecting money-laundering risks and threats through both internal data and external monitoring;
- analysing the risks and threats identified in order to assess their impact on the anti-money laundering system.

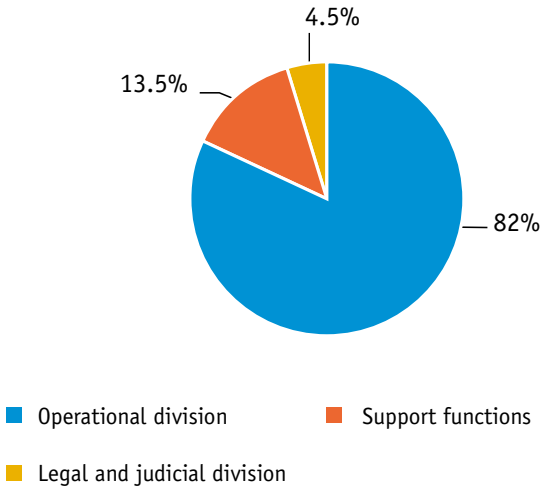
The vulnerabilities arising from the increased use of virtual currencies, an issue that was first raised in Tracfin's 2011 annual report, are a priority focus for the strategic analysis unit.

The strategic analysis unit monitors indicators relating to incoming information flows and the stock of information processed. These indicators help detect weak signals. These signals are then are cross-checked against the signals detected the previous day to identify changes in known risks and emerging vulnerabilities as early as possible. The analysis of the risks and vulnerabilities detected through this process is shared through case typologies and analysis notes containing legislative and regulatory recommendations. The strategic analysis unit also leads and coordinates working groups on cross-cutting themes that require the expertise of various public and private contributors.

STAFF FIGURES

The Unit was staffed by 89 employees at 31 December 2013. This represents a 55% increase in Tracfin's headcount since 2006.

Tracfin's role as an operational department is reflected in the breakdown of its staff numbers by department, with 38% of its employees assigned to the investigation department and 32% to the analysis and intelligence department.



Since 2009, Tracfin has strived to diversify its recruitment pool, hiring from both the economic and financial ministries and the private sector (contractors).

Tracfin's employees mainly originate from departments within the economic and financial ministries. 49% came from the General Directorate of Customs and Excise, 26% from the General Directorate of Public Finances, 17% from the General Secretariat and 5% are private contractors.

79% of the Unit's employees are classed in categories A and A+.

Tracfin continued with its employee training programme in 2013, calling on both institutional partners and internal resources to offer training courses on appropriate themes.

94% of the Unit's employees therefore completed at least one training course in 2013.

1. FATF, 2012: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF recommendations (Interpretive Note to Recommendation 29), February, p. 94

http://www.fatf-gafi.org

GLOSSARY

ACOSS
Central Agency for Social Security Bodies

ACPR
Prudential Supervision and Resolution Authority

AMF
Financial Market Regulatory Authority

AML/CTF
Anti-Money Laundering and Counter-Terrorist Financing

CMF
Monetary and Financial Code

CNAJMJ
National Association of Court-Appointed Receivers and Trustees

COSI
Systematic Information Disclosure

CSN
National Association of Notaries

DGGN
General Directorate of the National Gendarmerie

DGSN
General Directorate of National Security

DGDDI
General Directorate of Customs and Excise

DGFIP
General Directorate of the Public Finances

DGT
General Directorate of the Treasury

DNRED
National Directorate of Customs Intelligence and Investigations

FATF
Financial Action Task Force

FDJ
Public lottery and betting company

FIU
Financial Intelligence Unit

IFFPC
French Institute of Practitioners of Insolvency Proceedings

OCRGDF
Central Office for the Prevention of Serious Financial Crime

SCCJ
Central Racing and Gambling Unit

SDPC
Central Unit for the Prevention of Corruption

SNDJ
National Judicial Customs Unit

STR
Suspicious Transaction Report

Unit for intelligence processing and action against illicit financial networks

Publication Chief Executive: Jean-Baptiste Carpentier

10 rue Auguste Blanqui 93186 MONTREUIL - tél : (33)1 57 53 27 00

www.economie.gouv.fr/tracfin
crf.france@finances.gouv.fr