2015

# MONEY LAUNDERING AND TERRORIST FINANCING RISK

## TRENDS AND ANALYSIS

**TRACFIN** UNIT FOR INTELLIGENCE PROCESSING AND ACTION AGAINST ILLICIT FINANCIAL NETWORKS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

# 2015 MONEY LAUNDERING AND TERRORIST FINANCING RISK TRENDS AND ANALYSIS TRACFIN

**TRACFIN** Unit for intelligence processing and action against illicit financial networks

# CONTENTS

## THREATS, VULNERABILITIES AND CONSEQUENCES: THE THREE CONCEPTS THAT UNDERPIN RISK ASSESSMENT

Recommendation 1 of the international standards on combating money laundering and the financing of terrorism & proliferation laid down by FATF states that "countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified." [...] "

The concepts and methodology for the assessment of money laundering and terrorist financing risks are presented in the FATF Guidance that was published in February 2013. The goal is to identify, analyse, and understand money laundering and terrorist financing risks in order to better prevent them. The results of this assessment are not set in stone, but must be updated on a regular basis.

A risk arises from a combination of three factors: a **threat**, a **vulnerability** and the **potential consequences**.

A potential **threat** is defined as any person, group of people or activity that may harm society or the economic and financial system. Knowledge of the environment in which the offences underlying money laundering are committed is vital for analysing threats.

**A vulnerability** is any element (such as a system, product, transaction or practice) or situation that may be misused for the purposes of money laundering or terrorist financing. Vulnerabilities are inherent to a country's structure and its financial centre. They are linked to the practices, instruments and legal arrangements in a given sector of activity.

Scenarios are devised linking threats to the exploitation of vulnerabilities. The **consequences of these scenarios** are assessed to check that the prevention and mitigation measures taken are effective and proportionate and adapt them if necessary.

At ministerial level, the AML/CTF Advisory Board (COLB) is the national coordination forum that acts as the umbrella for all of the relevant government departments, supervisory authorities and representatives of the reporting entities. The Board carries out a national risk assessment and oversees production and updating of a document summarising the money laundering and terrorist financing threat in France.

# INTRODUCTION

The Unit's annual AML/CFT risk assessment process implements, at department level, the requirement introduced by recommendation 1 of the FATF standards, which specifies that "countries should identify, assess, and understand the money laundering and terrorist financing risks for the country [...]"[1] ". Recommendation 1 also states that "countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks"[2].

The backbone of Tracfin's approach is the money laundering and terrorist financing risk assessment methodology as set out in the FATF's Guidance published in 2013.[3]

Tracfin's risk assessment relies on two main sources: the information that it receives from those individuals and legal entities specifically designated in the Monetary and Financial Code, and the financial intelligence submitted by other departments. Comparing the information received and processed by the Unit against the information gleaned by monitoring open and closed external sources provides additional clarification that further informs the process.

The demand for a national risk assessment is repeated in Article 7 of Directive 2015/849 (the so-called "Fourth Directive") on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Article 8 of that Directive stipulates that Member States must ensure that reporting entities take appropriate steps to assess risks, taking into account, among other things, risk factors such as the nature of clients, geographic criteria, products, services, transactions and distribution channels.

To provide information to guide reporting entities in this process, Tracfin publishes case studies on its website and in its publications, organises awareness-raising initiatives and regularly conducts a risk assessment whose main conclusions are presented in the annual analysis report.

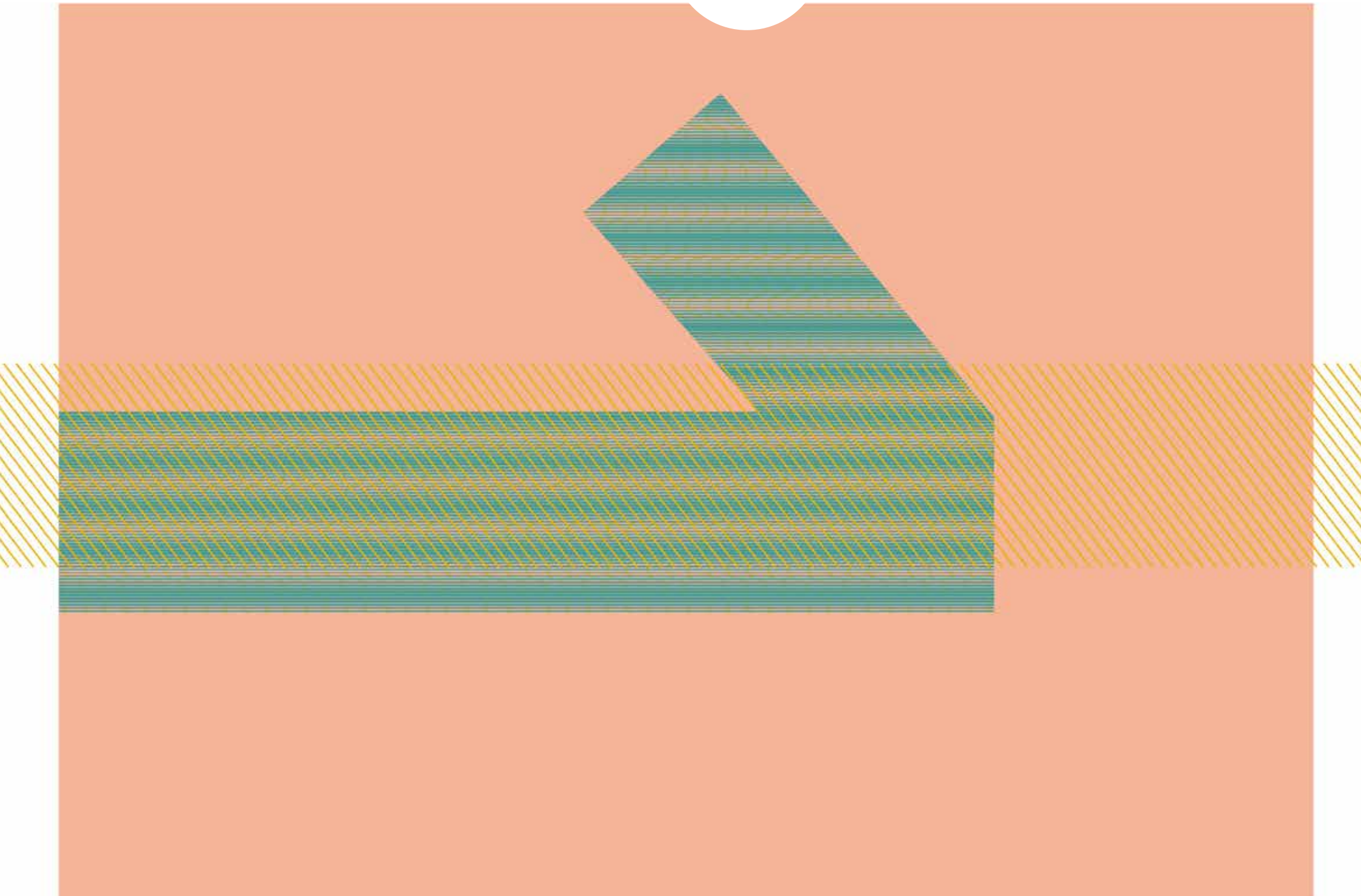




**1** FATF: International standards on combating money laundering and the financing of terrorism & proliferation, The FATF Recommendations, February 2012.

**2** Ibid.

**3** FATF: FATF guidance: National Money Laundering and Terrorist Financing Risk Assessment, February 2013.



# REPORTING FLOWS IN 2015: A SHARP UPSWING IN THE NUMBER OF STRS, BUT QUALITY TO BE IMPROVED

As observed in 2014, there was a sharp upswing in the number of STRs submitted during the year. Tracfin received 45,266 pieces of information in 2015, against 38,419 in 2014, an 18% increase. Of these, 43,231 were STRs submitted by private-sector reporting entities. The others were submitted by Tracfin's partner departments, authorities supervising professionals subject to AML/CTF reporting requirements and foreign financial intelligence units.

Four groups of entities accounted for 93% of STRs submitted. They included banks and credit institutions, the insurance sector (insurance companies, intermediaries and mutual insurance companies), payment institutions and money changers. This percentage was unchanged from the previous year. The increase in the number of submissions was due to greater involvement on the part of reporting entities.

In terms of quality, however, the assessments carried out by reporting entities leave a great deal to be desired. Far too many reports are still incomplete and contain little analysis. Some even lack grounds for suspicion.

The quality of Tracfin's assessment process relies not only on the volume, but also the wide variety and quality of the information received. To be useful, an STR should comprise:

- Clear identification of the individual or legal entity that is the subject of the suspicion and elements proving that the individual or legal entity is known to the reporting entity (Know Your Customer)
- A supporting statement of facts that explains the reporting entity's doubts
- A detailed list of financial transactions listing deposits and withdrawals and the means used
- Any supporting documentation that develops and clarifies the information provided

# UNEQUAL INVOLVEMENT BY REPORTING ENTITIES

A detailed analysis of STRs submitted by reporting entities is available in Tracfin's 2015 Annual Report, available online at www.economie.gouv.fr/tracfin/rapports-annuels.

In terms of quality, STRs submitted by the banking sector are the main source of information received by Tracfin. They primarily deal with medium to small amounts of money and are submitted by retail banking networks. On the other hand,submissions from corporate and private banks and from the trading sector are still lacking. Similarly, asset management professionals (investment companies, financial investment advisers and investment management firms) do not seem to be proactive with respect to amounts of assets under management.

Some entities such as money changers and casinos have made efforts to boost their participation, with 50% and 56% increases, respectively, in STRs submitted in 2015. But these STRs leave much to be desired in terms of both content and quality, given the exposure of these professions to AML/CFT risks.

With respect to STRs submitted by non-financial reporting entities, court-appointed receivers and trustees made significant efforts to boost the number of submissions and improve their quality.

Conversely, a number of non-financial reporting entities submit few or no STRs, although they are at high risk of fraud, money laundering and terrorist financing.

• The property professions have not yet fully adopted the reporting structure, even though real estate is a key weak point in the French system in terms of money laundering, as the FATF's most recent assessment of France makes clear.

• Art dealers appear to be little invested in AML/CFT due diligence procedures, although the sector is at risk of fraud and large-scale money laundering, as can be seen in several high-profile cases involving free trade ports and the use of trusts. The art market is also exposed to terrorist financing risks, due to the looting of antiquities from archaeological sites located in war zones in the Near and Middle East. Appropriate due diligence procedures would be of great utility.

• Despite recent efforts, chartered accountants and auditors are still fairly inactive considering that false invoicing and false agreements for the purchase and sale of goods (or provision of services) play a key role in money laundering schemes.

• Similarly, commercial registered office providers submit few STRs, even though shell companies are ever-present in fraudulent fund-collection and evasion schemes.

• The legal profession is, as a matter of principle, recalcitrant to the French anti-money laundering framework. Professional accounts management of certain law firms within CARPA (Attorneys' Settlement Fund) is outside the scope of the AML/CFT system.

• Sports agents do not submit any STRs. At international level, the sports sector is known for its vulnerability to criminal interests. Transfers of players between football clubs can be a vehicle for large-scale embezzlement and money laundering by criminal organisations.

# SECTORS AT RISK

Outside those reporting entities that play advisory or intermediary roles in financial transactions, Tracfin believes– in light of the STRs received – that certain economic sectors are at heightened risk in terms of money laundering and terrorist financing. There are a variety of reasons why a sector is more exposed to AML/CFT risk.

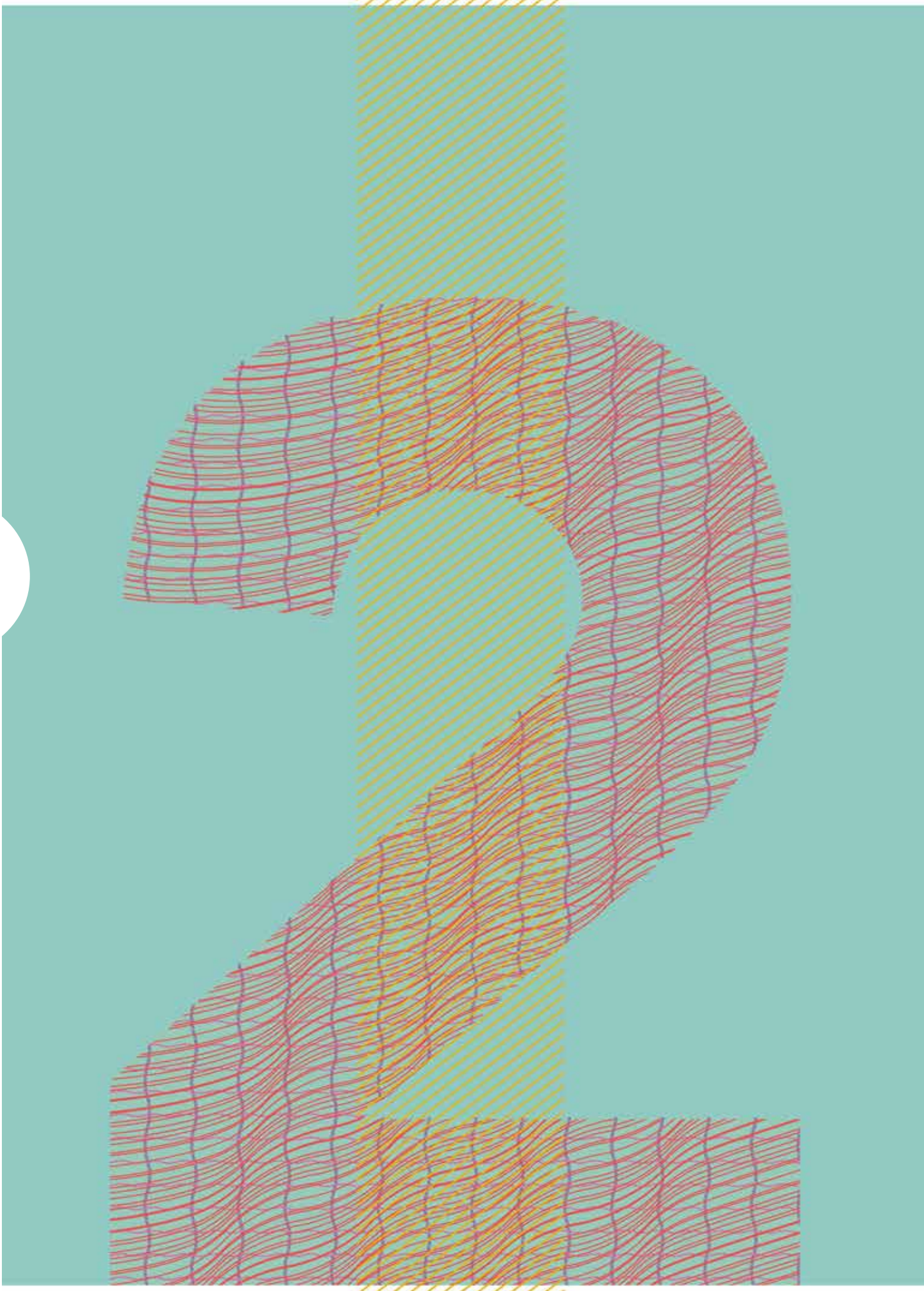
| | AML/CFT risk criteria |
|---|---|
| 1 | Of strategic interest for criminal organisations |
| 2 | Matches the needs and lifestyle of members of criminal networks |
| 3 | Is propitious for political corruption |
| 4 | Allows for undeclared work and/or laundering cash |
| 5 | Susceptible to fraud |
| 6 | Facilitates the non-transparency of valuations of companies and speculation |
| 7 | Useful for terrorist financing purposes |

In addition, every sector is vulnerable to the production of false invoices and false agreements for the purchase of goods and services. False invoicing is a key money laundering tool.

Using these criteria, an analysis of STR submissions shows the following activity sectors to be particularly at risk:

| Economic sectors | Risk criteria | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | Strategic | Lifestyle | Corruption | Undeclared | Escroqueries | Valorisations | Terrorisme |
| Logistics, transport: road, sea and air freight | X | | | | | | |
| Import/export: textiles, apparel or home furnishings, agri-food | X | | | X | | | X |
| Wholesale and retail trade | X | | | X | | | X |
| Luxury car dealerships, purchase and resale of second-hand vehicles, car hire | | X | | | | | X |
| Cafes/bars, hotels, restaurants and nightclubs | | X | | X | | X | |
| Gaming sector: casinos, online gaming, sports and horse-racing betting | X | X | | X | | | |
| Property management and development | X | | X | | | X | |
| Construction sector | X | | X | X | | X | |
| Municipal services: waste treatment, water treatment, heating | | | X | | | | |
| Public social housing management offices and their subcontractors | | | X | | | | |
| Business services: private security, janitorial services | | | | X | | | X |
| Environmental and energy transition: wind power, solar panels, heat pumps, metal recycling | | | | | X | | |
| Sales of computer equipment, mobile telephony, prepaid telephone cards, and mobile-based services | X | | | X | X | X | X |
| Pharmaceuticals, medical equipment and paramedical services (in connection with mutual insurance companies and social security funds) | | | X | | X | | |
| Vocational training and access to employment | | | X | | X | | |
| Communication: media, events management | | | X | | | X | |
| Purchasing departments for advertising space | | | X | | | X | |
| Audiovisual production and rights negotiations, live performance production | | X | | X | | X | |
| Sports economy: sports clubs, agents, sporting rights negotiators | | X | X | | | X | |
| Art market | X | | | | X | X | X |
| Commodity traders | X | | X | | | X | X |
| Arms | X | | X | | | | X |

This list has been drawn up based on information analysed by Tracfin. It is only illustrative and is in no way exhaustive. The nature of fraud is such that it can be found in most types of activities.



# FINANCIAL CRIME – FIVE TYPES OF THREATS

The FATF defines a threat as “a person or group of people [...] with the potential to cause harm to, for example, the state, society, the economy, etc.” Threats must be embodied, and they must be analysed with an eye to concrete objectives. They should not be confused with a list of criminal offences.

Based on STRs submitted by reporting entities, Tracfin has identified five major types of threat to the French economy: the terrorist threat and its financing (such as witnessed in 2015), criminal threats, corruption, tax evasion and social fraud, and frauds without links to criminal networks.

Detailed threat identification is the work of an interministerial national risk assessment process carried out by the AML/CTF Advisory Board (COLB). For criminal threats, the police and the court system are involved, in particular the Information, Intelligence and Strategic Analysis of Organised Criminality Department (SIRASCO), with which Tracfin is in regular contact.

# TERRORISM FINANCING

2015 was a landmark year for Tracfin due to the changing scope of the terrorist threat in the wake of the attacks in January and November 2015 in Paris, and the top priority assigned to the fight against terrorism and terrorist financing. As a result, Tracfin was given additional resources and the Unit was further integrated into the French intelligence community.

## THREAT CHARACTERISATION

The three main goals of financial intelligence regarding the fight against terrorist financing are :

- To detect criteria indicative of radicalisation
- To provide an exhaustive financial picture of the individuals or organisations in question
- To establish clear links between individuals

Financial intelligence gathering also allows Tracfin to focus on radicalised individuals leaving for war zones, the collection of funds to provide support for fighters, financing for proselytising and embezzlement of humanitarian aid.

In this area, financial intelligence runs up against issues such as micro-financing and weak signals. Analysis is not focused on large sums but on transactions details. It is mostly dealing with young populations with few financial resources. Travelling to a war zone or conducting a terrorist action on the French territory requires modest financing. Moreover, the flows examined involve:

- Laundered money, when actions are financed by predicate offences such as fraud, fraudulent papers when applying for consumer loans and sales of counterfeit goods.
- "Money blackening ?", when money of legal origin, such as wages or social benefits, are used to terrorist ends.

### Financing Foreign Terrorist Fighters (FTF)

Tracfin analyses and processes every transaction that could signal a departure to a conflict zone or a return to France. Thus, every element having to do with bank accounts and payment accounts, associated instruments and data gathered during transactions could be of interest as part of efforts to detect individuals preparing to depart or to return.

Case study no. 1

**Detecting an imminent departure for a combat zone**

Tracfin's attention was drawn to an individual in his twenties whose financial resources consisted of wages paid by a temping agency, benefits paid by Pôle Emploi (France's public employment service agency) and the CAF (Family Allowances Fund). The individual closed his bank accounts and transferred the money to an account opened in a new bank. He subsequently withdrew a large amount in cash. An examination of the young man's most recent account showed transactions such as the purchase of airline tickets and payments made only in a war zone in the Middle East.

**Warning signs**

- Single withdrawal of a large amount in cash, for no specific reason
- Sudden closing of French bank accounts, or a sudden lack of activity
- Purchase of airline tickets and/or visas for a sensitive zone
- Type and location of purchases made with a bank card
- Profile of the individual (young, radicalised)

Case study no. 2

### Detecting a potential foreign terrorist combatant

A reporting entity alerted the Unit to statements made by an individual. The person, who worked in a plant using dangerous substances and classified as such, had stated his intention to leave France for North Africa, and was changing his physical appearance (clothes and hair). His bank account showed regular wire transfers to a religious association, frequent travel (train, tolls and hotels) and a high number of withdrawals.

**Warning signs**

- Change in physical appearance
- Unclear plans to move to a geographically sensitive zone
- Regular financial flows to a religious association
- Expenses suggesting a great deal of travelling inconsistent with an individual's income

## Self-financing of radicalised individuals on French territory

Tracfin also analyses the bank accounts of individuals known for radicalisation willing to plan an attack on French soil. Financing for small terrorist cells operating in France involves small amounts when compared to transnational organisations operating abroad. Special attention must be paid to the means used by these groups to finance themselves, including consumer loans, the use of prepaid cards and the proceeds of illegal activities (drug dealing, theft, sale of counterfeit goods, etc.).

The attacks on the weekly magazine Charlie Hebdo and the kosher supermarket were financed by consumer loans, the sale of a second-hand car and transfers of cash earned from selling counterfeits. With respect to consumer loans, the warning signs are as follows:

- Withdrawal of the loan amount in cash
- Use of the money for other purposes than those indicated when signing up for the loan
- Large numbers of small loans from various establishments

Case study no. 3

### Detection of bank transfers to radicalised individuals

The Unit was alerted to the behaviour of a bank customer, who asked for a bank transfer despite having insufficient funds. He then paid the missing amount in cash.

When making the transfer, he gave the name of the beneficiary and stated that it was for religious reasons. The following day, he changed his mind and tried to cancel the transfer, and appeared worried that there would be a trace of it in his bank statements. After checking, the reporting entity noted that the name of the owner of the recipient account was not the name given by the customer. A public records search revealed a link with radicalised movements.

**Warning signs**

- Contradictory behaviour by a customer
- The name of the account holder is not the stated beneficiary of the transfer
- Links with radicalised movements

Case study no. 4

### The use of prepaid cards to finance a project

TTracfin was given information about payments being credited to two prepaid cards in an EU Member State. The cards, which belonged to two different users, were credited from one single payment account opened in France. Cooperative efforts between Tracfin and the Member State's FIU pinpointed payments made with the prepaid cards, and brought to light a terrorist plot.

Tracfin also receives STRs from online payment service providers that help identify suspicious behaviour. Thus, the Unit was alerted to cases of individuals using their online payment accounts to purchase items that could signal the preparation of a terrorist action on French soil[1].

1 These include goods such as masks, large coats and portable electrical splitter cables that could be used to make explosive devices.

## Money collectors

Tracfin investigates atypical transactions of cash transfers that originate within France. The funds are gathered by individuals acting as money collectors, who are generally located in relay countries or countries that border conflict zones.

## Financing non-profit organisation with radical aims

Tracfin is regularly alerted about humanitarian or cultural NGOs that are suspected of providing financing for terrorist networks. On paper, most of them provide logistical support for populations in conflict zones.

These organisations have several features in common:

- They were created after 2011, the year of the Arab Spring and the start of the civil war in Syria. Since then, they have expanded their scope of activity to other areas in the Middle East, the Maghreb and sub-Saharan Africa.
- They are involved in various efforts, including providing medicine, humanitarian aid (tents, blankets, etc.), non-perishable food items and even live animals (sheep) used in religious festivals.
- They use Internet and social media as platforms for innovative and effective marketing efforts, and to collect money. Contributors use mainly prepaid cards and PayPal accounts.
- Although French and European residents contribute small unitary amounts, taken together they provide these NGOs with millions of euros of capital.
- These organisations' treasury management practices are inconsistent with their stated humanitarian aims. They maintain large bank balances and take their time using the money to meet the needs of dispossessed populations.
- Some, that are well-established in the humanitarian sector, receive public financing.
- Their financial workings are less than transparent. Claiming that war zones do not have reliable banking systems, the heads of these organisations make cash withdrawals totalling tens and even hundreds of thousands of euros. Declarations of cash at a country's borders are not carried out systematically, and it is difficult to check how the funds are used in war zones.
- They provide mutual financial support via mutual bank transfers, sometimes between NGOs with widely varying aims. Such financial support allows highly radicalised associations to indirectly control other, more moderate organisations.

Whether it is a question of networks of money collectors or the misuse of humanitarian organisations, collection of funds is now increasingly done through crowdfunding platforms and money collection sites (see Part 4, "New risks triggered by the technological revolution in financial services").

## Financing for ISIL

Tracfin contributes to international discussions on the financing of terrorist organisation Islamic State in Iraq and the Levant, as described in studies by the FATF[2] and several specialist publications. This financing comes from several sources:

- Looting local banks
- Extorting money from local populations and diversion of religious alms, which are often demanded in kind
- Smuggling oil, mostly from wells in the Deir Ez-Zor region, and taxation of sales of petroleum products to local populations and to intermediaries
- Exploitation and resale of agricultural commodities such as cotton
- Smuggling antiquities
- Private donations, often from wealthy individuals from countries in the Persian Gulf.

In 2015, the Unit took part in a large number of international multilateral and bilateral meetings in order to present its efforts to combat terrorist financing and to exchange with Tracfin's foreign counterparts. These included the FATF, the Egmont Group, and the EU/US Summit organised by the European External Action Service

**2** FATF: Financing of the Terrorist Organization Islamic State in Iraq and the Levant, February 2015.

The FATF's Emerging Terrorist Financing Risks report, which was published in October 2015, was co-written by France and the US, with contributions by some thirty of the FATF's delegations.[3]

# ENHANCED RESOURCES TO COMBAT THE TERRORIST THREAT

## Operational actions

In June 2015, Tracfin helped set up a unit to coordinate the work of special services, which helps ensure that information can pass quickly and easily between departments.

Leveraging its closer ties with intelligence services, Tracfin provides them with prompt intelligence reports that have been combined with and enhanced by its own investigations. In-depth financial analyses are then carried out. At the time of the terrorist attacks of 13 November 2015, Tracfin fielded a team in real time, and in 48 hours completed a financial portrait of the known terrorists and a search for any and all useful financial information. These efforts were carried out in close cooperation with the Unit's foreign counterparts.

Tracfin's responsiveness and ability to quickly generate intelligence reports for specialised criminal investigation departments in accordance with an accelerated procedure demonstrates the need to have an experienced Financial Intelligence Unit (FIU) to process financial information.

This new involvement was absolutely one of the defining moments in 2015.

Tracfin is constantly strengthening its ties with foreign FIUs, particularly Belgium, Luxembourg, Switzerland and the US.

After the January 2015 attacks, Tracfin was provided with 10 additional members of staff: 6 in 2015 and 4 in 2016. This operational support led to the creation of a special CFT division on 1 October 2015. A total of 534 CFT cases were processed in 2015 (119% more than in 2014), not including cases involving multiple suspicions: 179 information notes concerning terrorist financing (a 130% increase over 2014) were referred to the Unit's special services partners or to the courts.

## Normative and legislative measures

Tracfin's operational commitment went hand-in-hand with an assessment of the Unit's arrangements for gathering and analysing intelligence. It appears that some "low intensity" information can be critical (such as the reactivation, closing or opening of a bank account, or new contact details), which requires a system that is more proactively able to search for relevant intelligence. For this reason, a proposal was put forward to define a new legal framework that would allow Tracfin to seek specific due diligence measures concerning individuals or legal entities that are considered to be high risks in terms of terrorism or money laundering.

On 18 March 2015, the Minister for Finance and the Public Accounts issued an action plan for combating terrorist financing. Its key measures include:

- Eliminating anonymity in the prepaid card and money changing sectors
- Lowering the ceiling for cash settlements of transactions from €3,000 to €1,000 for individuals or legal entities resident in France, and from €15,000 to €10,000 for non-residents[4]
- Reporting entities systematically informing Tracfin of all cash deposits and withdrawals totalling more than €10,000 in a month
- Increased inter-departmental cooperation and international coordination

This action plan was supplemented on 23 November 2015 and was enshrined in several legislative acts.

Act 2015-912 of 24 July 2015 concerning intelligence measures expanded Tracfin's powers with respect to information requests to include transport companies and travel agencies.

**3** FATF: Emerging Terrorist Financing Risks, October 2015.

**4** This lower ceiling for cash payments took effect on 1 September 2015.

Act 2016-731 strengthening the fight against organised crime and terrorism and their financing, and improving both the effectiveness and guarantees of criminal proceedings (the "Urvoas Act") includes several CFT provisions:

- Heightened vigilance: Tracfin may alert reporting entities to individuals or transactions that are high AML/CFT risks. This will allow these entities to adapt their due diligence measures. This provision will be applicable when an implementing decree is issued following consultation of the Conseil d'Etat.
- Extending Tracfin's powers with respect to information requests to payment and withdrawal card systems managers.
- Obligation to preserve new data: electronic money issuers must gather and maintain information about the activation, loading and use of prepaid cards for five years.
- Capping the amounts that can be loaded on prepaid cards as well as the individual amounts loaded, reimbursements and cash or anonymous electronic money withdrawals in order to have better oversight over how these payment instruments are used. The caps will be set by a decree.
- Direct access for Tracfin to certain administrative files, especially to prior criminal records (TAJ), in an effort to bring departments into closer cooperation.

# CRIMINAL THREATS

Based on information submitted to Tracfin and its investigations, the Unit has identified four key threats to the French economy in terms of financial crime:

- Criminal business networks specialising in large-scale financial fraud
- Fraudulent networks in Asian communities
- Laundering the proceeds of drug trafficking
- Long-standing organised crime

## CRIMINAL BUSINESS NETWORKS SPECIALISING IN LARGE-SCALE FINANCIAL FRAUD

These networks often have a clannish aspect, in connection with countries in the Mediterranean basin or Southern Asia. They specialise in tax evasion and social security fraud, including carousel fraud, debt collection fraud at the expense of banks, and laundering the proceeds of these offences.

Carbon carousel frauds carried out between the end of 2008 and June 2009 put these criminal networks on a whole new level. France's Treasury was defrauded out of an estimated €1.6 billion by carbon carousel frauds alone, and the figure is more than €5–6 billion for all of the EU. Several violent deaths are thought to be tied to these crimes. Other carousel frauds involving various types of goods continue within the EU.

Some gangs have been thriving over the past five years on SEPA transfer order frauds, as well as on unregulated binary option websites, most often FOREX-related.

### Transfer order fraud

SEPA transfer order fraud first appeared in 2010. It hit a peak in 2013–2014, but still continues at high levels. Between 2011 and 2015, the specialised criminal investigation departments have registered more than 1,550 companies who have fallen victim to this type of fraud, some of them more than once. By the end of 2015, total damages were estimated at €500 million, and attempted frauds totalled more than €860 million.

This type of fraud was initially carried out over the telephone. Through meticulous research using public records, the fraudsters would obtain as much information as possible about how their victim companies were organised and run. They would then call one of the company's financial or accounting executives pretending to be the president or CEO, and claiming that an urgent and confidential event (such as an acquisition or a looming tax audit) necessitated a sizeable bank transfer to a foreign bank account.

To avoid being traced and to remain anonymous, the fraudsters used prepaid phone cards and web-based VoIP calling, which would display a local telephone number on the handset of the recipient of the call.

The criminals refined their techniques by hacking into companies' servers to obtain sensitive information about their victims, including detailed organisational charts, accounting documents, and the names and bank account details of suppliers.

Hacking allowed criminals to alter their modus operandi – they would send letters on suppliers' letterheads, informing companies that the accounting department was being reorganised and that the suppliers' bank account details had changed, and requesting that payment for all future invoices be sent to the new account. Of course, the new account would be one opened by the fraudsters. Another technique involves sending victims a web link connected to spyware, and asking them to connect to their online banking website. The spyware records

the companies' logins and passwords and allows criminals to make bank transfers to themselves.

The stolen funds are then wired to transit accounts opened by missing traders throughout Europe, Eastern Europe in particular. The money is then transferred to China or Hong Kong, where it can be laundered and then invested in various ways, such as real estate investments in the Mediterranean basin.

In 2015, Tracfin was alerted to about a hundred cases of this type of fraud. Working closely with criminal investigation departments, the Unit is often able to freeze or recover money from foreign banks thanks to the speed and quality of the international cooperation between FIUs. To be able to freeze funds, Tracfin reminds victims of the need to file a complaint immediately. Banks should submit a Suspicious Transaction Report as fast as possible.

It should be pointed out that smaller companies are now being targeted, and even government-funded institutions, particularly in the healthcare sector.

## Unregulated binary trading options fraud

According to the specialised criminal investigation departments, by the end of 2015, unregulated binary option trading websites, primarily FOREX-related, had defrauded several thousand victims in France of more than €200 million. Annual proceeds on a global scale total more than a billion dollars.

Criminals purchase or set up web-based stock trading sites. Customers log into an online trading platform. They put up a sum of money on the prediction that the price of an asset (usually a currency) will rise or, conversely, fall on the international markets within a very short period of time (a few minutes). If a customer correctly predicts the outcome, s/he earns a certain percentage in profit and the company loses money. If s/he is wrong, s/he loses all the money invested in the transaction, which the company keeps. In contrast to other types of options contracts, binary options are high risk investments due to their "all or nothing" nature. No financial expert can predict how the price of an asset will change in such a short period of time. Instead of an investment, binary option trading is nothing more than betting.

Fraudsters set up call centres whose staff are trained to aggressively canvas individuals. New customers' initial investments are generally positive, giving them confidence. Then come the losses. The call centre operators then try to convince customers to continue to invest to recoup their losses and get back in the black. As it turns out, the value of customers' portfolios never improve.

Customers are never informed about the particularly high risks of the financial products they are being offered. In addition, on many sites the game is rigged. Potential payouts on correct predictions are calculated to keep the company's losses to a minimum. If an asset behaves too predictably, it will be delisted from the online platform. In some binary option trading companies, the platform is tampered with to supply false results, ensuring that customers always lose.

Companies also make it extremely difficult for customers to withdraw their money. In practice, it is impossible. To avoid paying, they send multiple requests for documents or additional supporting documentation. Finally, they refuse to take customers' calls and close their accounts, without them ever being able to get their money back.

There are hundreds of companies like these. Many are unregulated. Some are registered in EU jurisdictions where regulations are particularly weak, but which gives them the right to sell their products throughout the EU, under the freedom to provide services. Except a few regulated types of trades, binary option trading has been banned in the US since 2013.

## Reaction of the French authorities

On 31 March 2016, the Autorité des Marchés Financiers (financial markets regulator – AMF), the Autorité de Contrôle Prudentiel et de Résolution (Prudential Supervision and Resolution Authority – ACPR), the General Directorate of Competition, Consumption and the Prevention of Fraud (DGCCRF), and the Paris Tribunal de Grande Instance (Court of First Instance) held a joint press conference to

inform the general public about this threat[5]. It was reported that:

- The number of unauthorised sites appearing on black lists published by the ACRP and AMF went from 4 sites in 2010 to 380 sites at the end of March 2016
- The number of claims filed with the AMF rose from 64 in 2010 to 1,656 in 2015
- Fraudulent trading sites accounted for 41% of the 14,500 calls logged by the Assurance Banque Epargne hotline (a call centre jointly set up by the ACPR, the Banque de France and the AMF)
- The DGCCRF handled 75 complaints in 2015
- 44% of new Internet ads for financial investment in 2015 had to do with highly-speculative trading

According to the AMF, over four years' time, customers' losses totalled €175 million, compared with €13 million in gains. 90% of customers of authorised platforms lose money. On unauthorised platforms, the figure is 100%.

Tracfin regularly handles cases concerning such fraudulent sites, for amounts that, in 2015, varied from €200,000 to more than €3 million.

This infringement, which was initially considered to be stock exchange fraud, is now classified by the criminal investigation departments as a large-scale fraud that requires concerted coordination at international level.

The Transparency, Anti-Corruption and Economic Modernisation Act, known as the Sapin II Act, includes a provision to ban advertising for the highest-risk financial products.

According to the Paris Court of First Instance, estimated losses due to false transfer orders and binary option trading website scams totalled €4.5 billion over six years.

## FRAUDULENT NETWORKS IN ASIAN COMMUNITIES

Fraudulent networks in Asian communities combine legal activities (in such sectors as import/export, textiles and agri-food), tax evasion and social security fraud (customs fraud, concealment of revenue, carousel fraud, undeclared work, social security fraud), and illegal activities (counterfeiting, illegal immigration, prostitution, money laundering and illegal practice as an intermediary in banking and payment services).

They are significantly implanted in freight and merchandise zones where wholesalers and import/export companies dealing in Asian products congregate. A significant portion of imported goods, whether counterfeit or not, are not declared to customs. This share is estimated at between 20 and 40%. These goods are sold off the books, with no VAT or social security contributions, and thus generate large amounts of cash.

Various criminal investigation departments have estimated that, in several European freight zones, customs and tax frauds generate more than a million euros a day per zone, accounting for several billion euros in annual flows from Europe to Asia.

The cash sent to Asia is reinjected into the real economy for several purposes:

- Payment of suppliers
- Investment in new means of production or new textile collections
- Commercial and residential property
- Repayment of dark loans[6]

To this end, the funds are routed via circuits outside the banking system that are directly installed within the commercial sphere. A system of collectors and secret banks facilitates the collection and transmission of the money to Asia. Money is sent in several ways:

**5** A joint press release by the AMF, ACPR, DGCCRF and the Paris Public Prosecutor's Office was issued on 31 March 2016

**6** The Asian communities involved in these networks make use of parallel sources of financing (the so-called "tontine" system), thus bypassing the regular banking system. These take various forms and are often family- or community-based, but also allow loan-shark activities by criminal organisations to take root.

- Amounts are broken up and sent via wire transfer companies
- Mules carrying money on airline flights
- Bank transfers through relay countries

Larger volumes of cash means more transfers and increasing use of mules. Wire and bank transfers can be broken up by the use of a large number of front men.

More than one method is used sometimes: cash, which represents shopkeepers' undeclared income, is collected in person in Western European countries and brought to Eastern Europe by road, where it is deposited in local branches of Asian banks, which then wire the money to Asia.

Undeclared cash generated in Europe is centralised by intermediaries acting as shadow bankers entrusted with transferring this money to Asia. The role of shadow banker can be played by international money transfer agencies, or by informal agreements between shopkeepers who pool and self-fund their transfers, or by individuals who specialise in illegally practising as an intermediary in banking services. Shadow banking can be family-based, or it can be a large and highly structured operation. It always has a transnational aspect.

Tracfin receives a large amount of information concerning the circuits described above:

- In terms of individuals, the information primarily concerns serial cash transfers to multiple beneficiaries in Asia, significant cash deposits and a large number of cheques being deposited into individuals' accounts. It also addresses the purchase of standard properties with sizeable down payments by individuals who declare little or no income. Self-financing can come from cash or cheques from other individuals, according to a "tontine" scheme. Some individuals make several purchases in a short period of time, leading to mortgage payments that exceed their declared monthly income.
- When it comes to legal entities, Tracfin has observed repeated cash deposits into the bank accounts of wholesalers, round-number bank transfers to Asian suppliers, invoices presented as vouchers that do not match account transactions, the lack of operating expenditure and non-existent tax and social security contributions, particularly VAT payments.

Tracfin's investigations into these circuits requires assembling and cross-checking data that often arrives at the Unit piecemeal. Only after Tracfin has completed in-depth analyses of the STRs submitted by various reporting entities and conducted investigations can these mechanisms be attributed to organised networks.

## DRUG TRAFFICKING NETWORKS

Despite the increasing diversity in criminal gang's activities, drug trafficking remains the cornerstone of the criminal economy. According to France's specialised criminal investigation departments, the illegal drug market in France is thriving, with ever more dangerous products for sale. Although the number of violations of narcotics legislation remained unchanged in 2015, the quantities of drugs seized rose sharply. Several large-scale seizures of cannabis pushed the total to 77.6 tons, a 65% increase over the previous year. Seizures of cocaine increased by 58% to 10.9 tons. These included two seizures at sea of more than two tons each. Heroin and synthetic drug seizures were also higher.

The volumes of cash generated by drug smuggling networks makes money laundering indispensable. At European level, the annual earnings generated by sales of illegal drugs is estimated to be €24 billion; cannabis accounts for 38% of this[7]. In France, this market is estimated to be between €2 and €4 billion, 50% of which is derived from cannabis. The value of seizures of criminal assets connected to drug trafficking was up 14.3% in 2015: €55.3 million was seized, compared with €48.4 million in 2014.

The money laundering techniques used vary widely depending on the type of network: its size, how international it is and its position in the logistical and commercial chain.

**7** European Monitoring Centre for Drugs and Drug Addiction – Europol: EU Drug Markets Report, 2016.

- With respect to wholesalers and heads of networks, the cash to be laundered can reach into the hundreds of millions of euros per year, and requires sophisticated international circuits.
- When it comes to street sales, some of the profits of the cannabis trade are not really laundered, but directly injected into the legal economy in the form of consumption by the families that derive their living from it. For the rest, there are a number of vectors for laundering money, most of them simple. They include purchases of winning lottery tickets, sports betting, purchases of small businesses, especially in the fast-food sector, acquisition of residential real estate, and companies that buy and resell or hire vehicles.

Given the amounts of cash generated by drug trafficking each year, there are still too few drug-money-related STRs submitted to Tracfin. Often they concern large-scale flows of cash – wire transfers, gaming transactions or cash purchases of real estate. The appearance, in a Suspicious Transaction Report, of countries known for being drug manufacturing or transit zones should not be the only element leading to the suspicion, but could add credence to it.

Nevertheless, transactions submitted to the Unit cannot always be assumed to be linked to drug trafficking. There are so many incidents of drug trafficking and such a variety of methods to launder the proceeds of that trafficking that links between the money and the drugs cannot always be established. Tracfin's assessment of some of these methods is detailed in Part Three of this report. Linking them with certainty to narcotics trafficking requires the resources of the special investigation departments, which intervene after Tracfin.

## LONG-STANDING ORGANISED CRIME

Organised crime networks, which are primarily located in southeast France, although their reach is nationwide, remain a significant threat when it comes to money laundering. Gang members are engaged in a variety of illegal activities, including drug trafficking, racketeering, freight theft, conspiracy to defraud, embezzlement by means of corruption in public procurement or misuse of public subsidies, misuse of company assets and embezzlement within the sports economy.

The threat is all the greater in that some of these gangs have, due to their long-standing presence, managed to make inroads into the legal and institutional realms, which makes it possible to operate under the radar. Others have been destabilised due to turf wars and the persistent efforts of law enforcement.

Tracfin has in-depth knowledge of some of these gangs, with help from high-quality STRs. Most STRs concern property development projects and the purchase of high-end real estate, as well as cases of misuse of company assets and breach of trust, tax evasion, and handling large amounts of cash. STRs about organised crime in southeast France are processed with care, allowing Tracfin to actively cooperate with specialised police departments and other government departments involved at local level.

Nevertheless, the information that Tracfin receives comes primarily from credit institutions and partner administrations. There are still too few submissions from certain categories of reporting entities that are exposed to risk, such as notaries in sensitive geographic zones. Moreover, STRs, that are mostly focused on property issues, do not sufficiently factor in risks of embezzlement during the public procurement process, particularly in the construction sector.

It should be noted that Tracfin is legally obliged to completely protect its sources, and this obligation covers any referral of information to the courts. Sending STRs via Ermes[8], the secure online platform that issues paperless receipts, also helps reporting entities keep a low profile.

**8** Ermes is an online submission platform. It allows reporting entities to submit STRs to Tracfin in a completely secure fashion.

# CORRUPTION

Over the past several years, Tracfin has handled some fifty corruption cases per year, divided between judicial referrals and referrals to other partner departments. A look at the financial elements available to Tracfin shows that these cases have to do with offences of public and private corruption, unlawful obtaining of an advantage and influence peddling. The individual cases handled in 2015 involved amounts ranging from a few tens of thousands of euros to more than ten million euros. There are three categories of cases:

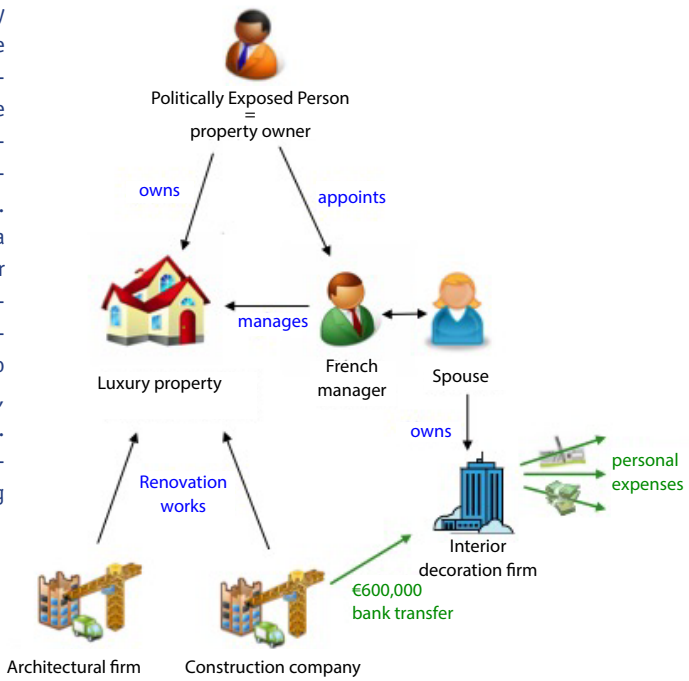
- **Corruption of French politicians** in the performance of their duties or related activities, such as acting as an intermediary in negotiating trade agreements abroad
- **Corruption of foreign public officials** by French economic stakeholders active in key international markets (energy, arms, infrastructure and equipment, pharmaceuticals, agri-food, etc.) These cases sometimes involve sensitive countries in terms of the risk of terrorism.
- **Corruption of foreign Politically Exposed Persons (PEPs)** who come to France to launder the proceeds of their corruption. These transactions involve either the purchase of property in France or deposits into bank accounts opened in their name or in the name of family members, or the use of front men. Deposits are made (i) directly in cash, (ii) by bank transfers from foreign bank accounts in which cash has been deposited, or (iii) by transfers from shell companies, which are either offshore (in sophisticated money-laundering cases) or part of the legal economy.



## Case study no. 6

### Corruption of a French intermediary

In 2015, Tracfin handled the case of a French intermediary who was tasked with managing a luxury property in the Paris region owned by a wealthy foreigner. The intermediary undertook large-scale renovation works, which were entrusted to an architectural firm and a construction company. In return for being given the commissions, both undertakings agreed to provide kickbacks to the intermediary. This was done by purchasing non-existent services from a third company, which specialised in interior and exterior decoration and which belonged to the French intermediary's spouse. The architect and the construction company issued payments totalling several hundred thousand euros to the decoration firm, which had little in the way of capital, no employees and only these two companies for clients. The money was used for personal expenses, including vehicle purchases and the upkeep of private residences, leading to the suspicion of corruption by a private individual.



# TAX EVASION AND SOCIAL SECURITY FRAUD

Following decree no. 2009-874 of 16 July 2009, tax evasion is an integral part of the AML/CFT system. The decree introduces 16 criteria for establishing cases of tax evasion, including the use of shell companies and individuals acting as intermediaries. If even one criterion is met, a Suspicious Transaction Report should be submitted.

Tracfin is tireless in its efforts to counter fraud involving the public purse, and works closely with the DGFiP and the social security funds. As a result, the number of STRs has steadily increased: 410 STRs were referred to the DGFiP in 2015 (+12% over 2014) and 109 were referred to the social security funds (+31% over 2014).

By nature, the data that the Unit receives does not allow it to carry out an exhaustive assessment of the tax evasion and social security fraud risks. STRs are submitted by legally-defined sources and are based on a suspicion, which is not a reliable indicator that fraud is present. On the other hand, statistical analysis of the information received by Tracfin shows that the percentage of tax evasion-related STRs increased by 24% between 2014 and 2015.

The files received and processed by Tracfin have to do with all types of tax evasion and social security fraud:

- **Social security contribution fraud** perpetrated by employers (undeclared work) and benefits fraud by beneficiaries (undue claiming of social benefits), as well as fraud involving the wage guarantee scheme (AGS).

In 2015, Tracfin and the Central Agency for Social Security Bodies (ACOSS)[9] signed an agreement that entered into force on 4 January 2016, boosting cooperation between both bodies in the area of combating illegal labour. The agreement provides for the secondment to Tracfin of a collection officer from URSSAF IDF.

The number of STRs that Tracfin refers to ACOSS increased 123% in 2015, and involved a total of €69.8 million.

- **Fraud by commercial firms**, whether it involves VAT, corporation tax or capital gains tax, or cases of embezzlement of assets during insolvency proceedings to the detriment of public creditors.

Tracfin is a member of the VAT Task Force, an interministerial operational unit tasked with early detection of VAT fraud. Task force members include tax and customs officials, and delegates from the Interior and Justice ministries. Tracfin presents cases that it has investigated in depth, and highlights resources that it has in terms of international cooperation.

The so-called "Blue Economy Act", which was adopted by parliament on 7 June 2016, calls for the introduction of the VAT[10] reverse charge procedure at France's ports. This is expected to bolster the ports' competitiveness in the face of competition from its European counterparts, particularly the port of Antwerp, which already have the procedure in place. On the other hand, this makes it easier to commit carousel fraud. Being able to defer VAT payments paves the way for shell companies and organised fraud. It will be important to ensure that import companies that use the reverse charge procedure are identified and well known.

Tracfin reminds reporting entities that it is important to consider cases of tax evasion in legal entities, which can involve significant sums of money, and to which all professionals should pay particular attention.

- **Tax evasion by individuals**, particularly those with high net worth, who have undeclared bank accounts abroad and who attempt to avoid paying wealth tax, death duties or capital gains tax, or who attempt to fraudulently organise bankruptcy.

**9** ACOSS provides joint, centralised management of the resources and funds of France's general social security regime.

**10** Up to the present, when importers have brought goods into France, they have had to pay VAT, for which they were reimbursed later. This applied even when they re-exported their own merchandise. Now, the new act simplifies the process by allowing importers to not pay VAT.

Financial assets held abroad by French tax residents is a recurring theme in the STRs submitted to Tracfin. A certain amount of STRs are a result of the tax compliance procedures rolled out by the DGFiP under the circular of 21 June 2013. In 2015, Tracfin sent 106 requests for information to the DGFiP's Offshore Disclosure Unit (STDR). These requests are to confirm or rule out whether an individual has submitted an application for filing an amended return. They represented nearly €107 million. After being analysed, cases where applications have not been submitted are the subject of a notification sent to the DGFiP after a precise determination of the assets in question. It must be pointed out that Tracfin also contributes to detecting amended returns that seem to be incomplete.

When it comes to tax fraud, reporting entities need to remain alert at every step in the process, whether the issue is tax avoidance, attempts to bring undeclared assets back to France from abroad, or reinvestment of funds derived from fraudulent activities and laundered overseas.

# FRAUD NOT LINKED TO CRIMINAL NETWORKS

Over and beyond organised criminal gangs, corruption and tax evasion and social security fraud, the threat of money laundering is also rooted in a number of fraudulent operations undertaken by individuals. Two types of fraud in particular stand out:

- Ponzi schemes (or pyramid schemes) that promise high-yield (but fictitious) investments, and deceptive marketing practices
- Misuse of legal and tax structures, particularly tax breaks in France's Overseas Communities, as well as subsidies for training and getting people into the work force.

Each year, Tracfin devotes considerable resources to cases like these, as can be seen in the following examples.



Case study no. 7

### Misappropriation by an investment company

An Internet-based investment company offered tax-exempt investment products based on investments in solar power plants, particularly in France's Overseas Communities. It offered a 7% annual return, since the product was eligible for tax breaks under the Girardin Industriel Act (which introduced tax breaks for investments in the Overseas Communities). The company collected €18 million from a great many private and institutional investors.

Some of the money was embezzled via a sophisticated scheme using economic structures with bank accounts located in European countries that offered advantages in terms of taxation and banking secrecy. The beneficial owner of these accounts was the director of the original investment company. The individual already had a criminal record for conspiracy to defraud.

Case study no. 8

### Misappropriation of public subsidies for vocational training

A limited liability company (SARL) in one of France's Overseas Communities specialised in vocational training and test preparation. It offered diploma courses and programmes to get jobseekers into the work force, for which it was granted, in a one-year period, several hundred thousands of euros in public subsidies from the European Social Fund. These subsidies represented the company's sole sources of funding.

As it turned out, the company made no expenditures relating to its stated activity. On the other hand, 40% of the subsidies were spent on wages (of which half went to the company's managing director/shareholder), 30% went to social security contributions, and 12% to spending on real estate and services companies. These facts are evidence of misappropriation of public monies and fraud. This case is connected to similar misappropriations carried out to the detriment of a university research centre.

Case study no. 9

## Misappropriation of back-to-work initiatives

A non-profit organisation was set up to help unskilled young people find work through the "Jobs for the Future" initiative. The organisation partnered with the youth employment division of Pôle Emploi (France's public employment service agency) as well as with two companies: one providing training for young people, and the other specialising in home services.

The organisation then created five regional offices in major French cities and began to offer trainings and "Jobs for the Future" positions. Doing so allowed the organisation to benefit from public subsidies granted by the Regional Directorates for Enterprises, Competition Policy, Consumer Affairs, Labour and Employment (DIRECCTE).

As it turned out, the two partner companies were indirectly owned by the chair of the organisation. Setting up the organisation provided access to subsidies unavailable to the private-sector firms, which the chair then partly misappropriated for personal use. In addition, the organisation provided inexpensive labour to the two companies, within the framework of two secondment agreements to supply not-for-profit "Jobs for the Future" staff, in direct violation of labour law.

Less than a year later, the Prefect decided to suspend the subsidies to the organisation on multiple grounds, including questions about the mentoring and tutoring conditions provided by the training firm, deficiencies observed with respect to HR management, doubts as to compliance with labour legislation and training sessions being ended in mid-cycle. Subsequently, the other DIRECCTEs also ceased to provide subsidies, which led to the winding-up of the five regional structures.

In 2015, Tracfin also noted several fraud patterns in the retail pharmacy sector.

Case study no. 10

## Undeclared activities by retail pharmacies

Some retail pharmacies have developed a sideline of selling infant formula and beauty products to tourists from Asia. This is sometimes carried out in collaboration with tour operators, who bring tourists to the pharmacies in question. Customers systematically pay in cash.

For example, one pharmacy deposited more than one million euros in cash into its bank accounts, although before starting the sideline its annual turnover was around €1.3 million. At the same time, the volume of its bills of exchange for orders from suppliers increased dramatically. The company stated that the cash deposits were the result of exports of healthcare products to Asia. However, under Article L.5125-1 of the French Code of Public Health retail pharmacies are statutorily prohibited from engaging in wholesale exports.

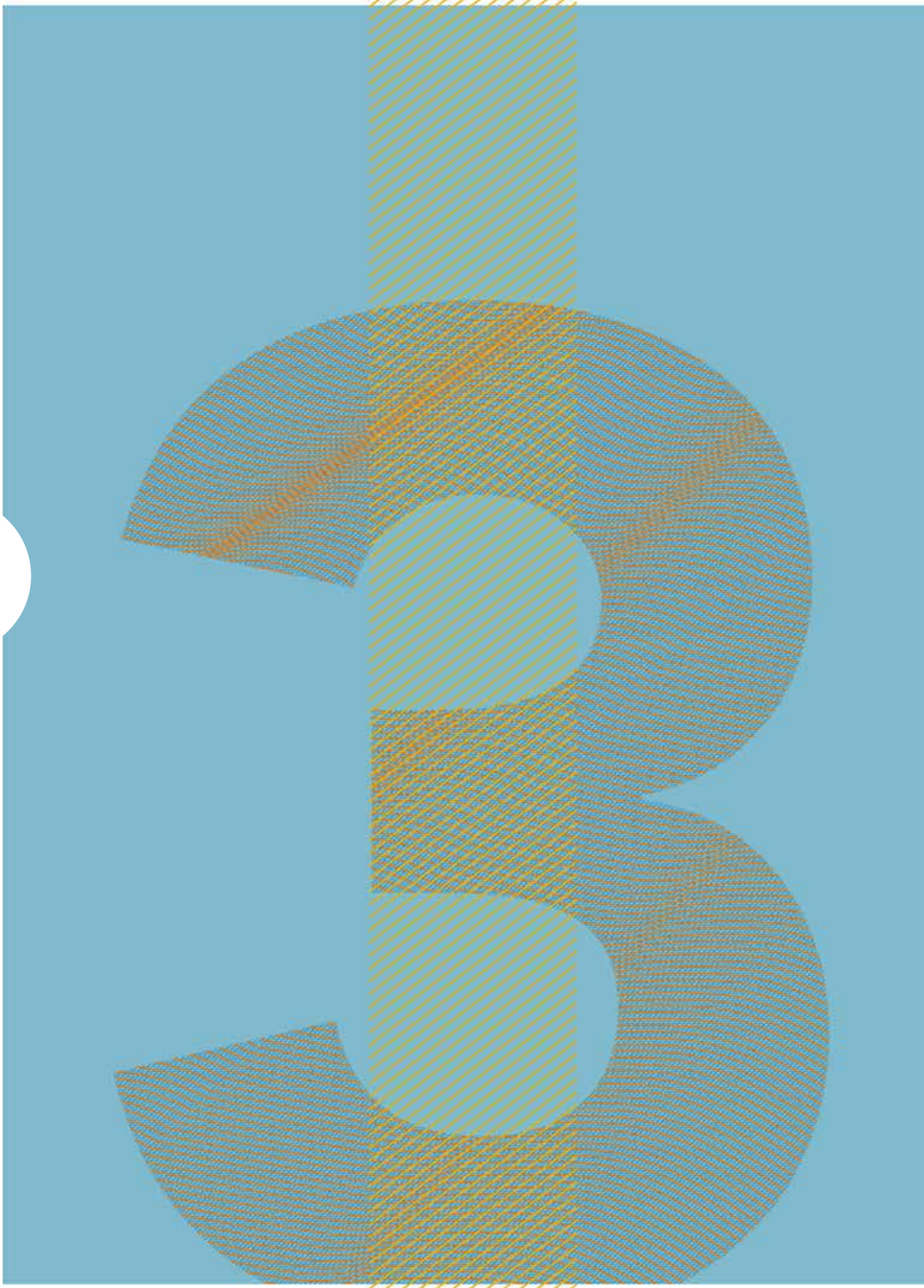
To support its claims, the pharmacy presented invoices to an Asian company. The amount of each invoice was less than €3,000, thus making cash payments legal. Upon closer examination, the invoices were found to be false, and the Asian company that purchased the goods could not be found. In addition, the pharmacy had not filed an export declaration with French Customs.

Case study no. 11

## Misuse of the regulation governing back margins

Another fraud pattern has been developed by several pharmaceutical firms seeking to provide pharmacies with financial incentives to sell their generic medicines. The system consists in circumventing the laws governing back margins, which cap the discounts drug companies can give to pharmacies. The drug companies set up firms whose business purpose is to provide consulting on how to process medical data, or which carry out opinion polls and surveys. These firms ask pharmacies to respond to survey questionnaires, for which the pharmacies are paid abnormally high amounts. This type of circumvention, whose aim is to encourage pharmacies to sell drug companies' products, also induces misappropriation of corporate assets and tax evasion.

This presentation of the main threats to the French economy is by no means exhaustive. It is the result of Tracfin's analysis of the STRs it receives, and of exchanges between the Unit and its partner departments. Its goal is to help each entity subject to AML/CFT reporting requirements to more precisely define its risk map, based on the nature of its business and its customers. Increasing the quality and accuracy of STRs depends solely on the quality of the due diligence of each individual reporting entity. This is the cornerstone of the structure that allows Tracfin to perform its duties effectively and to refer relevant information to the courts and other government departments.



# AN ANALYSIS OF THE VULNERABILITIES OF THE FRENCH SYSTEM VIA THE THREE STAGES OF MONEY LAUNDERING

Structural and institutional factors that may provide incentives to commit crimes and to carry out the associated money laundering transactions or terrorist financing constitute vulnerabilities. Vulnerabilities are linked to a country's legal and regulatory frameworks, to financial instruments and products, and to the commercial practices employed in a given sector. They are inherent to the structural nature of a country and its financial centre.

Article 324-1 of the French Criminal Code defines the crime of money laundering as "facilitating by any means the false justification of origin of the property or income of a perpetrator of a crime or misdemeanour from which the perpetrator has directly or indirectly benefited. Money laundering also includes aiding and abetting an investment transaction aimed at concealing or converting the direct or indirect proceeds of a crime or misdemeanour." "

As legal expert Gilles Duteil has pointed out[1], the second paragraph of this article sets out the three classic stages of the money laundering process:

The "placement" stage, also called "pre-laundering" or "immersion", consists of getting the proceeds of a crime or misdemeanour into the banking or financial system. This primarily has to do with infringements, the product of which is paid for in cash. The idea is to transform cash into book money, or to justify the possession of large amounts of cash.

The "structuring" stage, also know as the "layering" or "laundering" phase, consists of successive transactions for the benefit of multiple individuals or legal entities in different countries. At the end of the process, the money has taken on a legal appearance and is ready to be recycled or invested. These transactions make it more difficult for criminal courts to trace the money, as they must call on legal assistance from multiple countries.

The "conversion" or "integration" phase is when the money is laundered in the legal economy, most often via real estate (luxury properties or not), the acquisition of companies, shops, artworks and precious goods, and financial investments. For criminal gangs, these assets can also be used as bribes to facilitate their activities.

There are two types of laundering:

Laundering of cash (see page 35) generated, for example, by drug trafficking, arms sales, human trafficking and prostitution, smuggling, counterfeiting, trading in endangered species, some basic forms of tax fraud, etc. In all of these, payment in cash is always a factor. These flows of cash of criminal origin are often laundered using networks that collect and transport the cash, either physically or using a remittance system such as hawala.

Laundering of book money (see page 43) already present in bank and financial accounts. This book money can be generated for example by carousel fraud, SEPA transfer fraud, misuse of company assets, corruption and public procurement fraud. Changes in how fraud and tax evasion are carried out, combined with the advent of cyber-criminality, mean that today, illegal money is growingly in book form and inside the legal banking and financial system.





**1** Gilles Duteil, "Modes opératoires et évolutions", in AJ Pénal, April 2016, p. 171 (dossier "Blanchiment : nouvelles questions, nouveaux défis"). Gilles Duteil is head of the European Research Group on Financial Crime and Financial and Organised Criminality (DELFICO), head of the Centre for Financial and Technical Studies (CETFI) in the Faculty of Law and Political Science at the University of Aix-Marseille, and member of the National Enforcement Committee (CNS : Commission Nationale des Sanctions).

# LAUNDERING CASH: THE PLACEMENT STAGE

Tracfin notes that there is no letup in the use of cash in the underground economy. Cash is always very present in the illegal economy, and is still the basis for most criminal activities. According to the FATF, even with cases of book money-based fraud carried out via bank accounts, many criminal gangs withdraw part or all of the proceeds in cash in order to transfer it to another country and reinject it into a banking circuit, in an effort to make the money untraceable.

Cash, and especially small denomination notes, are the main form in which funds of illegal origin are generated. To make cash easier to store and transport, it is changed into large-denomination notes. Laundering consists of producing proof for the possession of this cash, or converting it into book money and getting it into the banking system.

## LAUNDERING CASH THROUGH GAMING

As Tracfin has indicated many times in its previous publications, the gaming sector is susceptible to the risk of laundering of sums in cash.

- Sports betting in physical points of sale allows individuals of unknown profession and/or with low incomes to wager large amounts in cash, using repeated bets, on sports matches where payouts are low. This means the winnings are proportional to the bets, but with a lower risk of loss. By accumulating their winnings, players pass the "large-scale win" threshold, and thus can be paid by check. In this way, players obtain justification of the origin of the money, allowing them to deposit it into the banking system and give it a legitimate appearance.
- Purchasing winning scratch tickets or horse race betting slips is a long-standing technique, but one that is still in use. The money launderer offers to buy the winning tickets from the winners in cash, and for more than the amount written on the ticket. Thus, in exchange for a payment to the initial winner, the launderer receives proof of the origin of the money.

These types of transactions often necessitate the involvement of managers of the points of sale, particularly when they agree to a sudden upturn in turnover for certain types of games, focused on just a few players who place bets primarily in cash.

Casinos remain a sensitive sector in terms of AML/CFT. They are a relevant indicator as to whether individuals are in possession of and are handling cash of criminal origin. The clients of casinos in urban areas that have high rates of criminal activity include representatives of this criminality, who wish to gamble some of their ill-gotten gains. Some players wager large amounts of illegal cash, either by inserting it into slot machines that accept banknotes (bill acceptors), or by repeatedly buying chips and cashing them in, often for amounts that are under the threshold at which they would have to present identification. The cash and chips often belong to different individuals, who agree to use the casino as a way to transfer money between them.

Suspicious behaviour of this type should be the subject of improved communication between pit bosses and cashiers, particularly in large casinos at busy times. KYC initiatives are an important part of the work of casino professionals, who offer various services to their customers to keep them coming back. These efforts should also be made in terms of AML/CFT due diligence.

In this respect, untraceable individuals wagers in casinos make it difficult to claim criminal offences in this sector, and contribute to high levels of AML/CFT-related risk.

Finally, non-compliance with regulations by a casino director opens the door to a number of ways to launder money, including issuing cheques to certain players for undue winnings and allowing cash of criminal origin to enter the casino's accounting system.

## LAUNDERING CASH USING PREPAID CARDS

Anonymous prepaid cards – which can be loaded using cash and which allow holders to make withdrawals, purchase items on the Internet and transfer money – represent a major AML/CFT risk.

Some cards, particularly those issued outside the EU, can be activated without a reliable identity check and have high load limits. They can be purchased in bulk and delivered by an individual or sent by post, thus allowing large sums of money to be transferred in complete anonymity. These cards have undeniable appeal for both criminal networks and terrorist organisations.

When it comes to French prepaid card issuers, Act 2016-731 of 3 June 2016 strengthening the fight against organised crime and terrorism and their financing is a first step towards setting a ceiling on use and urging reporting entities to increase their efforts to preserve data concerning the use of these cards for five years. The system needs to be strengthened, for example by systematically identifying the customer right from the purchase and each time the card is loaded, to ensure to identity of the card's bearer.

When a large number of cards are used to pay into certain systems, such as online gaming sites or binary option trading sites, they can also be vectors for money laundering.

Criminal organisations set up these sites in countries with weak regulatory structures, so that the sites can be run clandestinely, outside frameworks established by national regulators[2]. They can then be used for in one of two ways:

- To launder money through fictitious users: prepaid cards loaded with cash of criminal origin are given to accomplices, who act as mules. These accomplices knowingly place losing bets, thus transforming the cash into turnover on the accounts of the firm that owns the site, domiciled offshore in an unregulated zone
- To defraud genuine customers, who will never get their money back

## UNDECLARED WORK AS A WAY TO LAUNDER CASH OF CRIMINAL ORIGIN

Paying undeclared workers is one of the primary ways to launder cash of criminal origin. Undeclared work is one of the most common offences in Tracfin's judicial referrals, even though not all of the cases of undeclared work that the Unit deals with have to do with payments in cash.

**2** In France, the Autorité de Régulation des Jeux en Ligne (Online Gaming Regulatory Authority) (ARJEL) and Autorité des Marchés Financiers (AMF). Anyone operating in these two sectors must, in order to legally exercise the profession within France, be certified by the appropriate regulatory body.

Case study no 12

## Undeclared work as a way to launder cash of criminal origin

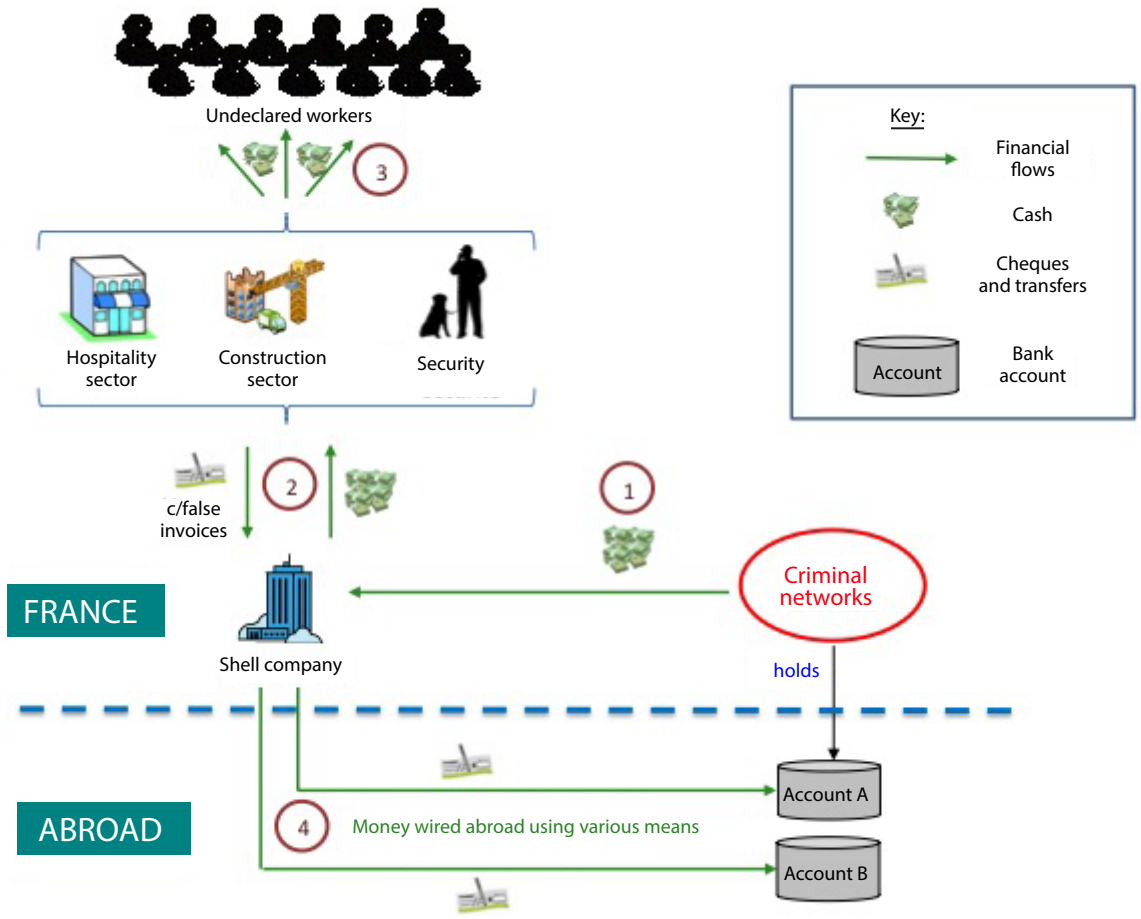
A criminal gang had large amounts of cash it needed to move into the banking system created a shell company to which the cash was entrusted. This firm then gave the cash to a series of companies that relied heavily on manpower, particularly in the construction and security sectors, and also the catering and hospitality sector. These companies then used the cash to pay undeclared workers. In exchange, they wrote cheques to the shell company in payment for non-existent services justified by false invoices.

The shell company cashed the checks and wired the money – now in the banking system – into the gang's accounts using various means. They can use a fund collection and evasion network, which wired the money to foreign bank accounts (see page 42). They also can buy and export goods – fictitious ones, if need be – to countries where the smugglers had support systems (see page 45).

Generally speaking, shell companies have similar characteristics, giving rise to the following warning signs:

- A young manager
- Use of a letterbox firm
- Unclear or shifting business purpose
- Rapid increase in revenue and financial flows that are inconsistent with the company's business activity and declared staff
- Missing tax and social security returns
- Short life span.





## THE USE OF FALSE INVOICES TO EXCHANGE CASH FOR BOOK MONEY

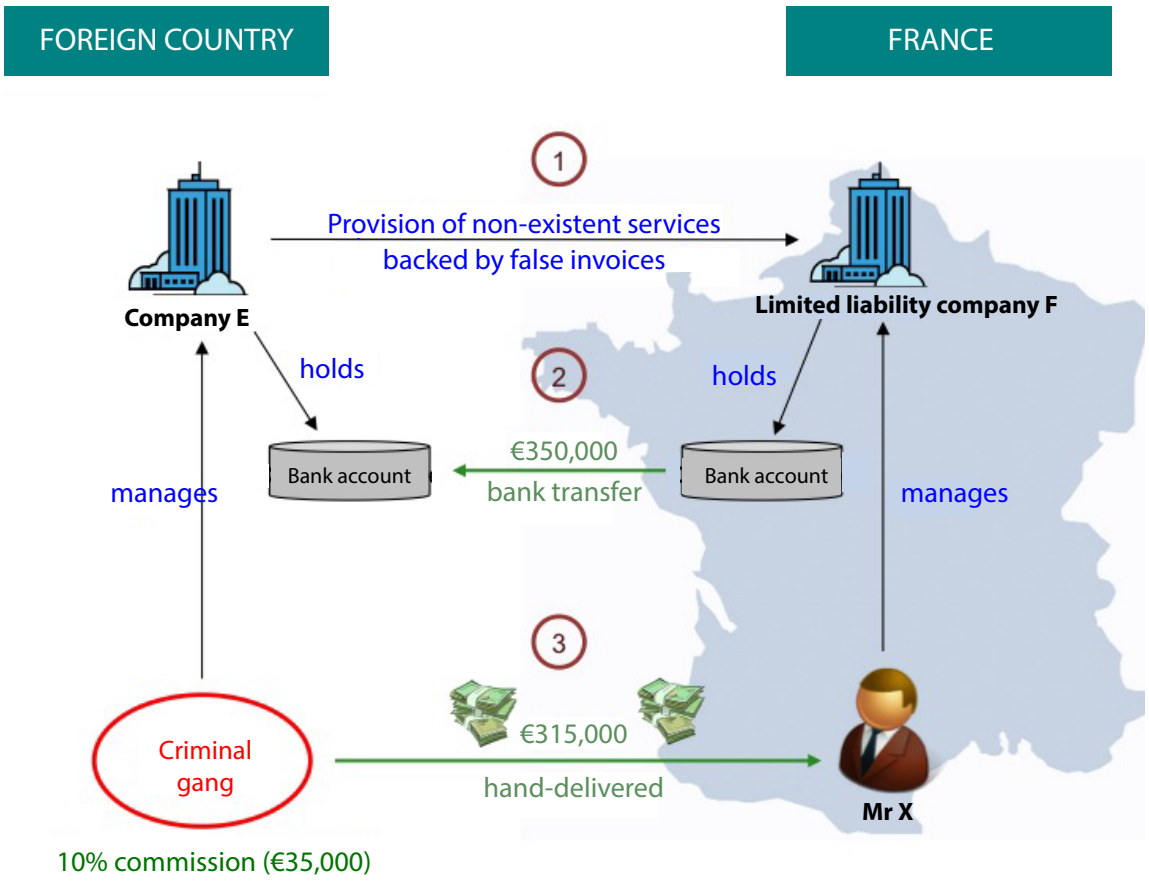
Exchanging cash for cheques, backed up by false invoices, is not exclusively the domain of those wanting to pay undeclared workers under the table. It could also concern company directors seeking to siphon off a part of their company's profits.

Case study no 13

**Between a criminal network that owned Company E, located outside France, and the manager of SARL F, a limited liability company in France.**

- SARL F signed a fictitious services agreement with Company E.
- Using a false invoice, Company E billed SARL F €350,000.
- SARL F wired €350,000 into the foreign bank account indicated by Company E.
- At an agreed-on meeting place, the manager of SARL F was handed 630 500-euro banknotes, or €315,000 (€350,000 less a 10% commission for the money launderers).

SARL booked Company E's invoice, in line with the service agreement. This invoice served to justify the €350,000 payment. What is more, the invoice artificially lowered SARL F's taxable profits. This case involved multiple offences, including forgery and the use of forgeries, falsifying accounting records, misuse of company assets, tax evasion and laundering the proceeds of tax evasion.



## SECRET CASH TRANSFER AND INFORMAL REMITTANCE SYSTEMS

Very often, the fraud and money laundering patterns described above require, at the end of the scheme, the use of clandestine international cash transfer circuits and informal, hawala-type remittance systems. These networks are an integral part of systems to launder cash. They make it possible to transfer large amounts of cash in complete secrecy and outside of any regulatory system[3]. They are also used by terrorist networks, both for channelling funds to war zones and for financing terrorist cells overseas.

### Physical transportation of cash

Collection and international transportation of cash is one of the commonest money laundering methods that exists, whether it is carried out by individuals using commercial airlines, private vehicles carrying cash by road or postal and freight shipments. According to the FATF, the methods used are in line with the end use for the money: blurring an audit trail, re-injecting the money into the banking circuit of another jurisdiction, paying suppliers (smuggling), reinvesting it by purchasing goods (such as cars or weapons) or services (informers, bribes, and so on). The use of the money determines the destination, which in turn determines what transport system should be used.

In France, there are two parts to the system for monitoring physical flows of capital:

- A European part based on Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community. The regulation is applicable to transfers of cash from or to EU Member States (extra-Community transfers).
- A domestic part based on Article L.152-1 of the French Monetary and Financial Code, codified in Article 464 of the French Customs Code, which governs intra-Community transfers of cash.

Thus, all sums of money (cash or cheques), securities (shares, bonds, etc.) or valuables (gold or silver coins, etc.) for an amount equal to or greater than €10,000 (or foreign currency equivalent) carried by an individual must be declared to French Customs, which carries out controls in this area.

Failure to declare sums and false declarations are punishable under Article 465 of the Customs Code, by a fine equal to one-quarter of the sum to which the offence or attempted offence pertains, together with confiscation of the entire amount by French Customs.

#### PHASING OUT OF THE €500 BANKNOTE

On 3 April 2016, the European Central Bank decided to cease printing new €500 banknotes. The stated reason for doing so was to discourage the use of this denomination by criminal networks, in line with the position of several European FIUs, including Tracfin. Those already in circulation will retain their value for an unlimited period of time.

**3** Several recent publications describe these circuits:
**FATF** Report: "Money Laundering Through the Physical Transportation of Cash", November 2015.
**Europol** Report: "Why is Cash Still King?", 2015.
**FinCen** Hawala Report: "The Hawala Alternative Remittance System and its Role In Money Laundering".

## The use of informal remittance (*hawala*)

The informal remittance system known as *hawala* meets the needs of customers who need to send money abroad or to receive it, free from international money transfer systems that require that the money be declared. *Hawala* is completely unregulated, and has the advantage of being rapid and low-cost. It has become increasingly popular with the increase in migrant remittances and the advent of the telecommunication revolution.

Hawala relies on intermediaries (known as *hawaladars*), who are most often shopkeepers that offer *hawala* services in addition to their regular activity. *Hawaladars* must be known and respected members of their communities, with a reputation for dependability. This dependability is the bedrock of the hawala system.

The remittance system is a simple one. The *hawaladars* find customers in their respective communities whose needs match – inverse but complementary.

### Case study no 14
### Operation of a *hawala* network

*Hawaladar* X is established in a European country, and has two customers: a migrant worker who wants to send €700 to his family back in Asia, and a student who wants to receive €1,000 from his family living in Asia. In parallel, *Hawaladar* Y, whose business is in Asia, has the two families as customers.
In Europe, *Hawaladar* X collects €700 from the migrant worker and gives him a code, which the man transmits to his family by telephone or email.
In Asia, *Hawaladar* Y collects the €1,000 from the student's family and gives them a code, which they relay to their son in Europe.
The *Hawaladar*s contact each other via telephone, email or chat site to validate the transactions and exchange codes or ID numbers.
When the customers present their codes, the European *Hawaladar* gives €1,000 to the student (less a commission), and his Asian counterpart gives €700 to the migrant worker's family (also less a commission).
There are no cross-border money flows or international transfers for the customers. At the end of the process, the Asian *Hawaladar* owes €300 to the European *Hawaladar*.

*Hawaladars* try to do business along corridors where financial exchanges balance out, which minimises the need for compensation between themselves. Settlements between hawaladars can take several forms. They can organise for cash to be physically transported between them, or use bank transfers. For privacy sake, settlement transactions are often carried out by means of purchase and resale of goods. To keep the system running properly, hawaladars operate in networks.

They are also particularly high-risk venues for money laundering. They can accept money of criminal origin and integrate it into a formal banking circuit by claiming that it is derived from the their commercial activities, or they can recycle part of the money collected into their commercial activities or into illegal investments.

Warning signs for the detection of hawaladars:

- Large-scale use of collection accounts in which small amounts are deposited on a regular basis and transferred abroad at intervals
- Frequent transfers of funds by shopkeepers to foreign countries without any economic justification
- Business accounts into which large sums of money are deposited, but without any of the usual professional expenditures

In France, hawala is equated with illegally practising the profession of intermediary in banking transactions, but in other Member States, such as the UK, it is entirely legal.

Certain sectors make regular use of the hawala system, in particular those whose commercial activity involves handling large amounts of cash and/or those whose customers belong to a same community.. Large bank transfers into a company's bank account that are unrelated to the company's turnover is a warning sign for the presence of an informal remittance network.

Detecting hawala networks involves a cooperative effort between Tracfin and other departments, and in particular French Customs and the police (the Central Office for the Prevention of Serious Financial Crime).

# LAUNDERING MONEY USING CURRENT ACCOUNTS: THE LAYERING STAGE

## BANK ACCOUNTS: CIRCUITS FOR COLLECTING AND SENDING BANK MONEY ABROAD

Tracfin repeatedly deals with fraudulent fund collection and evasion schemes that make use of the banking system, and which form a large part of the money laundering landscape in France.

These schemes do not make use of complex financial products or structures. Their effectiveness is the result of how they operate: payments divided between numerous companies and bank accounts, combined with speed and agility.

Their success is based on an extremely large number of shell companies and accounts, which blurs a scheme's overall pattern and allows bank transfers to be broken up into quite small amounts to avoid drawing attention to undue amounts.

Detecting these types of circuits requires the involvement of all of the reporting entities involved (commercial registered office providers, commercial court clerks, banks) as well as appropriate due diligence.

Case study no 15

## A fraudulent fund collection and evasion scheme

A criminal gang created a set of shell companies, all of them with the same characteristics: they all had young managers, they were domiciled with a commercial registered office provider, and their business purposes were very general and shifting (construction, wholesaling, communication).

These newly-minted companies each opened several bank accounts, and their turnover grew by leaps and bounds in a matter of months for no economic reason:

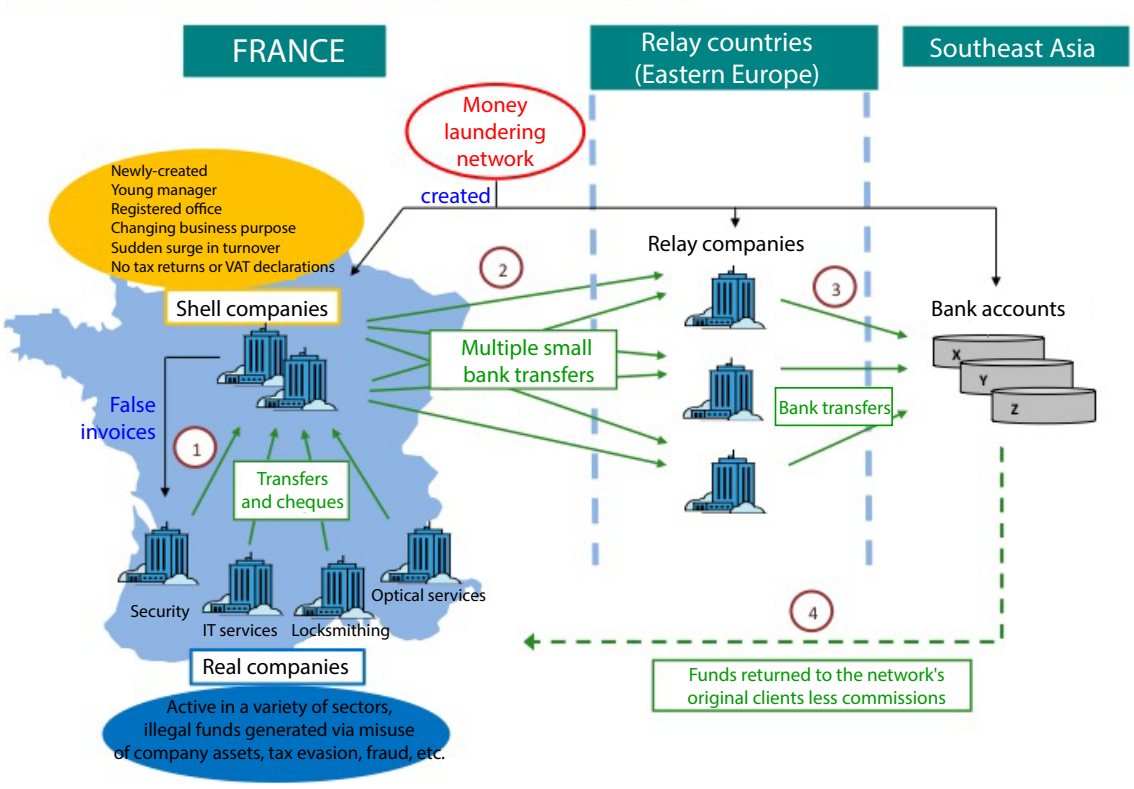
- Sharp upswing in turnover with no increase in staff
- Customers from a wide range of business sectors unconnected with the firm's business purpose
- Suppliers located in eastern Europe
- Financial flows outside France unrelated to the volume of goods declared to French Customs
- No tax returns or VAT declarations filed

Using false invoices, these companies gather clandestine funds from companies active in a number of sectors. The origins of the money stem from a variety of offences, including:

- Misuse of company assets, concealment of turnover either directly or by creating false expenditures, evasion of corporate tax or VAT, and social security and customs fraud as practised by companies in the construction, scrap-metal and vocational training sectors
- Fraud linked with aggressive or misleading sales practices, abuse of weakness or of trust: these are observed in the locksmithing, plumbing and electrical trades, and in the renewable energies sector ;
- Large-scale financial fraud: investment firms running Ponzi schemes, defrauding of mutual insurance companies in the optical and healthcare sectors, carousel fraud

The shell companies quickly transfer the money collected to relay bank accounts opened in several eastern European countries by a new set of companies, all of them created by the original network.

The funds are then once again wired to another set of foreign bank accounts, most of them in Southeast Asia, where they are definitively laundered and then returned to their original owners, who can then reinvest them.



Case study no 16

## Close-up: a fraudulent fund collection and evasion scheme using a mobile virtual network operator

Tracfin has observed that fund collection and evasion schemes, as described above, can be sophisticated operations and can be concealed within a legitimate business sector. In the case below, this involves prepaid phone cards and top-up cards sold by Mobile Virtual Network Operators (MVNOs).

An MVNO sells prepaid phone cards and top-up cards to wholesalers and distributors. It may also sell directly to consumers via a website. To do business in France, an MVNO must be certified by the French Electronic Communications and Postal Regulatory Authority (ARCEP). It has its own network infrastructures, but leases GSM and 3G capacity from the major operators.

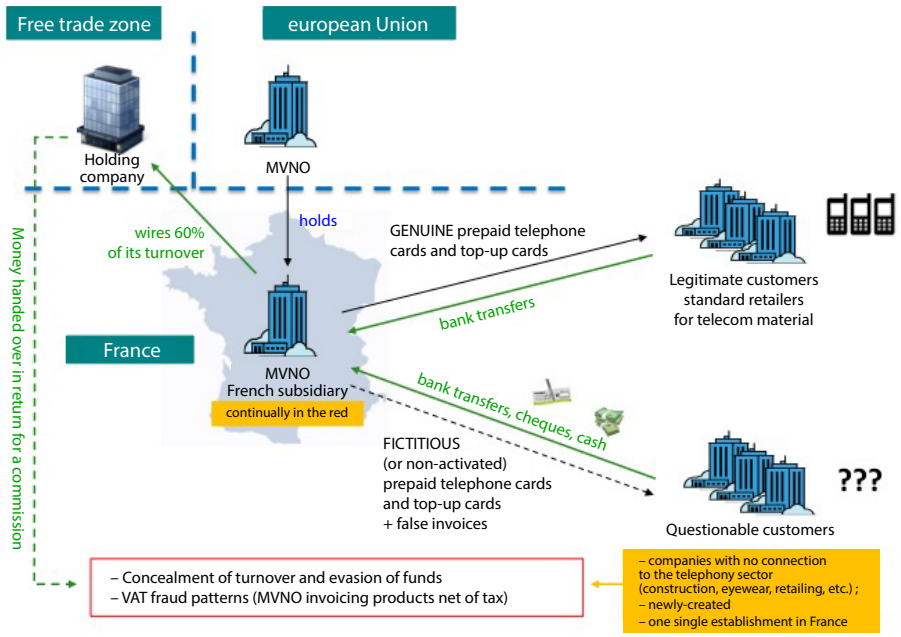
Tracfin worked on a case involving an MVNO which had a set of customers that had no connection with the telephony sector, including firms involved in construction, eyewear, leaflet distribution, property rental, construction of individual homes, installation of insulation, electrical work, etc. These companies, many of which were newly-created, had only a single establishment in France and no distribution network, unlike an MVNO's usual customers. They purchased large quantities of prepaid phone cards and top-up cards, almost as many as more standard customers bought, but with no clear economic reason, since they did not have the capacity to sell or use the cards under normal conditions. Some resold a portion of the cards to third companies. As proof, they showed their banks invoices that were patently falsified.

Finally, it appeared that the MVNO's French subsidiary was constantly operating in the red, but wired more than 60% of its earnings to a holding company whose offices were in a European free trade zone.

In this case, the MVNO operators aided and abetted, or perhaps even instigated a wide-ranging money laundering system that was guilty of a number of offences:

- Concealment of turnover and evasion of undeclared funds: the cards may be fictitious, i.e. undelivered, or delivered but not activated. In this case, payment for the fictitious cards took one of two forms: either with cash derived from criminal activities – which the operator would collect and have transported outside the country in order to enter it into the banking system – or via bank transfers. Banking flows were wired to a holding company in a European free trade zone and then send to the offenders' overseas bank accounts (less a commission).
- VAT fraud: the intra-Community VAT reverse charge procedure only applies to telecoms operators certified by the French Electronic Communications and Postal Regulatory Authority (ARCEP). Normally, the telephone minutes purchased by non-certified companies are liable for VAT. However, the MVNO frequently sold its products with no VAT added to companies with no connection to the telephony sector, which constitutes a breach of VAT collection. In addition, the purchase and resale of telephone minutes on unregulated platforms paves the way for carousel fraud.

In France alone, the amount of money laundered ran to tens of millions of euros per year..



## DOCUMENTARY CREDITS

A documentary credit is a line of credit opened between the bank of an importer in one country and the bank of an exporter in another. The idea is to make the commercial transaction secure by verifying that goods have arrived at their destination and that the contractual documents (bills of lading, customs clearance documents, records of receipt) have been checked prior to releasing payment.[4] Documentary credits are a critical part of financing international trade. Because of this, they are misappropriated and falsified for the purpose of fraud and money laundering. Fraudulent schemes are difficult to detect within the large volume of legitimate transactions.

Case study no 17

### Fraudulent use of a documentary credit

A criminal organisation accumulated money abroad that it wanted to bring back into the euro area via seemingly legitimate means. It set up two companies:

- Company A, an export firm located in the euro area
- Company Z, an import firm outside the euro area

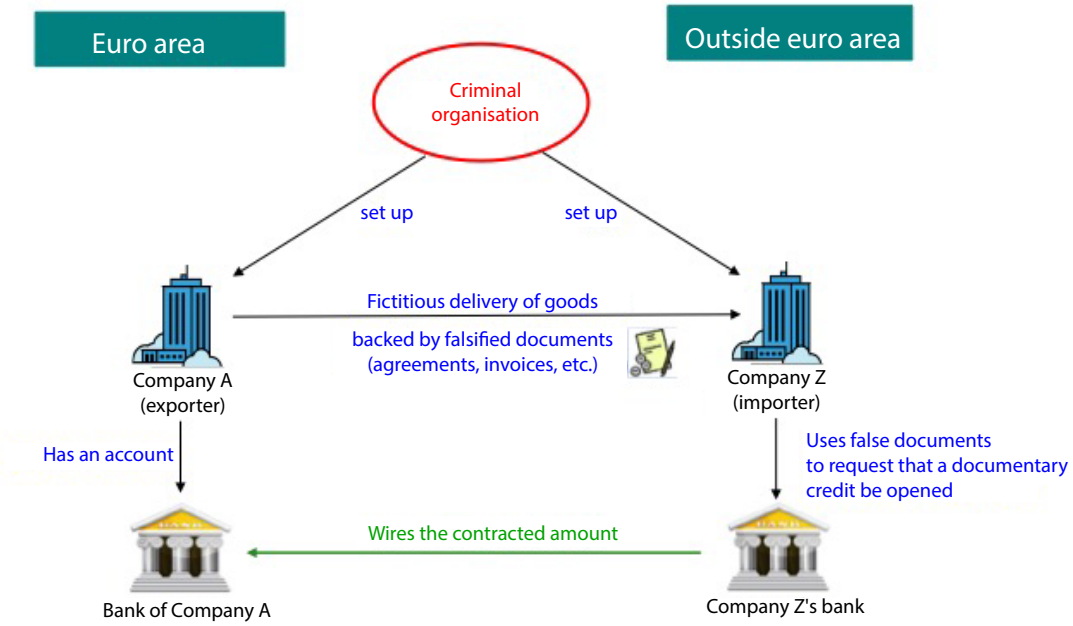
Company A would draw up a fictitious agreement for the sale of goods to Company Z.

Using this agreement, Company Z would request its bank to set up a documentary credit with Company A's bank.

The documents supplied to Company Z's banker were fictitious and had been forged by the criminal organisation.

After a cursory check and approval of Company Z, which would allege that it had received the goods that it had ordered, Company Z's bank would wire the contractual amounts, often running into the millions of dollars or euros, covered by a bill of exchange.

Company A's books would reflect the fact that an invoice had been issued and paid. The goods were fictitious and had never been delivered.




4 Documentary credits allow for the successful conclusion and settlement of a commercial agreement between exporters and importers based in different countries. The commercial partners' banks put up guarantees for their respective clients, which limits the risk that goods will be delivered but not paid for, or paid for and remain undelivered. After a buyer importer and a seller exporter sign the commercial agreement, it is the buyer's responsibility to initiate the signing of a documentary credit by contacting his or her bank. The bank will then open, with the correspondent bank, a documentary credit that is payable to its accounts. The seller can withdraw the funds once its bank has received the required documentation and ensured that it is in order (Le lexique financier, Les Échos).

Tracfin handles a number of cases involving other types of misappropriation of documentary credits:

- A French exporter of processed aluminium products opened a documentary credit to export his or her goods to Country A, and then wanted to transfer the credit so that the payment would be made directly to one of his or her suppliers in Country B.
- An oil company in a country at risk in terms of corruption opens documentary credits in order to export crude oil to a private commodity trader, who then immediately resold the shipments at a high markup. It was revealed that the commodities trading firm was managed by two associates from the exporting country. The documentary credits were proof of price fixing, allowing the private commodities dealer to misappropriate part of the country's oil revenues for the benefit of his company's directors.
- A newly-created French import/export company received payment from a company in Asia as part of a documentary credit, backed by an undated and imprecise invoice that was insufficient proof of the goods in question. The Asian company that issued the payment was difficult to identify. As it turned out, the French firm was using the documentary credit to get agreement for a loan to help it get started.
- Tracfin handles other cases involving documentary credits, for example ones in which payments are made to newly-created export companies whose registered offices are located at the owner's home address, or to offshore firms with no relation to the delivered goods, which were shipped from countries where corruption is rampant. In another case, the instructing party's payment was issued by a private bank whose offer of services did not include trade financing.

## COMPLEX PATTERNS INVOLVING BOTH CASH AND BANK ACCOUNTS

The needs of the grey and criminal economies continue to grow, which encourage money launderers to find new ways to accommodate the increase in volume. The most sophisticated money laundering systems combine several of the aforementioned tax evasion and social security fraud techniques with informal remittance systems and clandestine cash transportation circuits, as well as fraudulent banking circuits.

A significant trend is connected with the expansion in Europe of import/export freight zones under Asian control. These zones have undermined the traditional stakeholders in the textile and clothing sector, but serve as contact points between old and new players.

On the one hand, as a result of increasing flows of imports from Asian countries, including a significant portion of undeclared goods, Asian wholesalers operating in Europe find they have ever-increasing quantities of cash to launder.

On the other hand, increasing instances of large-scale financial fraud (VAT fraud, transfer order fraud, binary option trading websites) combined with networks for cash evasion have meant that specialised criminal gangs have been able to accumulate large sums of deposits – running into the hundreds of millions of euros – in bank accounts in Asia. The question of how to access these funds has become critical.

These parallel phenomena have resulted in a meeting of interests, given the two groups' intersecting needs to access their money. European criminal business networks specialising in large-scale financial fraud have set up their circuits such that the misappropriated funds are wired to bank accounts in a given Asian country. They then transfer the money to shadow banks, located in the same country, which then wire it to accounts opened in Asia by their customers operating in Europe. At the same time, the shadow banks collect the cash from their Asian customers operating in Europe and transfer it to the European fraud networks. For the Asian traders working in Europe, there are no traceable

international banking flows. For the European criminal networks, there is no need to transport cash across borders that must be declared, or which might be intercepted.

The same types of circuits are also used to launder the proceeds of drug trafficking in Europe. The drug trafficking networks give the cash to Asian traders and shadow banks, which then transfer it to Asia using false invoices and fictitious documentary credits, crediting the traffickers' foreign bank accounts, less a commission.

### OPERATION "YELLOW FEVER"

June 2015 was notable for a large-scale operation led by the courts that targeted import/export companies in the Greater Paris region run by members of the Asian community. For the most part, these companies dealt in textiles and fashion accessories, but also in agri-food and other popular consumer goods.

A significant portion of these companies' turnover was in undeclared cash, which led to them stockpiling large amounts of currency. They then offered illegal money laundering and fund transfer services to various networks that needed to recover laundered funds by receiving cash in France – or conversely, in the case of drug smugglers, to launder the funds by transferring them to foreign bank accounts. This constitutes the punishable offence of illegally practising the profession of intermediary in banking transactions and payment services.

In 2015, Tracfin handled a number of cases involving such companies.

## OTHER INSTRUMENTS USED DURING THE LAYERING STAGE

Over and beyond clandestine circuits for transferring cash and fraudulent fund collection and evasion schemes, other financial techniques and instruments can be employed during the layering stage.

### Using real estate transactions during the layering phase

Buying and selling property can be a way to erase the origin of funds.

Case study no 18

#### Transactions involve luxury properties

A France-based holding company acted as a property dealer and worked for family offices. The holding company bought and sold luxury properties. These real estate transactions resulted in significant compensation being paid to various intermediaries, including some known to law enforcement for drug trafficking and money laundering.

The compensation was supposedly for real estate consulting services, having to do with the search for customers and with structuring the financing. In reality, Tracfin suspected the intermediaries of being involved upstream with the family office investors and the holding company. The real estate purchases allowed them to invest funds of illegal origin and recover a portion of the money in the form of commissions. Compensating these intermediaries was the punishable offence of misuse of company assets, to the detriment of the real estate companies involved.

Case study no 19

#### Standard residential real estate transactions

Two brothers, one of whom was a property dealer and the other a craftsman, opened some forty bank accounts in a dozen banks. The idea was to obtain loans to finance the purchase of more than a dozen properties.

The volume of the investments was completely disproportionate to the parties' official incomes. The loans were granted based on false documents, which were obtained thanks to construction and heating installation companies, which acted as accomplices by supplying false pay slips, employer certificates, work estimates, and so on.

Some of the properties were quickly sold after being renovated, leading to capital gains.

There were a number of anomalies in how the properties were bought and sold – transactions that were quite close together, glaring price discrepancies, non-declaration of capital gains, and financing by exterior funds of unjustified origin. The brothers' standards of living increased dramatically (travel expenses, cars, etc.), out of proportion with their declared incomes.

An investigation revealed that the pair were working in collaboration with individuals with whom they were on friendly terms, and who were known to law enforcement for drug trafficking and money laundering. These individuals ran a number of companies, including the ones that supplied the false documents.

## Asset management and the issue of distribution agreements

The purchase and sale of securities also can be used to render funds untraceable. Tracfin calls on investment management companies to step up their due diligence efforts, particularly with respect to their distribution networks.

In distribution agreements for fund units, AML/CFT issues primarily concern the distributor, rather than the management company, which provides a way for the company to lay blame on a third party. This is even more of a problem with bearer units, which make it impossible to know the identity of the final beneficiary.

This flaw in the AML/CFT system could be fixed by getting management companies, custodians and clearance houses more involved.

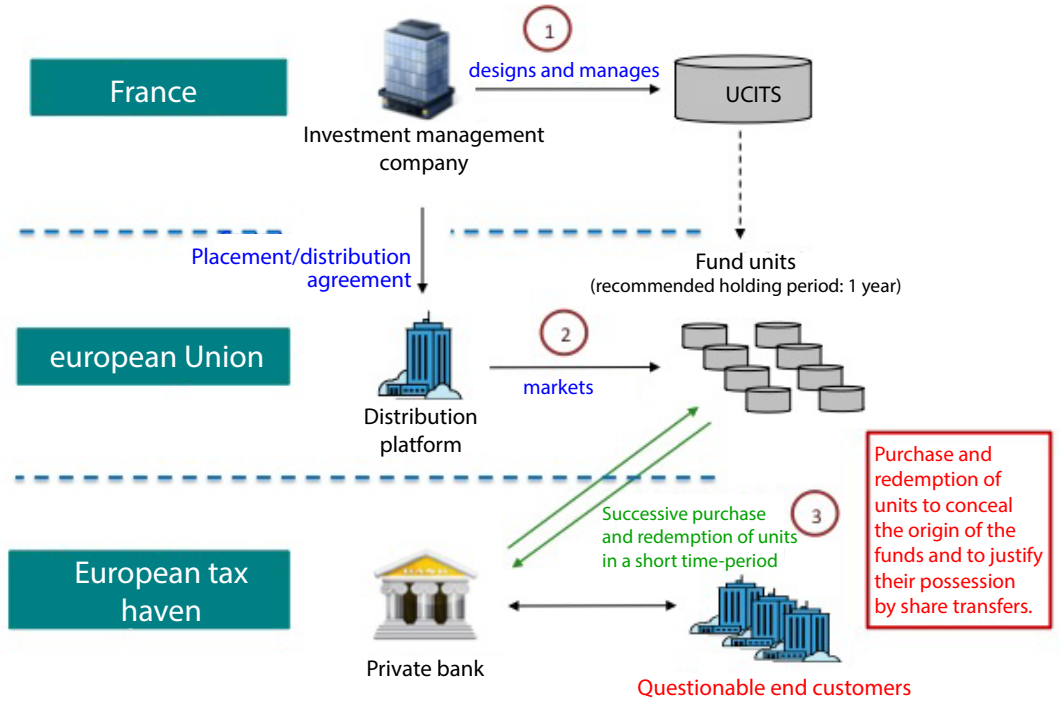
### Case study no 20
### How management companies deal with questionable customers

A French asset management company sets up and manages UCITSs[5], and a distributor, a platform operating in another EU country, markets the fund's units.

The foreign platform is the direct customer of the French asset management company, with which it signed a placement or distribution agreement. In turn, the platform sells fund units to second-level customers with whom the French asset management company does not have direct contact.

The second-level customers include a private bank located in a European tax haven that is well-known for its light-handed approach to regulating and its banking secrecy laws. The private bank acts on behalf of its customers with respect to buying and selling fund units. In a very brief space of time – less than a week – it purchases and redeems fund units that were designed to be held for periods of two years. The private bank could be attempting to hide the origins of the funds and to procure justification of the money through share transfers.

Authorities in the US publicly fined a private bank of this sort in 2015, which led several French asset management companies to provide Tracfin with ex-post STRs on their distributor and the aforementioned private bank. These STRs arrived late in the process, and it is unfortunate that the French asset management companies did not investigate the identity of the beneficial unit holders earlier.




5 Undertaking for collective investment in transferable securities.

## Derivative contracts

The volumes and the liquidity of the financial markets, the variety of underlying assets and the complexity of certain structures make derivatives the instrument of choice for money laundering networks that have sophisticated financial capacities. Case study 21 deals with the use of Euro Medium Term Notes (EMTN[6])

More generally, a money launderer can use market products to discreetly transfer funds between entities in two separate countries. To do so, the launderer uses front men to create two companies in two different countries, and has them take symmetrical market positions vis-à-vis the same underlying asset whose behaviour over time is easy to predict. The loss suffered on the derivative contract by the first company matches the gain by the second, allowing money to be discreetly transferred from one company to the other under the pretext of hedging transactions.

**6** Euro Medium Term Notes: a debt instrument issued by investment banks for professional investors. EMTNs are organised around benchmark underlying assets (interest rates, exchange rates, shares, commodities, etc.), the reimbursement conditions for which vary depending on how the asset evolves, based on scenarios worked out on trading floors. An EMTN is like an OTC-traded bond, whose lifespan and reimbursement conditions can vary.

Case study no 21

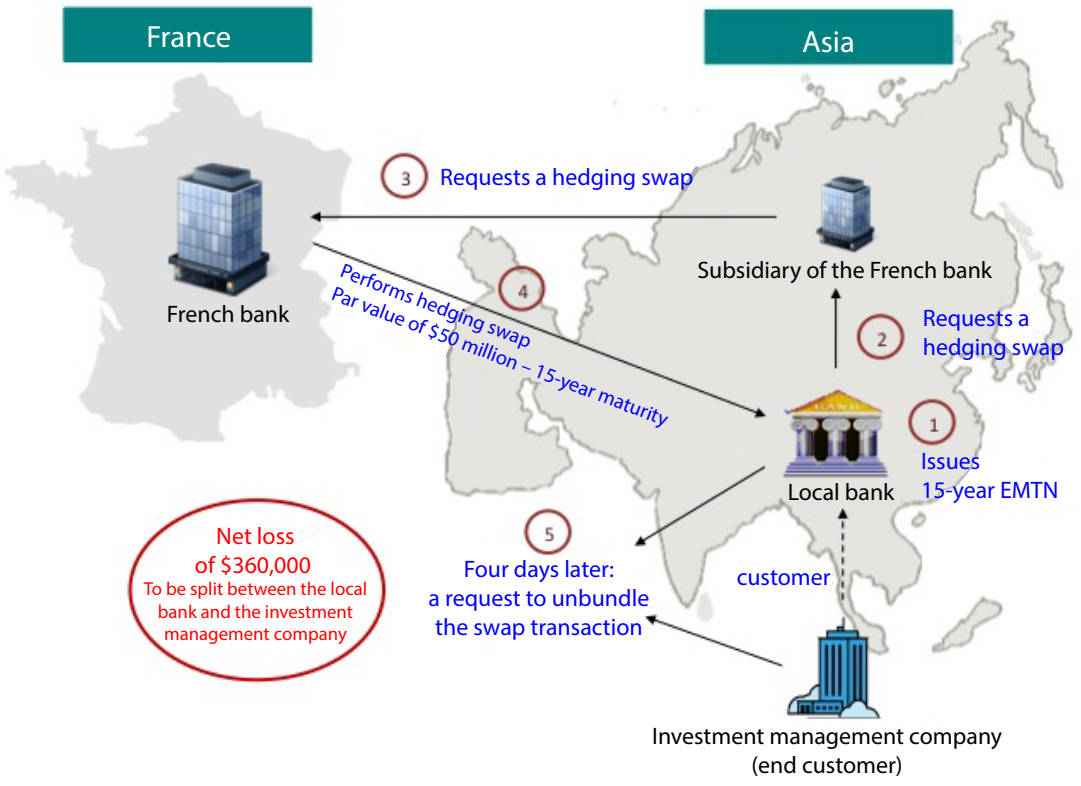
### Unclear transaction concerning an EMTN

A French bank was asked by its Asian subsidiary to issue a hedging swap as part of an issue of a 15 year EMTN.

It was issued by a local, second-level bank, and the end customer was an Asian investment management company. The French bank made out the hedging swap for a par amount of $50 million with a 15-year maturity.

Four days later, the local bank requested that the swap be unbundled, as the end customer had stated that it was no longer interested in EMTNs with 15-year maturities. The early unbundling resulted in a net loss of $360,000, which was divided between the end customer and the local bank that had issued the swap.

This transaction, which was highly unusual and done for no clear economic reason, led to a suspicion of money laundering. The maturity is a critical element that all parties were aware of, and the loss in value was significant for the end customer. The transaction raised the thought that the investment management company knowingly took a $360,000 loss to justify the possession of much greater sums by using the pretext of a trading transaction. The loss would be the cost of money laundering.



# THE INTEGRATION STAGE

At the end of the laundering process, money is reintroduced into the legitimate economy, with an eye to a stable investment where security is just as important as the return. Within the French economic system, money launderers invest primarily in property assets. Investment choices may however concern different categories of assets.

## THE PROPERTY SECTOR: AN ACHILLES HEEL FOR THE FRENCH SYSTEM

Laundered money is as frequently reinvested in **commercial property** as in luxury or standard r**esidential property**.

Case study no 22

### Property development for residential accommodation in the south of France

A property development company rolled out a programme for 200 accommodation units in a coastal municipality in the south of France. It worked closely with an estate agent, a building company and a restaurant management company.

The managers of the various companies involved had close family ties. They had criminal records for extortion, making death threats, armed robbery and fraud in local criminal circles.

These companies' management was characterised by undocumented cash transfers to their managers, who were individuals, which represented misuse of company assets.

Case study no 23

## Reinvesting the proceeds of fraud in an office building

An unregulated website for trading binary options on the Forex market, which had been publicly reported as being unauthorised by the AMF (financial markets regulator) and the ACPR (Prudential Supervision and Resolution Authority), allowed its operators to swindle dozens of victims in France out of a total of €2.5 million over a two-year period. The clients' funds were not reinvested in high-yield market products but were directly diverted to the bank accounts of a number of EU companies, some of which were held in Eastern Europe.

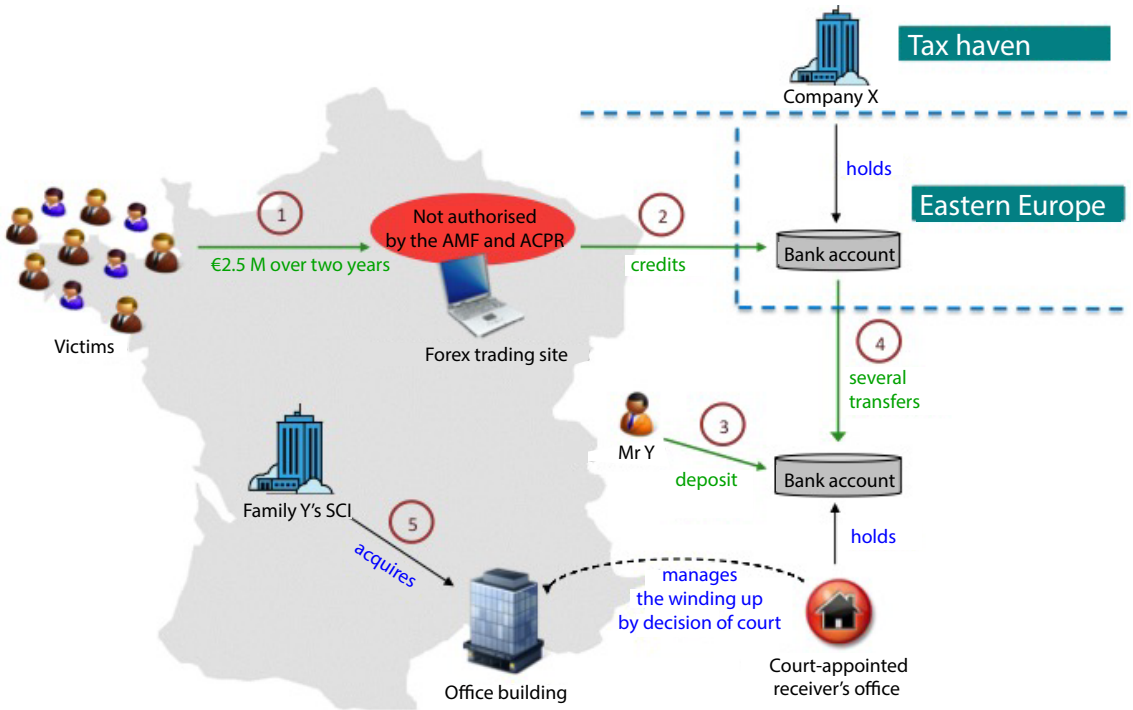
At the same time, a company being wound up by decision of court sold an office building that it owned on the outskirts of a major French city. After the sale appeared in a legal notices journal, the court-appointed receiver in charge of the liquidation was contacted by a potential buyer, who was an individual, and who paid an initial deposit prior to the hearing held to examine the offers.

A year later, it was not the individual who became owner of the property but a property holding company (SCI) owned by members of his family. The majority of the sale price was paid by several transfers to the court-appointed receiver's account by a third-party company which was registered in a Caribbean tax haven and which did not have identifiable beneficial owners. The third-party company sent these transfers from a bank account in an Eastern European country. This account had been previously credited with transfers from the French clients having been swindled by the false trading website.

The investigation into the various stakeholders and cooperation with the relevant foreign FIUs allowed the fraud and money laundering scenario to be reconstituted, with the funds collected by the conspiracy to defraud being directly reinvested in commercial property in France.

The acquisition of the property had all the hallmarks of a money laundering operation:

- Buyer replaced at the time of sale
- Involvement of an offshore structure having a bank account in another country
- Established financial ties with a company collecting the proceeds of fraud.



Case study no 24

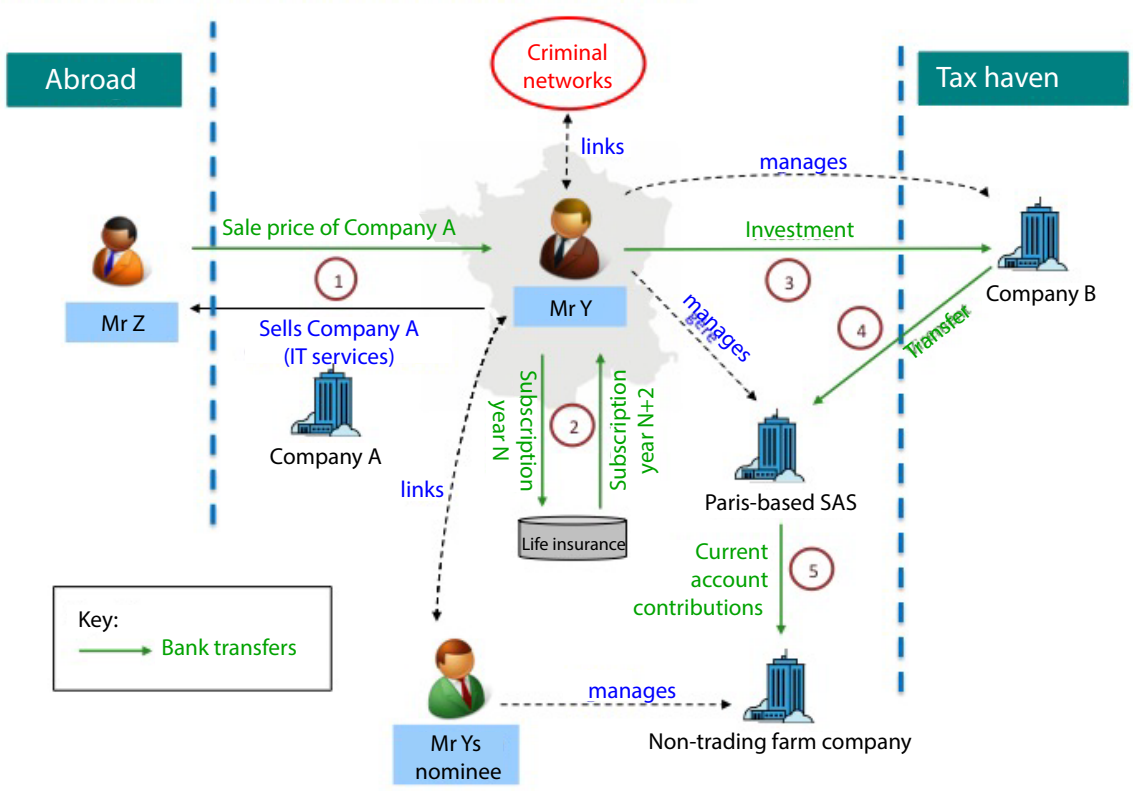
## Reinvesting funds in land for development

Mr Y, who had known links with a criminal organisation, sold an IT services company for an inflated price to an Asian buyer. It was easy to falsify the net book value of the business. The proceeds from the sale were initially invested in life insurance policies.

The policies were redeemed two years later and the freed up capital was paid into the bank accounts of a company registered in a European tax haven that applies banking secrecy. The capital was then transferred to a Paris-based simplified limited company (SAS).

Mr Y was the manager of both the European company and the Paris-based SAS. The funds were then transferred, under cover of current account contributions, to non-trading farm companies managed by a nominee of Mr Y, to fund acquisitions of land for development in the south of France.





Lastly, Tracfin is still handling many cases concerning the acquisition of luxury residential properties by means of complex arrangements in the Paris area and on the Côte d'Azur. When they are able to be identified, the beneficial owners turn out to be foreign businessmen, some of whom have questionable reputations in their home countries. Information on their reputations is backed up by regular and specific press reports or by criminal convictions abroad.

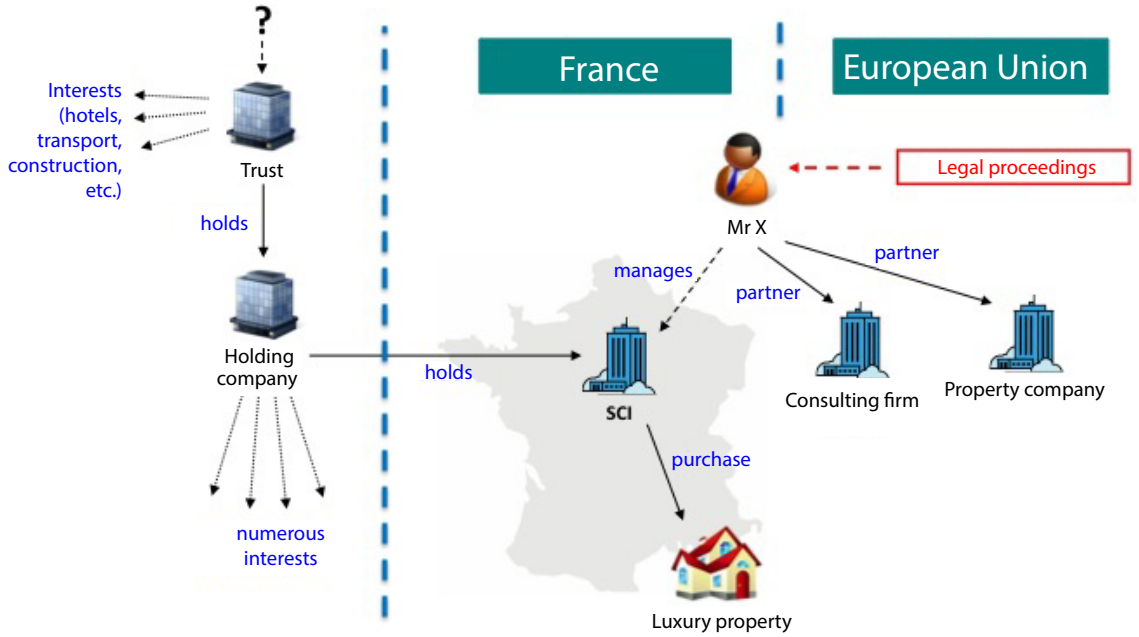
Case study no 25

## Acquiring a luxury residence by means of a complex arrangement

A European national, who was not a French resident, was the manager or partner of three companies: a French property holding company (SCI), a consulting firm with its registered office in Europe and a property company with its registered office in his home country. The majority shareholder of the French SCI was a foreign holding company that owned shares in several dozen companies. This holding company was itself fully owned by a trust which held a number of companies operating in different sectors (hotels, transport, construction), for which it was impossible to identify the beneficial owner.

The French SCI was used to acquire a luxury seafront residential property on the Mediterranean coast for €2.5 million. It was discovered that the European national, declared as manager of this SCI, had been prosecuted by his home country for breach of trust, forgery and mafia-type criminal activities.

The relatively complex arrangements aimed at keeping the buyer's real identity secret, the unusual financial conditions attached to the acquisition (abnormally high amount, funds originating from a non-cooperative country) and the criminal background of the buyer's representative, pointed to the offence of money laundering



## OTHER INTEGRATION METHODS: BUYING COMPANIES, FINANCIAL INVESTMENTS

The integration of the proceeds of crime into legitimate companies or into financial investments is often more discrete than their integration into property investments. Specialised units therefore have more difficulty proving such integration. Legitimate companies are often acquired right at the end of the money laundering process when the funds, held by investment funds or holding companies, already appear to be "clean".

### Buying legitimate companies with the proceeds of crime

The category of target company is dictated essentially by the criminal organisations' financial clout and goals.

- At the bottom of the pile, small-time drug dealers will look to recycle their cash in straightforward businesses such as fast-food restaurants, bars and night clubs, or retail outlets.
- More large-scale criminal organisations will want to buy companies in a sector, in a given country, to gain economic control in that country. Construction is the most-favoured sector. Building networks of SMEs, co-owned by cross-shareholdings between families, removes the competition for public procurement contracts and distributes the criminal organisation's assets, to mitigate the risks of dispossession in the event of court-ordered attachment[7].
- At the top of the scale, transnational criminal organisations with substantial and sophisticated financial resources invest in specific sectors in a number of countries. Their goals will be either vertical or horizontal industrial integration, or making capital gains, especially in sectors such as new technologies, which are subject to volatile valuations and speculation.

To better understand the third category, Tracfin bolstered its organisational structure by setting up an Economic and Financial Predation Unit in July 2015. It is tasked with examining information relating to criminal interference or attempts at criminal interference threatening the capital, know-how, human resources and research of French companies. Using financial analysis and background checks, investigations concern customer poaching, fraudulent operations or offences committed when taking over struggling companies, infringements of a business's intellectual property, and anything that harms France's fundamental interests, within the meaning of Article 410-1 of the Criminal Code. Case study no. 26 provides an example of this unit's work.

7 Clotilde Champeyrache has particularly well analysed this type of investment which is specific to well-established mafia organisations. Clotilde Champeyrache, Quand la mafia se légalise : pour une approche économique institutionaliste, CNRS éditions, 2016.

Case study no 26

## Investing the proceeds of crime in a French technological company

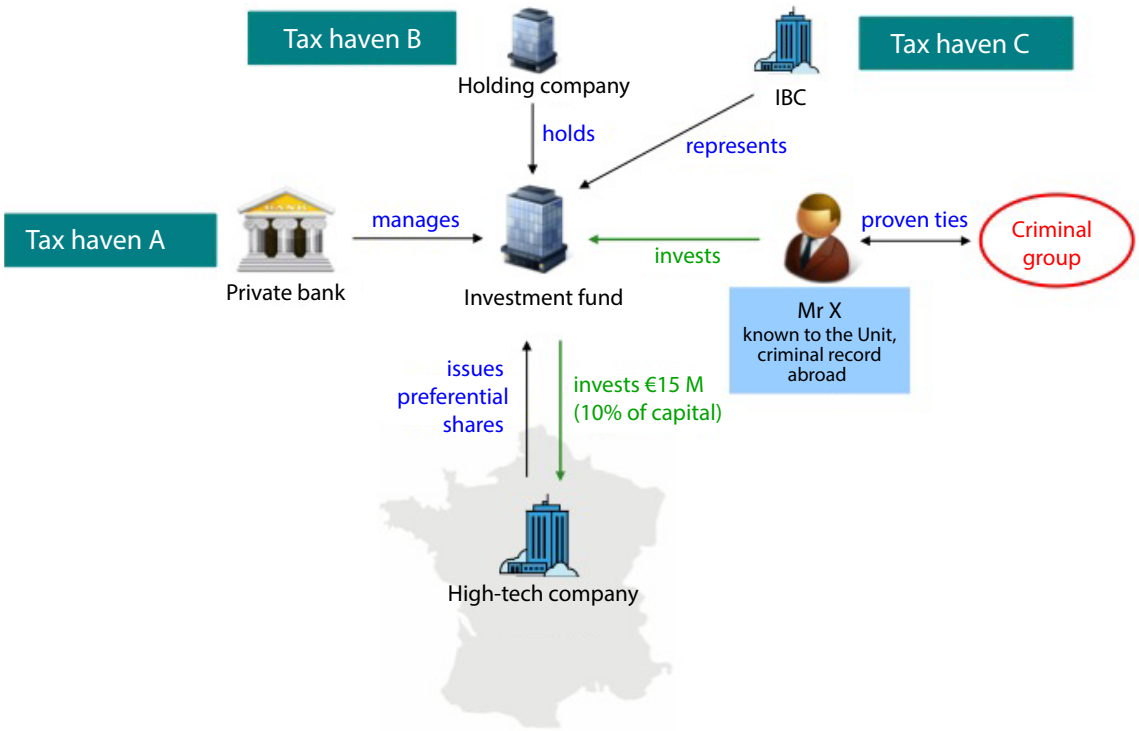
In 2015, a French high-tech company was preparing its floatation on the stock market. An investment fund registered in a tax haven took a 10% stake in the company for €15 million. A specific and excessively complicated process was used: The company's General Meeting granted a derogation to its Board of Directors to resolve to issue preferential shares to the fund.

The fund was not authorised by the markets regulator in the country where it was registered. It was represented by international business companies, registered in non-cooperative territories in South America or the Caribbean.

It became clear that one of the fund's main investors was a businessman who was no stranger to Tracfin and who came from a European country which applies banking secrecy.

The businessman was thought to represent the European interests of a transnational criminal organisation. He established these relationships in the 1980s when he was sales manager responsible for exporting industrial equipment. Starting in the 1990s, he advised clients on investments in Europe, in property, hotels and night clubs, prior to setting up a diversified industrial group (trading metals, metallurgy, services to local authorities).

He has been prosecuted on several occasions by various European justice systems for fraud, breach of trust, fraudulent organisation of insolvency, corruption, infringement of creditors' interests and expropriation of minority shareholders.



## Integration of the proceeds of crime into financial investments

Money launderers also invest funds in financial investments as the very wide range allows them to tailor the term, liquidity and risk/return ratio to the client's requirements.

In this respect, the very size of the French life insurance market means that it is vulnerable. According to Banque de France statistics, at the end of 2015, the French life insurance and endowment markets represented a total value of €1,983 billion, up €25.4 billion on 2014. The ACPR reminds insurance companies that before beginning a business relationship they should always carry out the checks provided for by legislation, particularly as regards customer identification and keep due diligence measures in place throughout the relationship[8].

At European level, however, the French system appears less vulnerable than those in countries that specialise in hosting family offices and/or investment funds, whether these are UCITS[9] or non-UCITS funds such as hedge funds.

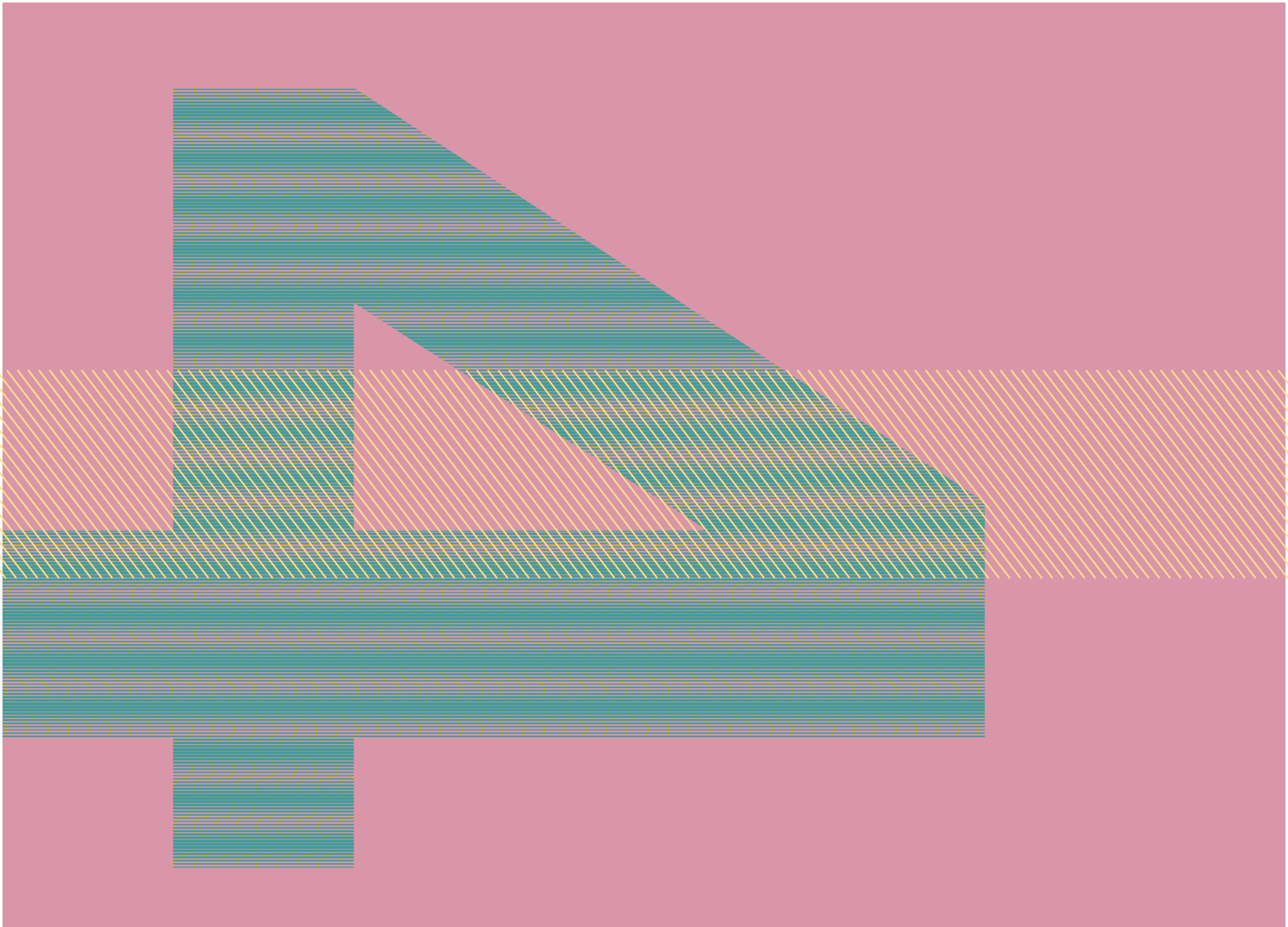
**8** For a presumed case of money laundering through subscription for life insurance policies, see Tracfin report, 2014 money laundering and terrorist financing risk trends and analysis, p. 13.

**9** The term UCITS (Undertakings for Collective Investments in Transferable Securities) refers to a European Directive intending to provide a harmonised framework for investment funds (European passport). The funds covered by this Directive and its amendments, especially mutual funds, are called UCITS funds.

On the basis of the analysis conducted and the information received by Tracfin, the products, financial instruments and legal provisions presented here can represent vulnerabilities for the french AML/CFT system, depending on the needs and intentions of the money launderers.

The case studies are presented in order to encourage reporting entities to definetheir own AML/CFT risk mapping based on the type of products and services they offer, using the warning signs set out. Tracfin draws the attention of obliged entities handling cash (credit institutions, money changers, money transfer companies, retailers in the gaming sector, casinos) and of professionals concerned by the setting up of commercial companies to act as missing traders (accountants, lawyers, commercial register office providers, credit institutions, commercial court registrars) to this.

Moreover, the ongoing technical advances in financial services make it difficult to detect and trace banking flows.



# EMERGING RISKS TRIGGERED BY FINANCIAL TECHNOLOGY REVOLUTION

Over the last two years, the digital revolution has stepped up its expansion into the financial services industry. The number of FinTech companies is on the rise, especially in the fields of payment and fund transfer services. Although it appears to have slowed down during the first months of 2016, the volume of funds raised in 2014 and 2015 rose sharply compared to previous years.

The FinTech boom is opening up a wealth of possibilities but also makes it difficult to regulate and combat cyber-crime.

- As regards regulation, two of the main reasons for creating FinTechs are to ensure smooth customer relations and remove regulatory red tape. This strategy can result innew risks in terms of money laundering and terrorist financing. A number of risks which Tracfin foresaw as early as 2011 have been confirmed whereas others are emerging.
- As regards cyber-crime, the digital revolution, which is extending to most banking activities, is, by its very nature, widening the scope of possibilities and speeding up the transfer of real world forms of crime to the digital arena. Cyber-crime is growing fast and criminals have understood that the digital world provides the best expected gain to prosecution risk ratio. In this respect, the two intrusions into the SWIFT bank messaging system in February and May 2016 are serious warnings. Hackers gained access to ID codes to create and approve SWIFT messages enabling them to transfer several dozen million dollars to bank accounts previously opened in countries lacking robust banking regulation. In both cases, the cyber attacks were aided and abetted by accomplices within the banks using the SWIFT system.

# PAYMENT SERVICE PROVIDERS

Payment service providers figure prominently on the international financial services scene and Tracfin has been paying particular attention to them for a number of years. The Unit has noted two main types of misuse of payment service providers. The first, and most widespread, is the use of legitimate and authorised institutions by criminals. The second, which is less frequent, involves criminal organisations setting up payment institutions to carry out cyber-crime.

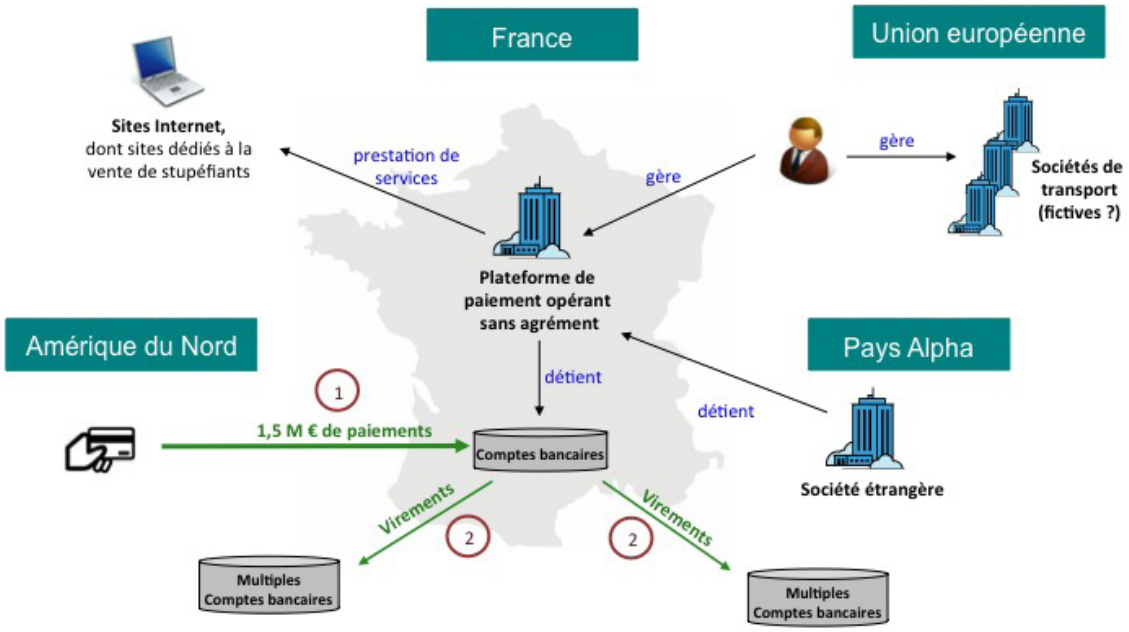
The following case study belongs to the second category. It demonstrates the money laundering risks associated with setting up a payment service provider, which operates without an authorisation for the purpose of committing bank card fraud.

Case study no 27

## Setting up a payment platform for fraudulent purposes

Company A, based in France offered payment management and collection services on the Internet for e-commerce. The company, which was fully-owned by a foreign company with the same name based in European country Alpha, had a large number of bank accounts in France with various banks. But, Company A, which carried on a payment service provider business, did not have any authorisation either in France or abroad.

An examination of Company A's financial flows showed that it had collected approximately €1.5 million in payments by foreign bank cards on its French bank accounts, mainly from the American continent. Many transactions were followed by notices of outstanding bank card payments, the abnormally high number of which aroused suspicions of fraud and fraudulent use of means of payment. Some customers tried to make purchases without paying or their card was hacked by the managers of the company's website. The unusual nature of the flows and the fact that the institution was not authorised point to the fact that the services offered by Company A were fictitious.



Once the payments had been made, the funds credited to the French accounts were quickly transferred to accounts in Country Alpha and in other foreign countries. It appears that the French bank accounts were used during the layering stage of a money laundering operation.

The payment platform managed by Company A was identified as being a payment service provider for foreign websites selling drugs. Company A's manager headed up other companies based in European countries that mostly operated in the transport sector. These other companies did not appear to have a real business activity. Some of these companies had the same address as Company A.

The ties between these companies with very different business activities pointed to the existence of a major money laundering operation connected with an international drug trafficking network. It appeared that the various companies identified were set up with the sole purpose of committing fraud and laundering the proceeds of criminal activities.

The Unit has conducted in-depth investigations into other cases. The international scope of the illicit networks was critical to each case and cooperation with foreign FIUs proved to be vital for conducting the investigations. The presence of foreign institutions and individuals carrying on with their business activity in France under the freedom to provide services creates significant vulnerabilities that are frequently taken advantage of by criminal groups.



# CROWDFUNDING

Crowdfunding has swiftly become a new source of funding for individuals, non-profit organisations and businesses. Crowdfunding was first set up to receive donations but has gradually extended to cover loans and capital investments. As it has scaled up over the last two years, the amounts collected have increased significantly.

Between 2014 and 2015, the amount of funds collected in France doubled. Loans are in pole position with €196.3 million collected in 2015, compared to €50.3 million for investments and €50.2 million for donations[1].

In its 2013 annual report, Tracfin underscored the fact that certain features of crowdfunding such as paperless exchanges, immediate transactions and the lack of physical relations between users mean that it is open to risks of diversion for fraudulent purposes. This risk has been confirmed by a number of international news reports.

A special legal framework was introduced in France in 2014. Crowdfunding platforms are now regulated by Order no. 2014-559 of 30 May 2014 on crowdfunding and its implementing Decree no. 2014-1053 of 16 September 2014, which took effect on 1 October 2014. Its obliges loan and investment platforms to choose between the status of crowdfunding investment adviser (CIP), supervised by the AMF, or that of crowdfunding intermediary (IFP), overseen by the ACPR. Both statuses are subject to AML/CFT obligations. For donation platforms, the choice of IFP status and compliance with the obligations are not mandatory.

**1** France 2015 Crowdfunding Indicator drawn up by CompinnoV for Financement Participatif France.

The rollout of a European regulatory framework is long overdue. France was one of the first Member States to adopt a regulatory framework for crowdfunding. Regulations are however only binding for French platforms and do not extend to the numerous foreign platforms offering donations, loans and investments. Harmonisation of regulations at the EU level, for instance by issuing common certification attesting to consumers that a platform has been verified and approved by a supervisory authority, would enable a certain amount of attempted fraud, money laundering and terrorist financing to be prevented. Making European regulatory frameworks consistent would also stop unscrupulous stakeholders from regulatory shopping to get around the AML measures rolled out in certain countries.

## CROWDFUNDING AND FRAUD

Crowdfunding presents a high risk of fraud, particularly through diverting payments or by setting up Ponzi schemes. Tracfin has noted the existence of such practices.

Certain types of frauds are more prevalent on a type of platform, with loan platforms seeming to be the most at-risk. Furthermore, money laundering may be facilitated by, for instance, applying rates over and above the usury rates.

In the US, the Lending Club scandal rocked the lending sector. After it went public in late 2014, Lending Club was one of the world's crowdfunding leaders. In May 2015, sales of $22 million in near-prime loans were made to a single investor without the lenders having been consulted beforehand. This fraud led to the resignation of the CEO and founder, causing Lending Club shares to lose almost a quarter of their value. In the wake of this major scandal, the American supervisory authorities have been especially attentive to loan platforms to bolster investor protection. French regulations require that investors are kept constantly informed of the use of their investments.

Cases of document fraud and identity theft have been brought to light, thus establishing proof of attempts to get around the due diligence measures. The vast majority of STRs on crowdfunding platforms received by Tracfin in 2015 related to the use of false documents, refusal to reveal identities or to justify the origin of the funds. In most cases, the process points to attempts at layering illicit financial flows with an eye to money laundering.

## DIVERSION OF COLLECTED FUNDS FOR TERRORIST FINANCING

Tracfin pays particular attention to attempts to finance terrorism through crowdfunding platforms, and more specifically through donation platforms, or via money collection sites.

The examination of a platform predominantly dealing with donations, and offering educational and humanitarian projects, led to the discovery of abnormal fund collection practices. Certain financial flows came from sensitive geographic areas. Funds were collected very rapidly and the total amounts collected were unusually high for the type of project being financed. Various projects offered by the platform were examined and it was discovered that a number of them were connected to non-profit organisations whose managers were known to be associates of radicalised Islamists.

The scenario underscores the risks of terrorist financing presented by donation platforms and money collection sites. These platforms may be used as collection points to aggregate flows from various sources towards projects whose actual existence and purpose may be hard to establish. It is sometimes difficult to distinguish contributors who are acting in bad faith, who are involved in projects and who are aware of their final purpose, from those who are acting in good faith, who are ultimately victims of a type of fraud or abuse of trust and who believe that they are supporting the project as presented whereas its purpose is totally different.

As French legislation currently stands, Articles L.548-1 to L.548-3 of the Monetary and Financial Code provide that donation platforms may choose whether or not to become obliged entities. Currently, adopting IFP status is optional for donation platforms. At present, the legislation does not specify

the status of independent money collection sites, which have no links to any crowdfunding platform operator; these websites are not subject to any authorisation and are not obliged entities.

This is the case even though donation platforms and money collection sites are exposed to serious money laundering and terrorist financing risks. Only these stakeholders have information that is required to detect high-risk situations, i.e. on the identity of the beneficiaries of campaigns and the project leaders, or on the nature of the projects themselves. Payment service providers act as the financial medium for collecting funds. They do not have detailed information on final projects. That said, they do process information on the contributors financing the projects or funding the campaigns, in respect of which they are bound by AML/CFT obligations.

Making reporting mandatory for donation platforms and money collection sites would provide enhanced information on the beneficiaries of funds and the project leaders, improved fraud detection and would give a guarantee to consumers that the platform has been subject to minimum verification by a national authority. It is becoming vital to overhaul the European regulatory framework.



# MOBILE PAYMENTS

In a report[2] published in June 2013, the FATF flagged up mobile payments as being one of the new payment products or services which required special attention as part of the risk-based approach to money laundering and terrorist financing. In 2015, mobile payments were available in 93 countries worldwide and telecoms operators managed an average of 33 million transactions per day for 411 million user accounts, up 31% compared to 2014[3].

The expression "mobile payment" covers several types of use:

- Mobile payment associated with a bank card, i.e. contactless payment in stores[4] and online payments to e-merchants, and debited from a bank account
- Online purchases charged directly to the customer's phone bill
- Mobile-to-mobile, national or international, cash transfers requiring a physical sales outlet where the client deposits an amount in cash in return for a code sent by SMS to the recipient. The recipient uses the code to withdraw the cash in another sales outlet.

**2** Guidance for a risk-based approach: prepaid cards, mobile payments and internet-based payment services , FATF, June 2013.

**3** 2015 State of the Industry Report, Mobile Money, GSM Association (GSMA).

**4** In this case, NFC (Near Field Communication) technology is most frequently used. It is similar to a Bluetooth connection between the customer's mobile terminal and the payee's payment terminal.

The risks created by mobile payments are dictated by the types and uses of the technology:

- When the mobile payment is associated with a bank card and account in an EU Member State, the risk is the same as for an ordinary payment by bank card. This risk seems to be under control as the bank holding the account is the main obliged entity as regards AML/CFT obligations and has all the information needed to analyse the flows.
- Payments charged to the customer's phone bill are much less transparent. Only the telecoms operator has information on the origin and destination of the payment with the customer's bank having no access to these details.
- Cash transfers, that are offered by numerous mobile operators worldwide, represent the most significant money laundering and terrorist financing risks. These non-banking transactions, which can only be partially monitored, may lack transparency as cash transfers are anonymous and cannot be easily detected both domestically and internationally.

At the present time, telecoms operators have a substantial share of the market for payment management, which is administered using the various protocols of standard banking architecture. In this respect, they should be subject to specific vigilance.

In France, there is no single legal framework to regulate the expansion of mobile payments. As the financial services offering of mobile telephone operators includes both payment orders and telephone transactions, a single AML/CFT regulatory framework cannot be identified:

- If the transactions are payment orders (contactless payments associated with a bank account, cash transfer transactions using an Electronic Money Institution), they are subject to AML/CFT regulations through the payment service provider used and not the telecoms operator
- If the transactions are telephone transactions, (payments charged to the phone bill), they are not subject to AML/CFT regulations.

## MICROPAYMENTS CHARGED TO THE PHONE BILL

At the outset, payments charged to phone bills were limited to purchasing digital services that could only be used on mobile phones (ringtones, games, apps). They now include purchases of physical consumer goods from online merchant websites for which the telecoms operator merely acts as an intermediary between customer and supplier. As a result, the amounts of the transactions is on the rise.

These micropayments hamper traceability of financial flows which can only be seen by the operator and which are not detailed on the bank statement. The customer's bank only sees a global monthly phone bill debited directly by the operator and is unable to differentiate the amount of the subscription from the flow of ad hoc payments.

As regards regulations, telecoms operators are not subject to AML/CFT obligations and payments charged to bills are expressly excluded from the European Directive on payment services (PSD1) , despite the fact that directly-generated volumes are on the rise. The revised Directive on payment services (PSD2), which was adopted by the European Parliament on 8 October 2015, stipulates that payments charged to phone bills are subject to AML/CFT obligations when amounts exceed €50 for a single payment transaction or a cumulative value of €300 per month. PSD2 should be translated into French law before the end of 2017.

## CASH TRANSFERS BY MOBILE TELEPHONE

During the last five years, cash transfers by mobile telephone have increased rapidly in Africa. These transfers are particularly well-suited to countries where relatively few people have bank accounts. Telecoms operators offer low-cost basic financial services that meet users' needs. This can include payment for goods and services as well as cash transfers.

Cash transfer services by mobile telephone are currently emerging in France with the target audience being Africans living in France who want to send money home. Although, for the time being, these services only concern transfers from France to certain African countries, there is no legal or technical barrier to prevent these flows being sent from foreign countries to France in the future, especially with the potential arrival of new operators.

These transfer services use infrastructure in both the sender and recipient countries, comprised of:

- A payment service provider (PSP) that is a partner, or subsidiary, of a telecoms operator
- A network of distributor agents managing physical sales outlets, who are tasked with collecting or remitting the cash. The agents may be sellers of telecom products, distribution channels and sundry storekeepers, or even kiosks operating a cash transaction business.

From a legal standpoint, within the meaning of the Monetary and Financial Code, this service is a transfer of book money by a PSP in the sender's country to a PSP in the recipient's country. In this case, the AML/CFT risks are similar to those for fund transfer services.

AML/CFT obligations are binding on PSPs offering these services in France. The obligations firstly cover customer identification measures (Articles L.561-5 to L.561-12 of the Monetary and Financial Code), with the primary contributors being the agents and, secondly, the selection and supervision of its agents by the PSP (Articles L.523-2 and L.523-3 of the Monetary and Financial Code).

Besides crediting accounts with cash, transfer services by mobile telephone create a number of vulnerabilities:

- Identifying the customer sending the funds: customer identification information is collected by the sales outlets and must be sent immediately to the PSP in the sender country, which is bound to analyse it and keep it for at least five years. Customers are responsible for updating their ID data with the PSP.
- Identifying the customer receiving the funds: this is the main vulnerability of this type of service. The PSP may be an Electronic Money Institution (EMI) which offers customers an e-money account that can be used with their mobile phones. In this case, besides being able to be withdrawn in cash, the funds received may be used directly to pay for other goods and services.
- Verifying the agents: if the PSP is registered in France, the agents will be declared to the ACPR and be listed on the REGAFI (Financial Agents Register). The ACPR will verify the PSP's agent management procedures. If the PSP is registered in another EU Member State and operates in France under freedom to provide services or freedom of establishment arrangements, its French agents will be recorded with the supervisory authority of the country where it is registered, which will report on them to the ACPR.

The standard of these procedures, and compliance therewith, may vary from operator to operator.

Close monitoring of the risks of money laundering and terrorist financing involves the PSP laying down maximum amounts for transactions, whether these are cash transfers, receipt of funds, withdrawals, account closure or reloading e-money accounts.

Tracfin would like to see regulations adjusted to reflect this new risk to ensure that telecoms operators rolling out this type of service are fully involved in AML/CFT measures and do not leave the PSP to bear all the due diligence obligations. As regards customer due diligence, telecoms operators and the partner PSPs should be able to exchange information on the identity and addresses of their customers in real time. Moreover, the FIUs should have full and direct access to this information.

# VIRTUAL CURRENCY AND BLOCKCHAIN TECHNOLOGY

A currency is said to be virtual when it is not issued by a central bank, credit institution or EMI. It does not have legal tender, is unregulated and is completely controlled by its issuer. It does not guarantee repayment of the funds. As it acts as a gateway between the legitimate and underground economies, and ensures that transactions remain anonymous, virtual currency carries a high AML/CFT risk. It fosters the circumvention of AML/CFT rules, of international financial sanction arrangements, and carries proven risks of fraud and hacking.

Tracfin has been anticipating these risks for the last five years[5] and now they are becoming more of a reality. Use of virtual currency is scaling up although the number of transactions is still marginal in proportion to total payment volumes. In 2015, average daily Bitcoin transactions doubled from 100,000 to 200,000. In nominal terms, aggregate daily transactions were estimated at around $50 million in January 2015 and rose to $125 million in December 2015, with peaks of over $200 million[6].

In summer 2015, new types of virtual currency, such as Ether (ETH), emerged and rapidly gained ground in early 2016. In just a few months, Ether took second place behind Bitcoin in terms of nominal volume of units issued and, at the start of 2016, it was the second most-exchanged virtual currency again trailing Bitcoin.

In France, new companies based around virtual currency are being set up and, as a result, its use is becoming more commonplace. The new companies may be real and virtual currency exchanges, price comparison websites between exchanges and wallet providers[7]. Some wallet providers offer removable media such as smart cards allowing private keys to be stored in hardware wallets.

## USE OF VIRTUAL CURRENCY FOR MONEY LAUNDERING

In 2015, Tracfin investigated a number of cases of misuse of virtual currency for money laundering, including a case concerning the laundering of the proceeds of drug trafficking.

The following case study shows how criminals are able to adapt to new technologies and make use of the anonymity offered by virtual currencies. The lack of regulation and the limited traceability of individuals on virtual money exchanges hampers investigations and fosters the use of technology for fraudulent purposes.

**5** The Encadrement des monnaies virtuelles report, published in June 2014, is based on the work of the "Virtual Currencies" working group led by Tracfin.

**6** Source: www.blockchain.info

**7** The providers supply network interface programmes enabling virtual currency transactions to be carried out. An interface programme allocates encrypted keys to the user allowing him/her access to the addresses where his/her units of account are stored, to sell them or buy new ones.

Case study no 28

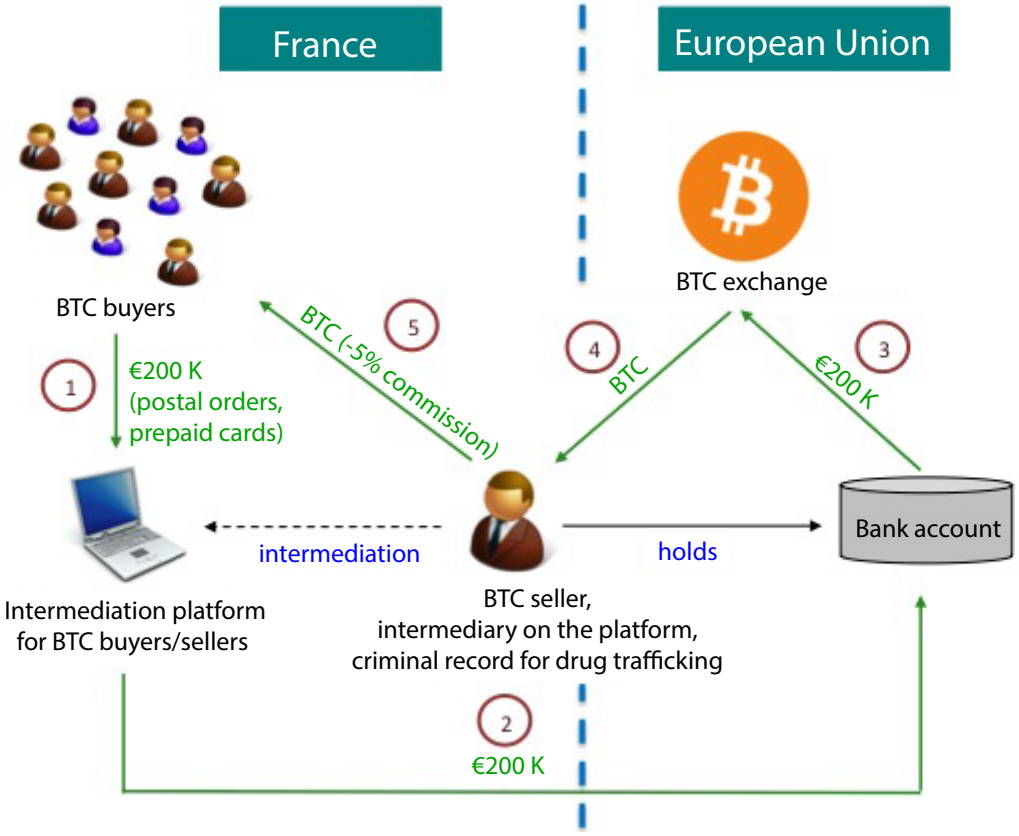
## Laundering the proceeds of drug trafficking by buying virtual currency

A platform offered to put buyers and sellers of virtual currency in touch with each other. An individual acted as an intermediary and, using the platform, collected funds in real currency from hundreds of people representing an aggregate amount of over €200,000 in less than a year. The individual had a criminal record for drug trafficking. The funds were all paid into a foreign bank account before being transferred to a second platform which was an exchange where virtual currency can be acquired by paying in real currency. The intermediary then paid the virtual currency amounts into his clients' wallets which were managed by the initial platform and took a commission.

Once the clients' funds, which were obtained by illegal drug trafficking, had been converted into Bitcoins, the financial flows became untraceable. There are three ways for the individuals to access their funds:

- By withdrawing them in cash at local counters or from terminals
- By using them online to buy goods or services on websites accepting payments in Bitcoins
- By transferring the Bitcoins.





## UNCERTAINTIES REMAIN CONCERNING VIRTUAL CURRENCY

### The regulatory framework

The regulatory framework covering buying and selling virtual currency is still a work in progress. As matters stand, the fact that virtual currency has no legal status means that it is impossible to have blanket regulations extending to all transactions. The role of intermediaries needs to be clarified.

The EU needs to spell out the legal nature of virtual currency to associate it with a payment currency or instrument. Bitcoin buying/selling intermediaries, who up until now have been treated as retailers, could become Banking Transaction and Payment Service Intermediaries (IOBSP) and would be subject to AML/CFT obligations.

On 5 July 2016, the European Commission moved closer to that goal by publishing a proposal to amend Directive (EU) 2015/849, known as the Fourth AML Directive. Amongst other measures, the aim of the amended Directive is to limit the improper use of virtual currency for money laundering or terrorist financing by bringing virtual currency exchange platforms and custodial wallet providers underits scope. These entities will be required to conduct customer due diligence when virtual currency is exchanged for real currency or during virtual currency transactions to reduce the anonymity surrounding these transactions

### Risks of fraud

Virtual currency is open to risks of fraud and hacking. Following the Mt. Gox Bitcoin scandal in February 2014, Ether was hacked in June 2016 and lost half its value.

The Ethereum blockchain was not targeted directly but rather a related entity, called the DAO (Decentralized Autonomous Organization). The DAO is similar to a decentralised investment fund, operating by consensus, and funding projects related to the blockchain and connected devices. Ether could be traded in for tokens giving voting rights within the DAO. The equivalent of $150 million was exchanged in this manner. The hackers exploited an IT flaw to duplicate the DAO and extract 3.6 million Ether worth around $40 million.

### Technological uncertainties

The expansion of virtual currency could be hampered by technological uncertainties. Thus, the steady rise in the volume of Bitcoin created and the increasing number of transactions using the virtual currency are causing network saturation and a potential deterioration of the service.

A number of technical solutions are being considered and are the subject of major disagreements amongst Bitcoin users. The side which manages to have its solution taken up by a majority of users will impose its own standard. It is however possible that no system clearly wins out and this would cause the network to break off into several sub-sets.

## THE DEVELOPMENT OF BLOCKCHAIN APPLICATIONS

The blockchain, or DLT (Distributed Ledger Technology), is an open-source algorithm technology which allows huge ledger databases to be set up. It is used for fully decentralised management of large volumes of financial transactions. Two counterparties can use the Blockchain to securely and instantaneously exchange payment, contracts and ownership title flows. Trusted third parties acting as the central authority (bank, notary, land records) no longer verify the transactions or run checks for related fraud. The features of transactions are constantly checked with all the network's members.

Whilst this technology has been used as a medium for Bitcoin, it can be used to manage financial service processes (payment systems, market transactions, settlement-delivery, etc.) as well as many

industrial procedures. It could shake up organisational structures and significantly cut costs.

Private and public stakeholders both in France and abroad are currently investing in and experimenting with this new technology. In March 2016, during the Convention on Crowdfunding, the then French Ministry for the Economy, Industry and Digital Affairs announced the trialling of a blockchain for the "minibonds" (cash vouchers) market. If the experiment is a success, it could be extended to cover unlisted securities to foster the emergence of an SME stock exchange. In turn, a number of major private stakeholders have announced the launch of experimental blockchains for SMEs, concerning both fund-raising in the unlisted sector or processing listed mid-caps.

Nevertheless, the blockchain has a number of limitations. On one hand, the processing capacity in number of transactions per second is currently well below those for market undertakings and multilateral trading systems. On the other, the transparency of transactions due to decentralisation runs counter to the finance industry's current practices.

Tracfin is closely monitoring the ongoing research work. As it offers management of public records and huge databases, blockchain technology could be used to fight fraud. Conversely, the lack of a central authority raises the issue of liability if the system was indeed subject to fraud or hacking. Furthermore, "private blockchains" could emerge and be restricted to a determined number of individuals. They could offer special and difficultly-identifiable transaction channels with high AML/CFT risks. Legislation needs to be amended to reflect the arrival of this new technology.



## OTHER TECHNOLOGICAL DEVELOPMENTS

The expansion of the FinTech industry is spreading to other financial services, including correspondent banking. A number of startups are looking to penetrate the interbank information exchange market: international wiring; payment tracking; interbank billing. These startups are able to rapidly find their feet as they are set up by experienced managers with high-level knowledge of these professions gained with central or private banks. Both Tracfin and other FIUs need to pay specific attention to the development of these activities which are highly exposed to the risk of money laundering and terrorist financing.

The entire FinTech sector that is directly or indirectly connected with financial services should measure the extent of the AML/CFT risk, cooperate with the public authorities on the shared assessment of the new risks, and act to prevent money laundering and terrorist financing. Failing this, the sector could be saddled with a bad reputation which could become a systemic risk in the event of misuse by criminal or terrorist organisations.

# CONCLUSION

The increase in STRs received annually by Tracfin was confirmed in 2015. Nevertheless, this increase should be more equally spread out amongst all reporting entities. The entities now need to focus on improving the standard of the STRs. All professionals must comply with their AML/CFT due diligence obligations through appropriate customer knowledge, and conduct their own risk assessment on the basis of their business activity, in order to better target and inform the STRs sent to Tracfin.

Owing to the increased terrorist threat in 2015, the majority of stakeholders focused on the detection of financing networks and they should remain vigilant in this respect. Professionals should also address the other threats present in the French economic system, which undermine both individuals and businesses, and which foster "capital flight" involving substantial amounts in macroeconomic terms.

In many money laundering schemes, cash currency circulation and false invoicing play a key role. Interaction between several networks whose interests complement each other and the combination of various licit or illicit legal and financial instruments make for complicated circuits which require major administrative and judicial resources to detect and sanction them. Success is largely dictated by the standards of cooperation between Tracfin, the other relevant government administrations, the supervisory authorities and the judicial authorities.

The speed and responsiveness of exchanges between the FIUs are also vital to improve collective AML/CFT effectiveness. Rapid implementation of the 4th AML Directive into domestic law and work on the amendments to the Directive should make a significant contribution by removing operational barriers to cooperation.

The pace of technological change which has an impact on financial services will pick up even more in the coming years and raises issues in terms of regulating and adjusting the AML/CFT system. The fight against anonymity and bolstering the transparency of financial flows are still core goals to protect the integrity of the economic system. Taking emerging risks into account involves fast tracking the rollout of fresh responses.

Tracfin

**Unit for intelligence processing and action against illicit financial networks**

Publication Manager: Bruno Dalles
English translation: centre de traduction du ministère de l'économie et des finances

10 rue Auguste Blanqui 93186 Montreuil
Tél. : (33)1 57 53 27 00

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

Maquette: Studio graphique SIRCOM — 11.2016