2016

MONEY LAUNDERING AND TERRORIST FINANCING RISK

TRENDS AND ANALYSIS

TRACFIN UNIT FOR INTELLIGENCE PROCESSING AND ACTION AGAINST ILLICIT FINANCIAL NETWORKS

MINISTÈRE
DE L'ACTION ET DES
COMPTES PUBLICS

CONTENTS

Every year, Tracfin assesses the main money laundering and terrorist financing (ML/TF) risks in France. Its starting point is the rollout, at national level, of recommendation 1 of the Financial Action Task Force (FATF) standards which specifies that "countries should identify, assess, and understand the money laundering and terrorist financing risks for the country". At EU level, this recommendation is buttressed by Article 7 of the Fourth Anti-Money Laundering Directive[1] which encourages all Member States to take appropriate steps to assess the risks of money laundering and terrorist financing affecting them.

Tracfin's "risk trends and analysis" reports are primarily intended for reporting entities to inform their own risk assessment. The reports may also be used as mediums for exchanges with the government departments involved in anti-money laundering and combating the financing of terrorism (AML/CFT), and as a source of information for the general public (students, researchers, journalists, etc.).

The "2016 risk trends and analysis" report follows on from the previous report. Without attempting to cover all bases, the 2015 edition took a pedagogical approach to provide the broadest possible overview of money laundering issues, as observed by Tracfin in France. The 2016 report is more selective in its choice of topics which it addresses in greater detail.

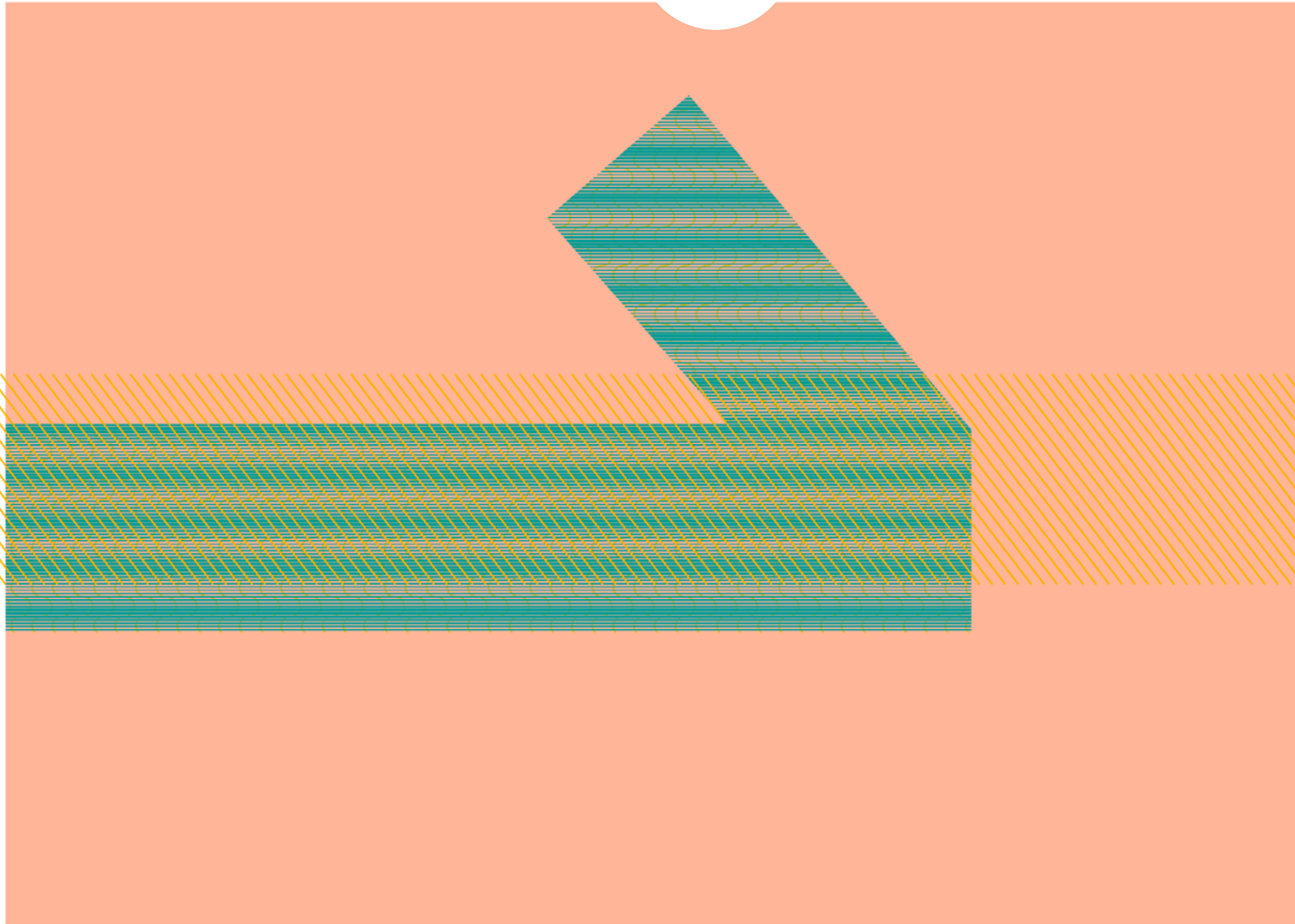
Tracfin issues warnings concerning the extent of the threat of financial crime as major fraudulent undertakings are on the rise. These are carried out by organized groups in conspiracy with others and are highly detrimental to the economy.

The report then sets out Tracfin's work to combat the financing of terrorism which is still one of the Unit's main priorities and a leading focus of national and international cooperation.

The report also covers the fight against corruption and tax and social security contribution evasion which are long-term Tracfin assignments. There are high expectations in this respect owing to the global context, particularly with implementation of the automatic exchange of tax information.

Lastly, the report concentrates on the technological transition which is profoundly altering the financial sector, especially payment and international money transfer services. This upheaval represents a real challenge for established commercial banks and has a knock-on effect to AML/CFT regulations which were designed, at the outset, for this type of stakeholder.

1 Directive (EU) 2015/849.



CRIMINAL THREATS ARE CONSTANTLY INNOVATING AS REGARDS THE FINANCE SECTOR. HOWEVER, CONCURRENTLY, TRADITIONAL MONEY LAUNDERING METHODS ARE STILL USED

In respect of finance, criminal threats can be placed in two different categories:

***- Organized groups in conspiracy with others which** aim to illicitly obtain funds from the victims by fraudulent means. The perpetrators constantly innovate by syste-matically exploiting loopholes in regulations on new financial products and services.*

***- Money laundering networks** which aim to remove the proceeds of illegal activities, to recycle and reintegrate them in the legal economy. These networks may be more or less complex and on an international scale depending on the nature and quantity of money to launder.*

Large scale criminal networks, acting as conspiracies, work in conjunction with wide-reaching international money laundering networks, and this interaction is permanent.

NETWORKS THAT SPECIALISE IN LARGE-SCALE FINANCIAL FRAUD ARE CONSTANTLY INNOVATING

Tracfin has identified networks specialising in sophisticated large-scale fraud as representing one of the main criminal threats. These networks are often built on the back of fraud such as false advertising inserts, VAT fraud (especially carousel fraud) and debt collection fraud at the expense of banks. Tracfin's "2015 risk trends and analysis" report drew attention to diversification involving false transfer orders and fraud on unregulated trading websites (binary options, Forex, etc.)

Since 2016, Tracfin has witnessed the emergence of new opportunities for fraudsters: white certificate (CEE) fraud, SEPA direct debit fraud or proposals for investments in physical commodities such as diamonds. The identified networks of fraudsters may also encourage other economic agents to commit fraud, for instance by offering payment services and Electronic Payment Terminals (ETPs) to enable them to conceal part of their turnover.

WHITE CERTIFICATE (CEE) FRAUD: A SYSTEM THAT IS MISUSED BY INTERNATIONAL CRIMINAL ORGANISATIONS AT THE EXPENSE OF FRENCH ENERGY SUPPLIERS

The white certificate market

The French public authorities introduced the white certificate system in 2006[1]. It was scheduled to ramp up in several stages[2], aimed at a fast increase in the number of white certificates issued.

The purpose of the system is to encourage legal entities to carry out energy savings work or to have such work carried out. In turn, the public authorities provide these businesses with the number of white certificates representing the volume of energy saved due to this work[3].

The system is buoyed up by **energy generating companies**, known as "**obligated parties**" (suppliers of

1 Articles 14 to 17 of the Pluriannual Energy Policy Act no. 2005-781 of 13 July 2005 (called the POPE Act).

2 Stage 1 from 2006 to 2010; Stage 2 from 2011 to 2014; Stage 3 from January 2015 to the end of 2017. Starting in 2018, a fourth stage should enable volumes to be doubled.

3 Energy savings are measured in "kWh cumac" (cumulative kilowatt-hours updated). These constitute the kilowatt-hours saved due to the installation of high energy performance devices and equipment.

electricity, petrol, diesel, liquefied petroleum gas, natural gas, heat or cold)[1].

Each obligated energy generator is given an energy savings target based on its volume of sales. To meet their targets, at the end of the period, these companies must hold a number of white certificates that correspond to the energy savings goals attributed to them.

Should an obligated party fail to achieve its targets, it will be subject to financial penalties. These penalties are in the form of fines of around ten times the amount of the shortfall in white certificates, at the average price for the period under review.

THERE ARE A NUMBER OF WAYS IN WHICH THE OBLIGATED PARTIES CAN MEET THEIR WHITE CERTIFICATE OBLIGATIONS:

1/ Carrying out energy savings measures on their own assets, and converting them into white certificates with the public authorities.

2/ Having their individual or business customers carry out energy savings measures, by paying them subsidies.

The obligated party executes an energy savings work financing agreement with its customer. The customer subsequently sends a work completion certificate to the obligated party and the latter converts this into white certificates with the public authorities. The customer never owns the white certificates directly and may not trade them.

3/ Transferring all or part of their obligations to third party companies (delegatees) by executing an ad hoc agreement with them[2].

These companies may operate, for instance, in the construction or renewable energies sectors. When a delegatee signs such an agreement with an obligated party, it becomes an obligated party itself. It has access to the market and may receive white certificates from the public authorities upon providing proof of the relevant work.

4/ Purchasing white certificates over-the-counter from other obligated parties, other delegatees or from another type of stakeholder called eligible parties.

In the main, eligible parties are local authorities, semi-public companies and social housing landlords. They have no energy savings targets to meet but they can receive white certificates directly from the public authorities when they carry out the relevant work.

White certificates are recognised in a national register kept by a private company which allocates an individual account to each economic stakeholder.

Prices are not determined by the government but adjust themselves on an over-the-counter market between buyers and sellers.

Work providing access to white certificates is categorised by sector (agriculture, industry, services, transportation, residential). The work is divided up into pre-determined operations: the standardised operation factsheets define 189 types of operation and always specify the fixed volume of energy savings permitted by each operation. In some cases, the work is comprised of specific operations analysed as such by the public authorities.

Inspections are carried out by the National Unit for White Certificates (PNCEE), which checks the eligibility of operations providing entitlement to white certificates.

Shortcomings of the white certificate market: Documentary fraud

The delegatees appear to be the system's most vulnerable stakeholders. For a delegatee, the cost of entry into the white certificate market is minimal as it only needs to receive a delegation from an obligated party. Once a delegatee has access to the market, there is a risk that it will produce false files to receive white certificates without having carried out the relevant work.

1 Article L.221-1 and L.221-12 of the Energy Code, and Articles R.221-1 et seq.

2 Article R.221-5 to R.221-7 of the Energy Code.

In practice, the PNCEE's verification work is arduous as little information is provided by the applicant companies, especially when they have used a subcontractor. In theory, the PNCEE does not receive any supporting documents. Obligated parties and delegatees are only compelled to produce detailed documents in the event of an inspection. To compound matters, the PNCEE only has a dozen or so staff. Inspections, conducted by sampling and ex-post, appear inadequate even though they have led to the detection of a number of cases of fraud. In early 2017, the PNCEE had still not handed down any penalties.

A number of provisions governing the white certificate market which encourage business expediency may help maximise the benefits gleaned from documentary fraud.

The valuation of white certificates is dictated by the expected long-term energy performance levels by carrying out certain energy savings measures. However, this valuation does not factor in the actual cost of the work or equipment installed. On a comparable basis, certain measures may lead to high energy performance levels for a minimal actual cost. Amongst the 189 predetermined operations providing entitlement to white certificates, some are more profitable than others. The fraudster companies direct mass promotional campaigns towards the general public, by mailshots or radio and television ads, concerning the most profitable operations.

Furthermore, the purpose of the system's third stage (2015-2017) was to support households suffering from energy poverty by forcing energy suppliers to earmark, over around two years, a billion euros in subsidies for work carried out by the lowest-income households[1]. As the "energy poverty" white certificates are worth more than the traditional certificates, this can compound the risk of cost/benefit distortion and therefore foster the involvement of unscrupulous stakeholders.

Tracfin is dealing with increasing numbers of white certificate fraud cases

Tracfin has seen a sharp rise in the number of cases connected with white certificate fraud. In certain instances, the Unit has exercised its right of opposition to avoid fraudulently acquired funds from disappearing abroad.

1 Refer to the Energy Transition and Green Growth Act (LTECV) of 17 August 2015.

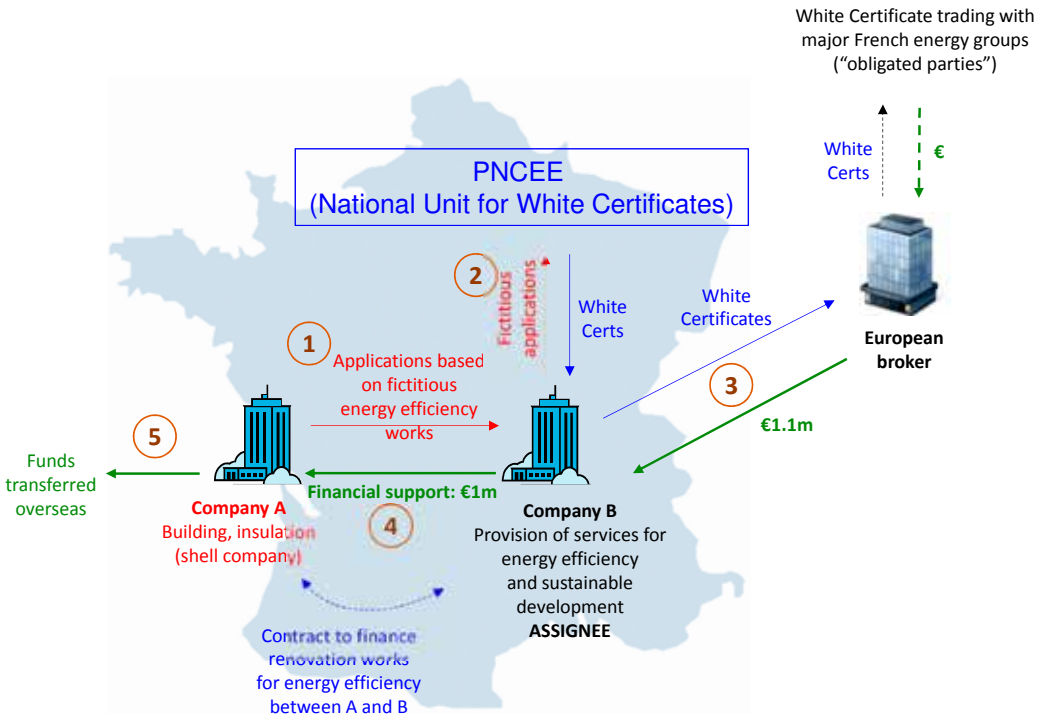
Case study no. 1

A reporting entity drew Tracfin's attention to two companies:

- Company A described itself as a very small enterprise operating in the construction sector and specialising in insulation work. Whilst its annual turnover was around €350,000, it received close to €1 million in financial subsidies from Company B over a three-month period.
- Company B's corporate purpose had been the sale of mobile telephony items and it had recently switched over to providing services for energy savings and sustainable development. It was granted delegatee status by the PNCEE. During a quarter, it did pay almost €1 million in financial subsidies to Company A in the form of cheques and transfers. Over the same period, it sold almost €1.1 million of white certificates to a European renewable energy products broker.

Companies A and B had signed an energy savings work financing agreement permitting Company B to pay subsidies to Company A to encourage it to carry out this type of work and to present the resulting supporting documents. Tracfin's investigations revealed that Company A had presented false work certificates that Company B used to obtain white certificates from the PNCEE. Ultimately, €7 million worth of white certificates were obtained in this manner.

Company A became Company B's main supplier. However, it did not have either the workforce or financial flows to generate enough business activity in the construction sector to warrant work for such amounts being carried out. The structure of its operating expenses did not match those of an SME in the construction sector.



Case study no. 2

Over a little more than a year, Company G, a delegatee, collected more than €13 million from the sale of white certificates to other delegatees. Company H, one of its main customers, purchased more than €10 million worth of white certificates from it. From the funds it collected, and using false invoices, Company G transferred over €7 million to a wholesale furniture and light company based in Eastern Europe. In turn, the latter transferred the funds to Asia. Company G appeared to be the Eastern European company's only customer.

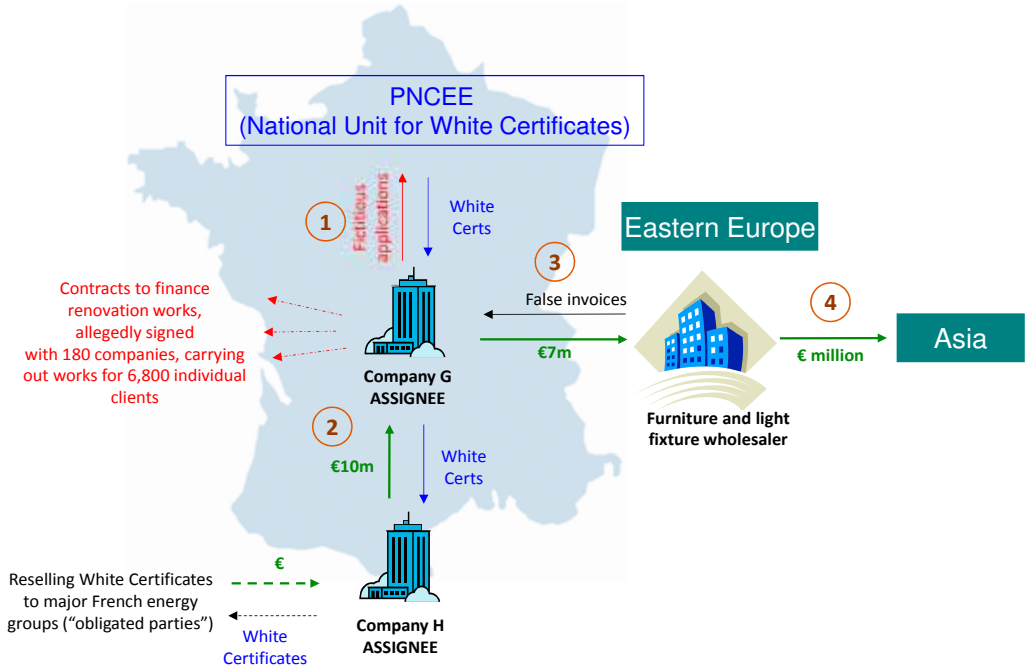
Tracfin's investigations brought to light white certificate fraud using false documents with the proceeds being laundered through a standard illicit bank fund evasion scheme[1].

Vis-à-vis the PNCEE, Company G had justified having carried out 9,000 operations with 6,800 individuals through 180 companies. Company G claimed that it had executed agreements with construction companies to leverage energy savings. It is thought that Company G paid a bonus to the relevant construction companies for each energy savings operation carried out, with this bonus being passed on to the end customer who ordered the work. Company G subsequently received the work completion certificates and provided them to the PNCEE in order to receive the corresponding white certificates. Company G also maintained that it paid over 90% of the white certificates' value to its construction company partners.

Yet, none of the 180 construction companies were able to confirm that they either carried out the operations or received the bonuses. Company G transferred the majority of the funds to Eastern Europe.

Company G's main customer, Company H, bought most of the white certificates that had been fraudulently acquired from the PNCEE from it before selling them on to large obligated parties.

Tracfin invoked its right of opposition in respect of the transfer of €2.2 million from the French accounts of Company G to a foreign account. The Courts were subsequently able to seize €5 million.



1 Concerning fund evasion schemes: Refer to Tracfin's "2015 ML/TF risk trends and analysis" report, pages 42 to 44 (case study no. 15).

In light of the foregoing, the white certificate scheme resembles **an instrument by which France's major energy groups find themselves funding cross-border criminal networks.**

These groups have to meet their targets by buying quotas. Criminal networks cater for this requirement by generating quotas on the basis of false documents and fictitious work. The system is flawed as verification is not sufficiently widespread, either in terms of organisation or scope. Delegatee status is easy to obtain without having to present adequate supporting documents relating to the nature of the activity. As the government does not disburse funds itself, it does not suffer direct financial losses. However, the scheme's public policy targets have not been met.

Its stage 4 will start in 2018. It provides for a sharp increase in the volume of white certificates to be presented by the obligated parties. There is a tangible risk of fraudulent companies circumventing legitimate companies and that unearned white certificates will replace lawfully gained certificates.

It should be noted that the **list of delegatees is made public**[1]. Reporting entities, in particular financial institutions, must use this list to check whether their legal entity customers are delegatees. If this is the case, **Tracfin recommends heightened due diligence.**

SEPA DIRECT DEBIT FRAUD: THE ADVERSE EFFECTS OF EUROPEAN HARMONISATION AND THE FREE MOVEMENT OF CAPITAL

Another type of emerging fraud exploits the shortcomings of the SEPA (Single Euro Payments Area) standard.

This standard was introduced by European regulations on the single European payment area[2] and it took full effect on 1 August 2014. This led to the creation of a standardised euro payment area instead of the patchwork of national standards and instruments previously in place[3]. It recast bank payments in the euro area by altering banks' pre-payment verification processes.

SEPA direct debits

The SEPA standard extends to three payment instruments:

- Transfers (SEPA Credit Transfers or SCTs) which compel banks to carry out the transaction within one business day
- Direct debits (SEPA Direct Debits or SDDs)
- SEPA Cards Framework

SDDs are the most likely to be subject to the risk of fraud. They involve a customer authorising a company to debit the amount of outstanding invoices from his/her/its account.

The customer provides his/her/its creditor with a pre-authorisation (mandate). Instead of the **debtor's banker,** the **creditor** is tasked with electronically saving and archiving the mandate signed by the debtor and for presenting it in the event of a dispute. This has been a major innovation for a number of countries, including France. In the past, the debtor's banker was responsible for managing the authorisation and verified that the creditor holding the mandate actually had a right over the account for which he/she/it gave the identification number.

Now, when the debtor's bank receives a direct debit request, it assumes that there is a mandate and debits

1 See www.ecologique-solidaire.gouv.fr:

Click on the section: "Politiques publiques / Energies / Certificats économies d'énergie / Dispositif des Certificats d'économies d'énergie / Troisième période (2015-2017)". Scroll down.

In the "Obligés de la P3" sub-section an attachment entitled "Liste des délégataires au 2017-09-25" may be freely accessed.

2 Regulation (EU) No 260/2012 and Regulation (EU) No 248/2014.

3 Régis Boulaya (2013), "Les paiements à l'heure de l'Europe et de l'e-/m-paiement", RB édition.

its customer's account. In theory, neither the debtor's nor creditor's banks are obliged to check whether there is a mandate in place.

To shield users from undue direct debits, the process for bringing claims has been streamlined. The European Payment Services Directive (Directive 2007/64/EC of 13 November 2007, called PSD1)[1] sets out the conditions in which debtors can make claims and receive reimbursements of SDDs:

– For authorised direct debits: refund following an ordinary claim within **eight weeks** of the amount being debited, irrespective of the reason
– For unauthorised direct debits: thirteen-month timeline for challenging the setting up of a direct debit (Articles L.133-18 and L.133-24 of the Monetary and Financial Code).

In the event of a claim from a customer debtor, the bank re-credits his/her/its account. It then contacts the creditor's bank. When the latter receives the reimbursement order, it is obliged to return the funds to the debtor's bank. If it cannot take action against its customer, it assumes the non-payment risk from its own funds.

In the same way as cancellation of a direct debit, opposition only relates to the means of payment, and is separate from the underlying receivable. The creditor is responsible for having the debt honoured by his/her/its debtor by any other means.

A system susceptible to the risks of fraud

Throughout the SEPA, it is simple for an entity to set up a direct debit from an account. It only has to provide its bank with details of real bank accounts and the addresses of debtors in SEPA format. Fraud is based on the automatic reimbursement of SDDs which is applied for within the eight-week deadline. Tracfin has observed two main patterns of fraud.

The fraudster receives unauthorised direct debits which have been set up without the debtors' knowledge:

With SDDs, there is nothing to prevent an unscrupulous company from opening accounts in countries with lenient regulations, from obtaining real BICs and IBANs using licit or illicit means (carding), and then issuing a series of cross-border direct debits, before transferring the funds to third party accounts and then disappearing. The fraudster is able to exploit the lack of due diligence by certain debtors and the timelines required for claims to feed through.

Criminals tend to favour direct debits at the end of the business day. This means that the bank will only carry out the necessary checks the following morning whilst the funds will be credited to the recipient's account overnight. This gives the criminals time to transfer the funds to a third party account.

The fraudster issues authorised direct debits and then requests reimbursement:

A fraudster sets up or takes over a company and gives the impression of being solvent vis-à-vis its bank and suppliers by receiving funds in compliance with its corporate purpose. It pays its suppliers by SDDs in consideration of services that are actually provided. As the eight-week deadline for challenging direct debits approaches, the company will tend to buy an increasing number of services.

Although it has actually been provided with the relevant services during the eight-week period, the company applies for the reimbursement of all the direct debits made. Reimbursement is automatic and the bank will re-debit the amount of direct debits received from the suppliers' accounts. As soon as the funds are re-credited to the fraudster company's account, they are transferred to a third party account abroad. Stripped of all its assets, the fraudster company no longer has any funds available when the supplier(s) contact it to be paid their receivables.

With this form of fraud, certain companies will often conspire together:

– Either the debtor companies and the creditor company to defraud the latter's bank. The creditor company will have defaulted while the debtor companies will recover their funds whilst having benefited from the services.
– Or the debtor company and its customers, to defraud the creditor company or its bank.

1 PSD1 was updated by PSD2 (Directive (EU) 2015/2366 of 25 November 2015) which was written into French law in August 2017 (Order no. 2017-1252 of 9 August 2017).

Case study no. 3

Company K bought and sold IT equipment, software and office automation equipment. Having been dormant for three years, the company suddenly changed its shareholder-manager and recorded turnover of €6 million over a three-month period. The revenue came from a number of companies operating in economic sectors susceptible to fraud (renewable energies, security, call centres, etc.).

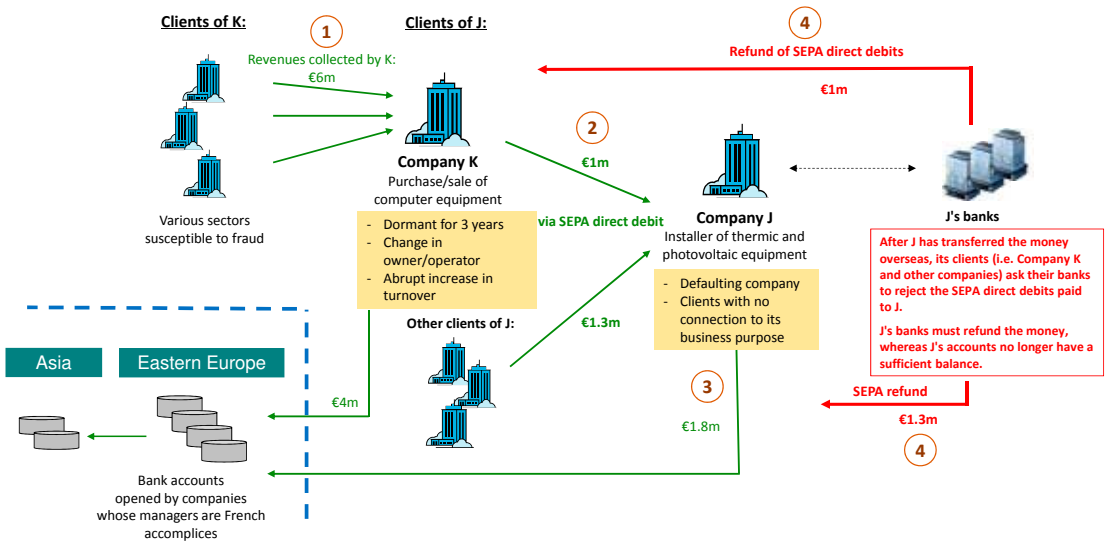
This turnover was subsequently transferred as follows:

- €4 million directly to accounts held in Eastern Europe by companies with French managers, and which was then transferred on to Asia
- €1 million to Company J in the form of SDDs

Company J was a thermal and photovoltaic equipment installer. Its customer base was comprised of a large number of companies, including Company K, that were unrelated to its corporate purpose. It received payments essentially by SDDs.

Company J was a defaulting company. Counting the funds received from Company K and its other "customers" that were unrelated to its corporate purpose, it collected a total of €2.3 million in SDDs over a three-month period. €1.8 million were re-transferred to companies in Eastern Europe.

Once the funds had been transferred abroad, Company K and the other "customers" requested the rejection of the SDDs. Company J's banks were obliged to re-credit the accounts of Company K and the other "customers" in spite of the fact that Company J's accounts contained insufficient funds.



Case study no. 4

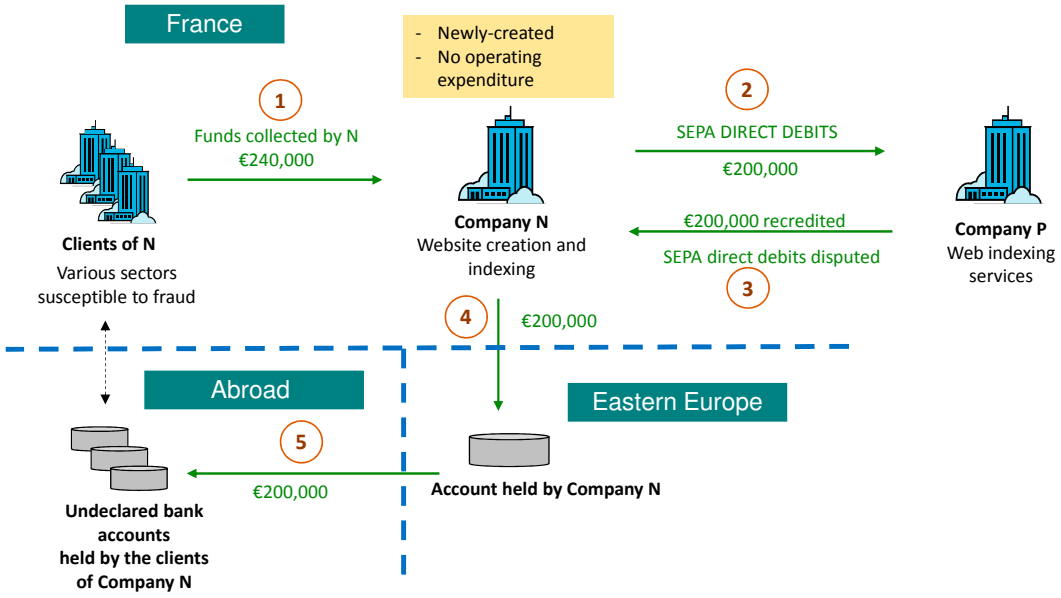
Company N, which was set up by a young manager, offered website creation and listing services.

Over an initial three-month period, Company N had strong business activity and recorded turnover of €240,000 with a number of sundry SMEs (a decoration store, a call centre, two construction companies, etc.). These companies had also been recently set up and had failed to comply with their tax and social security obligations.

Over the same period, Company N did not book any operating expenses (rent, wages, etc.). It did however have SDDs amounting to €200,000 to pay an Internet service provider for listing services.

Less than a month after the first direct debits, Company N's manager challenged all the payments made. In accordance with legislation, the amounts were fully re-credited. The funds were immediately transferred abroad to an account in an Eastern European country. They were then paid over to Company N's initial customers on undeclared foreign bank accounts.

These arrangements enabled Company N's customers to reduce their taxable income by shifting part of their turnover abroad, with this being justified, from an accounting viewpoint, by purchasing online listing services.



Case study no. 5

Company R was a recently-created company specialising in trouble-shooting in the home (locks, plumbing, renovation and insulation work, etc.) essentially for individuals. Over a six-month period, it recorded turnover of more than €400,000, €300,000 of which came from cheques written by individuals.

This commercial success could be put down simply to the company's excellent online visibility which enabled it to reach a broad customer base in a very short space of time. 70% of the company's expenses covered the cost of listing with Internet service providers which was settled by SDDs.

However, Company R was soon subject to complaints from customers about its business practices which were almost tantamount to fraud (over-billing for urgent trouble-shooting or services provided in the homes of vulnerable persons, etc.). Company R's bank decided to end relations following an increasing number of challenged and unpaid cheques.

Following this decision, Company R's manager contested all the direct debits paid to Internet service providers for listing services. As a result, Company R benefited from listing services, recorded high levels of turnover and had its listing expenses reimbursed.

COMMODITY INVESTMENT FRAUD, INCLUDING PHYSICAL DIAMONDS

Since 2016, Tracfin has witnessed a rising number of suspicious offers for investments in diamonds. The Unit has dealt with a large number of cases with similar features. The *Autorité des Marchés Financiers* (Financial Market Authority, AMF) has issued a number of warnings concerning such offers[1].

Offers for investments in diamonds

Gemstone investment companies or brokers provide online offers to invest in physical diamonds which are put forward as a safe asset giving high returns. These companies advertise online, on the radio and television, and aggressively canvass individuals.

They claim that the diamonds are kept in safes in free trade ports outside France. Using free trade ports means that buyers are exempt from paying VAT under customs warehousing arrangements and this further increases the return on investment when the diamonds are sold on.

The purchasing terms offered to individuals lead to doubts as to the actual existence of the diamonds. Clients do not take possession of the purchased goods and do not seem to have any proof of ownership. When they attempt to verify the physical nature of their investment, relations with the companies become strained. It is very difficult, if not impossible, to obtain refunds. In a short space of time, the companies may be unable to be contacted.

Even if a company does have a certain inventory of diamonds, the process of valuing these gemstones is complicated and cannot be easily understood by outsiders. Unlike precious metals such as gold and silver, there is no global public price for diamonds. The diamond market regulates itself and sets its own prices. There is a list that is authoritative: the Rapaport Price List, which is published every week. However, this list is composite and provides price lists by sub-category of diamond based on numerous criteria: weight, quality, actual inventories, production, etc. The investment companies operating in France can easily give false valuations to their clients.

On several occasions, Tracfin has exercised its right of opposition in respect of this type of fraud to prevent funds collected from individuals being transferred abroad. A number of identified beneficiaries were already known to Tracfin for their involvement in fraud on unregulated Forex and binary option trading websites.

1 Refer to AMF press releases dated 6 January, 3 April and 24 July 2017.

Case study no. 6

Company X, a diamond and gemstone trader and broker, received a total of €8.8 million during its first ten months of operations. The credits mainly consisted of transfers and cheques from individuals based throughout France. Over the same period, €8.6 million were debited from the company's accounts, over €6 million of which was sent abroad.

Company X provided its clients with the opportunity of purchasing diamonds which would then be kept in safes under its responsibility. In consideration, buyers were exempt from VAT on their purchases. On its website, the company presented diamonds as a promising investment that should give an annual return of more than 6%.

Tracfin's investigations brought to light a body of evidence throwing doubt on the reality of the company's activity.

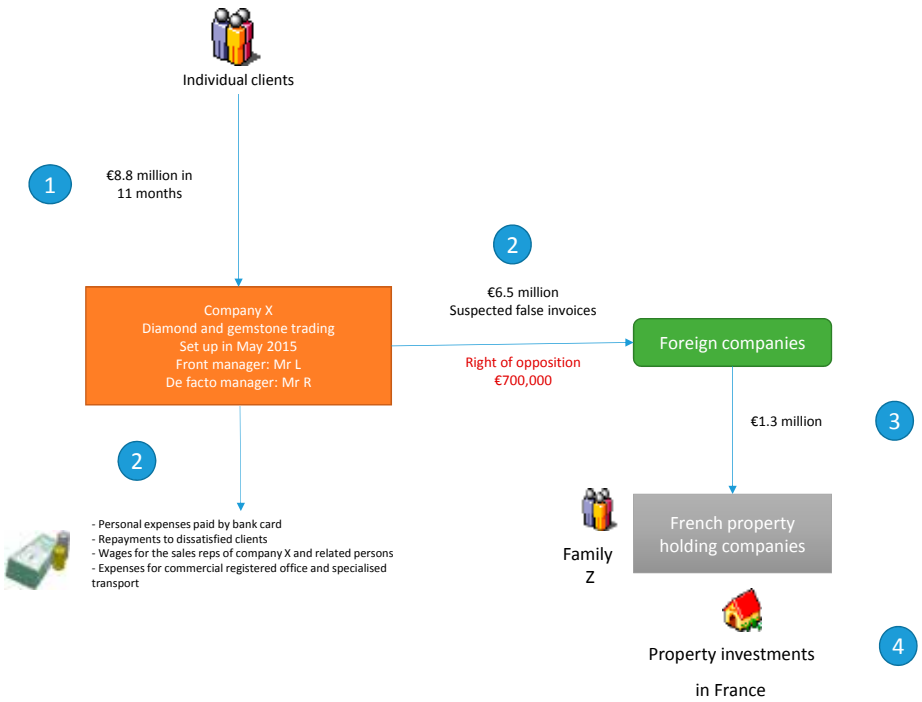
The foreign beneficiaries of the funds were difficult to identify or their business activity had no connection with that of Company X. Inconsistencies between the tax returns and customs declarations filed by the company and the credits and debits on its accounts implied that false invoices had been presented to the banks. Company X's systematic use of virtual office addresses heightened doubts as to the reality of its business activity.

On the debit side, there were expenses for sales reps' wages, repayments to dissatisfied clients and substantial flows abroad. An examination of information received from the Unit's foreign counterparts led to confirmation of the laundering in France of part of the funds sent by Company X abroad (€1.3 million was identified). These funds were reinvested through property holding companies which acquired property on behalf of a family whose members had no declared source of income.

On two occasions during its investigation, the Unit exercised its right of opposition concerning a number of transfers abroad totalling €700,000. Fast identification of the possible victims and the companies suspected of being related to the fraudulent network enabled, in conjunction with the judicial authorities, a precautionary attachment of around €2 million on the French bank accounts of the suspected perpetrators.

Warning signs:

- A recently-created company
- A high-risk investment activity, subject to warnings from the supervisory authority
- Registered office with a commercial registered office provider
- Change of management
- Substantial credits recorded over a short period of time
- Debit flows abroad



Proposals for investments in rare earth metals and minerals

Diamond investment fraud can be replicated for another types of commodities. Rare earth metals and minerals are traded on a poorly regulated and highly volatile market. As these commodities are not financial instruments, traders in this sector do not have to be accredited as investment companies. Information on these markets is fragmented and not easily available to individuals.

Case study no. 7

Company Z claimed to be a broker in rare earth metals and minerals, and strategic metals, for informed professionals and individuals. Using the same methods as diamond investment companies, Company Z offered investments in these commodities to individuals. The investments would be stored in free trade zones and be exempt from customs duties and VAT. Company Z used a virtual office address.

Tracfin's investigations revealed that, over a four-month period, Company Z received payments of €360,000 from individuals in France. On the debit side, the company's expenses did not relate to procurement of goods. The Unit found no trace of purchases of commodities corresponding to the payments made by the individuals. Company Z had not filed any customs declarations covering imports of rare earth metals or minerals.

There were debit movements to a partner company tasked with sales strategy for €80,000, and to a number of individuals for around €200,000. Company Z's manager appeared to be the main beneficiary as he received almost €100,000 on his personal accounts held in another EU country.

This evidence appeared to throw doubt on the reality of Company Z's business activity and potentially represented the offence of fraud by conspiracy.

FRAUD WITH ELECTRONIC PAYMENT TERMINALS (EPTS)

Networks specialising in large-scale financial fraud may also encourage other economic agents to commit fraud. Some payment service providers, which are very probably controlled by criminal networks, offer their customers different ways of evading taxes and laundering money. More specifically, a number of service providers offer their professional customers and store keepers Electronic Payment Terminals (EPTs) enabling them to divert part of their turnover to undeclared foreign accounts.

Case study no. 8

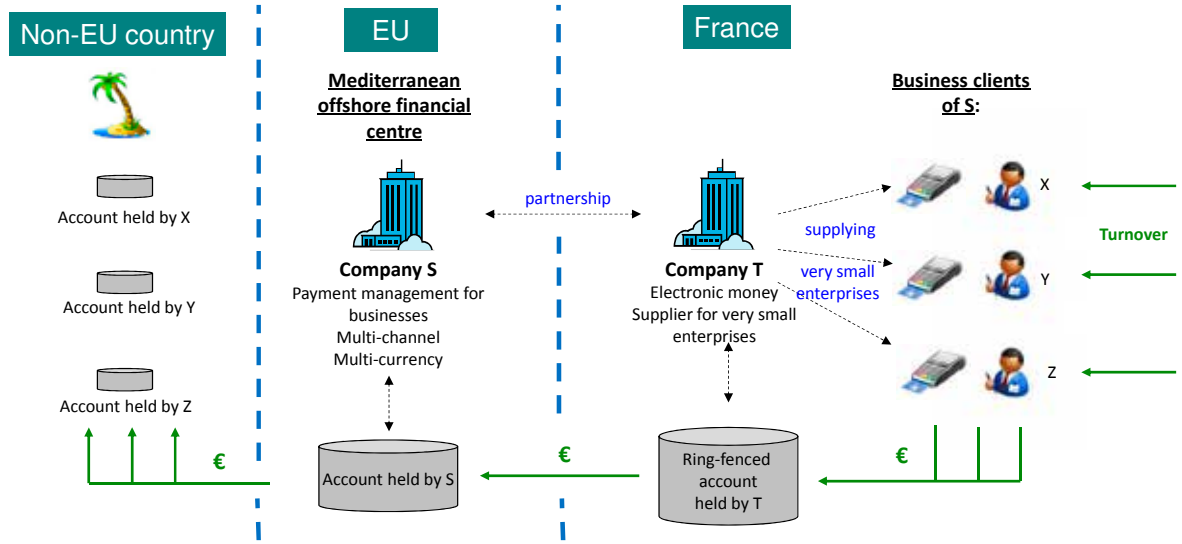
Company S was based in a Mediterranean offshore centre. It offered professionals and store keepers centralised management of their collections irrespective of the sales channel (physical, online, mobile telephone, etc.) and in a large number of currencies. Company S was accredited in its home country as a payment institution and operated throughout the EU under the freedom to provide services.

In France, it worked with a partner, Company T, which specialised in electronic payments and payment services. Company T was accredited in France as a payment institution. The two companies executed a service agreement for Company T to provide EPTs to Company S's customers.

The transactions carried out on Company T's EPTs were centralised on a French ring-fenced account in T's name. This enabled the record of the names of the store keepers benefiting from the transactions to be removed. The funds were then transferred to an account held by Company S in the country where it was accredited. Company S then redistributed the funds to foreign accounts opened for each store keeper customer. Each account had a foreign bank card attached to it thus enabling the store keeper to use it to fund his lifestyle.

Here again, various fraud and money laundering methods were superimposed and interconnected. Amongst Company S's customers, Tracfin was able to identify a number of companies involved in bank fund evasion schemes. Their profile was that of shell companies: under-declared income, failure to file returns, ongoing tax audits, discontinuation or closing of business activity whilst bank accounts are still active, bank credits unrelated to business activity, major transfers abroad, etc.

Companies S and T were accomplices to the fraud committed by their professional and store keeper customers, were guilty of handling stolen goods and laundering the proceeds of this fraud.



The criminal threat represented by large-scale and sophisticated fraud is based on networks that are:

– highly organised in their methods and constantly looking for loopholes in new legislation and regulations to allow them to innovate
– broad and flexible as regards structure: a single network may carry out a number of activities. The networks are superimposed and interconnected which creates synergy between the various frauds, including customs fraud, tax evasion and money laundering.

The networks may be partly coordinated by powerful cross-border criminal organisations. Law enforcement authorities experience difficulties in combating these networks owing to their lack of transparency, scope and flexibility. They use major investigative resources and wind up with complex legal cases whose boundaries are sometimes hard to determine.

CRIMINAL MONEY LAUNDERING STILL USES TRADITIONAL METHODS

Alongside networks involved in conspiracy to defraud, other criminal threats still rely on traditional money laundering methods. Every year, Tracfin handles cases originating from drug trafficking or illegal immigration.

Medium sized criminal networks still predominantly use cash: they use the services of money transfer companies and sectors handling large amounts of cash, such as the gambling sector.

DRUG TRAFFICKERS USE CASH AND ACCOUNTING FRAUD

Use of cash transfer services

In the downstream part of the drug trafficking logistics chain, the distribution networks handle huge amounts of cash. They use money transfer companies, which offer international cash transfer services, to send their earnings abroad. The majority of money transfer companies conduct heightened due diligence using transaction analysis instruments which detect inconsistencies either from senders or recipients.

Senders:

This may concern an individual who regularly sends cash to a number of recipients, all based in the same at-risk country.

Research into this individual reveals that the total amounts sent are far in excess of his known income.

Research into the recipients shows that they receive other transfers from other individuals with the same profile as the first sender (address, location, low known income, etc.).

Recipients:

This may concern a single recipient, based in an at-risk country, who receives, within a short time-span, large numbers of cash transfers representing significant amounts in total, from a number of senders all living the same geographical area.

Research into the newly-identified senders reveals that they send funds to a handful of recipients who all live in the same area of the same at-risk country.

Case study no. 9

A group of 65 people, mostly French nationals living in Brittany, sent around 150 cash transfers by money order from the city of Rennes to the capital of a South American country flagged up as being at-risk as regards drug trafficking with Europe. The transactions amounted to €361,000 over an eighteen-month period. When compared to the senders' socio-economic circumstances, these were large amounts and the fact that the transfers were fragmented demonstrates the intention of avoiding the due diligence measures implemented by the money transfer companies. The identified transfers enabled a link to be established between the majority of the senders, several of whom had been implicated in drug-related offences, on one hand, and a group of 49 recipients, on the other. Research led to the conclusion that the transfers could have originated from a conspiracy to smuggle drugs between South America and mainland France.

SME management and accounting fraud:

In SMEs, accounting fraud, tax evasion and misuse of company assets can be used to launder the proceeds of all crimes and offences.

Case study no. 10

A music production company was based in a sensitive district known as the scene of major drug trafficking. The company produced rap performers and presented rational operating accounts in its tax returns. Nevertheless, its bank movements showed that its operations bore no resemblance to the figures reported to the tax authorities.

Its revenue matched its business activity. It came principally from a music distributor that was a go-between for production companies and general public distribution networks, and the SACEM (French association of songwriters, composers and publishers). Conversely, the structure of its expenditure was inconsistent with the operating expenses that could be expected for this type of company. None of these expenses related to performers' compensation. Wages only amounted to €15,000 per year although the company had declared that it had three salaried employees. Payments to suppliers only accounted for €30,000 per year, the majority of which was paid to a company operating in a sector unrelated to music production. The company did however transfer around €500,000 per year to savings accounts, half of which represented investments in term deposits. The company also made payments of around €75,000 per year using

bank cards. These were recreational and leisure expenses for the manager and his relatives. There were also substantial cash withdrawals.

The manager's personal accounts showed abnormal movements and there were no living expenses. The company invested its revenue in life insurance policies and savings accounts. The manager's brother, who claimed to be a company employee, received cash transfers from third parties who/which had previously received payments from the company.

The insignificant amount of debits from the accounts of the company and its manager implied that they were using funds from outside the banking circuit to settle some of their expenses. During its investigations, Tracfin very rapidly established the fact that the manager's family was notorious for drug trafficking as well as being involved in settling scores using firearms. It is highly likely that the company's accounts were used to launder the proceeds of drug trafficking by introducing illicit funds into legitimate operations.

ILLEGAL IMMIGRATION NETWORKS USE CASH AND MONEY ORDERS

Tracfin has noticed a rise in the number of cases concerning suspected violations of immigration legislation and involvement in illegal immigration networks. These networks may be more or less structured. Whereas some are highly organised, others seem to be extremely fragmented, and may even represent individual initiatives.

Case study no. 11

Mr and Mrs X came from the Middle East but lived in France. Over a four-year period, they received a large number of cash transfers:

- Around €500,000 by means of 250 money orders from a single sender based close to a Middle Eastern war zone

- Almost €120,000 by means of 60 money orders, the majority of which were sent by individuals in countries bordering the war zone

There was no justification for these transfers which were inconsistent with Mr and Mrs X's lifestyle.

Moreover, Mr X cashed these money orders in a number of French cities, as well as abroad in Northern European cities. His bank movements attested to frequent travel, both to Europe's Mediterranean borders and to cities located in more Northern countries.

The judicial investigation revealed that these money order transfers between the Middle East and the Schengen Area were part of the setting up of an illegal immigration network.

Case study no. 12

Mr Y, who hailed from South Asia, lived on a housing estate in the north of the Greater Paris region. He was a salaried employee of a retail textile and clothing company that sold its products on markets. He had a criminal record for undeclared work-related offences. His wife, a French national, was a cleaner.

Over a one-year period, whilst Mr Y declared earned income of €14,000 to the tax authorities, he received credits of €200,000 on his bank accounts, including €120,000 in cheques and €60,000 in cash. Most of the cheques were written by SMEs in the construction sector. Mr Y also received transfers and cheques from individuals who were nationals of his home country.

In terms of expenditure, over the same period, Mr Y spent almost €30,000 with travel agents and airlines which was incommensurate with his declared income. The investigation found that all the airline tickets had been purchased for third parties. In addition, Mr Y made 25 cash transfers of around €1,000 each, half of which were to his home country.

The judicial investigation confirmed Mr Y's involvement in the offence of aiding and abetting illegal entry and stays in France.

VULNERABILITY OF THE GAMBLING AND GAME OF CHANCE SECTOR

The gambling and game of chance sector is still highly exposed to the risks of the laundering of illegally-acquired cash. All the sector's stakeholders are concerned.

Tracfin pays constant attention to horse racing and sports betting, and scratch card operators. Every year, the Unit receives and deals with cases of buying back winning tickets, repeated sports betting on competitions with low odds, which could involve the complicity of the retailers.

Casinos also remain vulnerable. In 2016, Tracfin handled cases involving large amounts, attributable in particular to Asian networks.

Case study no. 13

Mr Z claimed to be unemployed but had a personal business in the form of a second-hand car dealership. He had a criminal record for theft and handling stolen goods. The only payments into his bank accounts came from the CAF (Family Allowances Fund) and they were systematically withdrawn in cash. There were no living expenses. Following a tax audit, he was found to owe €140,000 to the tax authorities.

Over a two-year period, Mr Z won more than €610,000 by gambling at a number of casinos in France, both on slot machines and table games. Factoring in the redistribution rates for these forms of gambling in the long run, Mr Z would have had to have staked at least €670,000 over the two years in order to have won such an amount. However, Mr Z's bets recorded by the casinos only amounted to €14,000.

Mr Z only gambled cash and intentionally placed bets of less than the €2,000 limit to avoid having to provide details of his identity. This was made easier as cash can be fed directly into slot machines and electronic roulette games (so-called bill acceptors). The Unit's investigations were hampered by the lack of traceability of the bets.

An examination of his bank accounts showed that none of his cash winnings had been paid into them (at least in France). The fact that his bets and winnings were not debited or credited to his bank accounts implies the illicit origin of the cash, whether from undeclared (Mr Z owes €140,000 to the tax authorities) or criminal activities. Mr Z committed the offence of money laundering through gambling.

Tracfin also handled a number of cases involving members of the Asian community. They bet very large amounts of cash in casinos and made proportionate losses. The amounts were inconsistent with their declared income or the movements on their bank accounts.

Case study no. 14

Mrs W and Mrs H were both of Asian origin. Mrs W had French nationality. They visited the same gambling establishments and knew each other. The former wrote a number of small cheques made payable to the latter.

There were inconsistent movements on Mrs W's bank account. Although she and her husband only declared annual income of €15,000, her bank account was highly active. Over a two-year period, she received:

- €300,000 in cash deposits
- €50,000 in transfers from third parties
- €50,000 in cheques

There were the following debits over the same period:

- €175,000 in bank card payments in a number of casinos
- €130,000 in cash withdrawals (including €35,000 from cash machines inside casinos)
- €100,000 in written cheques

As for Mrs H, she did not declare any income and there were almost no movements on her bank account.

The inconsistent movements on their bank accounts went hand in hand with intensive gambling in casinos as they each paid almost 500 visits to various establishments over two years. The amounts passing through Mrs W's accounts cannot explain the sums gambled.

Over the two-year period, Mrs W lost a total of €280,000 on table games. She staked a total of €1.2 million, including €1 million in cash for substantial purchases of chips. In return, she received €920,000 in winnings.

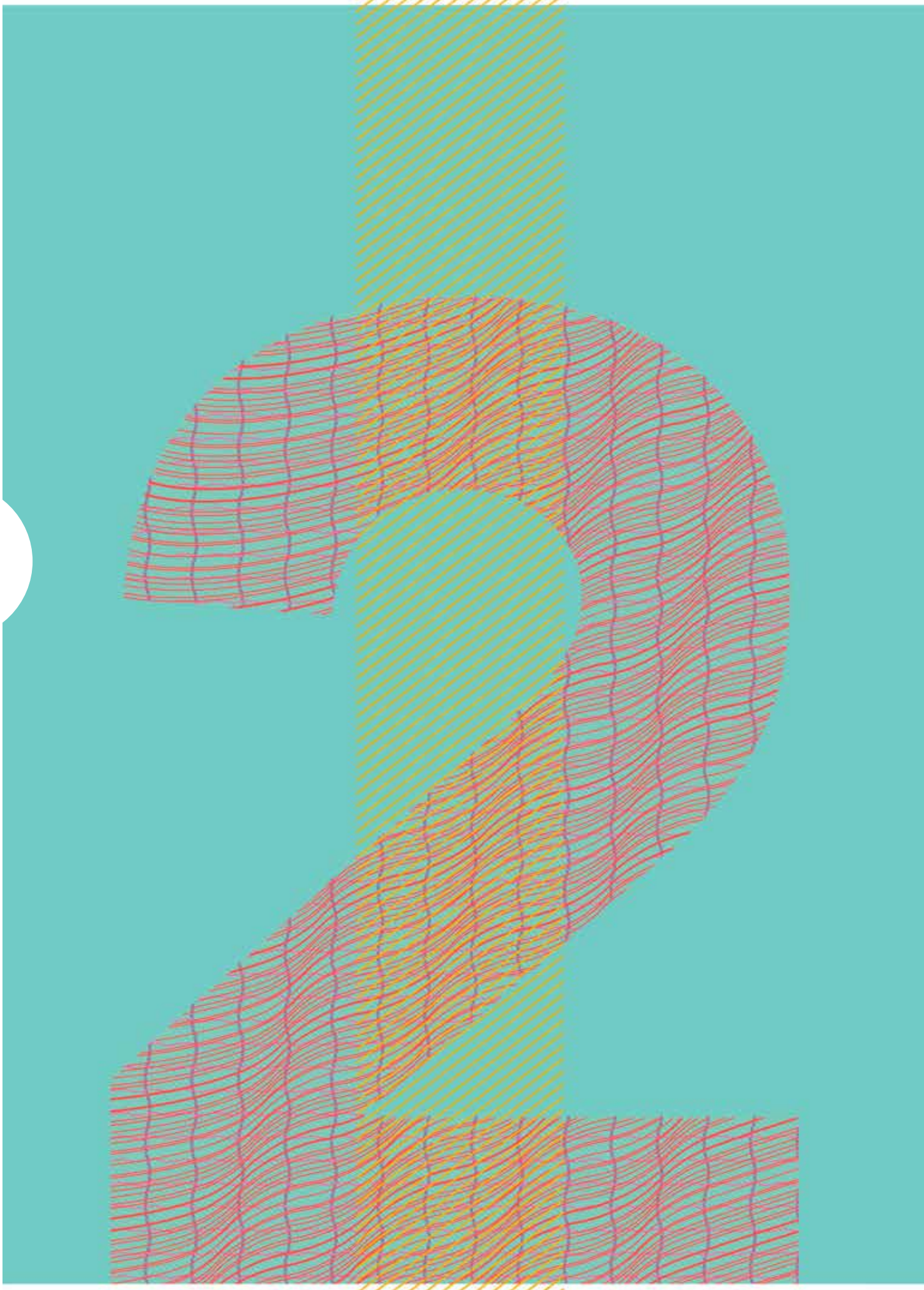
Over the same period, Mrs H made total losses of €1 million. She only gambled cash, exchanged €1.3 million for chips but only converted €3000 of chips into winnings. She also deposited and withdrew chips representing a total of €800,000.

There were a number of warning signs:

- Mrs W handling a large amount of cash, of unknown origin, that was discovered both through the workings of her bank accounts and her gambling in casinos
- The lack of movements on Mrs H's bank accounts and the fact that she had very few living expenses
- Intensive gambling in casinos although the two interested parties had no official revenue

- A lack of correlation between the debit transactions on their accounts and the transactions carried out in the casinos: in particular, no cash withdrawals matching the amount of losses.

The explanation for these cash movements by Mrs W and Mrs H is that these liquid assets did not actually belong to them. Their ultimate losses were logical if one is to suppose that they regularly handed out the chips in their possession to other gamblers who were accomplices. In light of the foregoing, the amounts handled could have originated from illegal actions that generated cash and the casinos were used as "undeclared" banks to launder the funds provided by the community and to return them to their owner.



COMBATING THE FINANCING OF TERRORISM: THE EFFORTS INVOLVE CENTRAL GOVERNMENT STAKEHOLDERS AT EVERY LEVEL

In 2016, effort to fight terrorism and its financing were considerably stepped up. Tracfin processed an ever-growing amount of information:

– 1,177 Suspicious Transaction Reports linked to terrorist financing were received and processed, a 47% increase over 2015.

– 396 investigations led to a referral note, which represented a 121% increase over 2015. These included:

- *352 notes that were sent to the various intelligence services*
- *44 notes that were sent to the courts or to the criminal investigation departments tasked with fighting terrorism*

*Notes concerning terrorist financing that resulted from Tracfin's investigations were sent to the intelligence services, the police and the courts of first Instance (*tribunaux de grande instance*). With respect to the courts, Tracfin works in close collaboration with the anti-terror division of the Paris Public Prosecutor's Office, which is the primary recipient of the Unit's investigations.*

The information passed onto the courts in 2016 is a reflection of the primary terrorist financing patterns observed by the Unit:

- *Detecting weak signals of radicalisation and the imminent departure of combatants*
- *The issue of combatants returning from war zones*
- *The financing of terrorism via networks of money collectors*
- *Terrorist financing via non-profit organisations*

In addition to profiling individuals with links to those responsible for terrorist attacks – both successful and attempted – that have taken place in France and across Europe since 2015, Tracfin's disclosures to the courts are mainly concerned with 1) money collectors who act as intermediaries between sources of funding and combatants on the ground, by concentrating and subsequently redistributing transfers of cash abroad; and 2) financing via non-profit cultural and religious organisations.

These terrorist threats use a variety of financial channels. In addition to standard bank flows, over which Tracfin has significant visibility, terrorist financing involves other forms of products and participants. Prepaid cards – the regulatory framework for which was adjusted by lawmakers in the wake of the 2015 attacks – are used to transfer funds to networks of money collectors. These collectors mainly use wire transfer companies to send and receive funds in cash. Similarly, radicalised movements have benefited from the growth in and widening acceptance of crowdfunding platforms. The creation of money collection websites to collect money for non-existent projects have resulted in donations that are ultimately used to support terrorist networks both materially and financially.

COMBATANTS AND/OR THE DETECTION OF WEAK SIGNALS OF RADICALISATION

In the fight against terrorism, financial intelligence focuses on detecting weak signals. The preparation of terrorist attacks involves the use of micro-payments that are hard to trace. Within the volumes of legitimate micro-transactions, flows that are characteristic of a shift towards terrorism rarely stand out.

Strictly financial elements must be crossed with behavioural criteria. Emphasis is placed on the details of small transactions involving individuals showing signs of radicalisation or an imminent departure for a war zone.

To best meet this challenge, Tracfin has diversified the ways in which it transmits referral notes to the competent authorities. In addition to court referrals, the Unit has developed so-called "flash" referrals to quickly and accurately respond to emergencies and the occasional needs of our partner intelligence services and the police. Flash referrals deal with specific financial transactions and individuals. The Unit has issued 80 flash referrals since they were introduced in 2016, or nearly 20% of total CFT-related referrals during the year. This figure is expected to rise significantly in 2017.

Case study no. 15: Detecting a departure for jihad

A reporting entity notified the Unit about the desire of an individual, who was born in 1995, to give one of his parents power of attorney over his bank account prior to closing it. The individual stated that he was going abroad for personal reasons and for an indeterminate period of time. When he was closing out the account, the parent said that the individual would not be returning to France. An analysis of the individual's account revealed a large number of expenses for camping and outdoor supplies prior to the closing of the savings and checking accounts.

Warning signs:

- Abrupt closing of all of an individual's bank accounts
- Departure for a unknown destination for an indeterminate period of time
- Purchase of camping supplies
- Unclear explanations as to the reasons for the trip and the final destination
- Age of the individual

Case study no. 16: Detecting a radicalisation process

A reporting entity notified the Unit about recent changes in the behaviour of a customer who wanted to leave France and move to a North African country where he had no roots. The individual, a salaried worker, had received a large sum of money from his company after terminating a permanent contract by mutual agreement. He had recently converted religiously, changed his appearance and refused to have any contact with the reporting entity's female employees. He also made wire transfers to a non-profit religious organisation, and requested information about how to transfer money abroad.

Tracfin's was quickly able to establish that the individual's name was marked with an "S" in the Wanted Persons File.

Warning signs:

- Rapid and/or ostentatious religious conversion
- A change in the individual's physical appearance
- A plan to travel to a North African country

Case study no. 17: Detecting suspicious bank transfers to radicalised individuals

Tracfin was informed that an individual had deposited €15,000 into a bank account without stating the origin of the funds. The following day, he made a bank transfer for same amount to a person in Belgium who had been accused of murder in connection with terrorist acts. The Belgian person had provided logistical support to someone who had carried out a terrorist attack; he has been in provisional detention since his extradition to France.

Warning signs:

- Large deposits of cash
- Bank transfers to a person in detention
- Links to individuals known in public records for belonging to a terrorist movement

THE ISSUE OF RETURNEES

It costs several thousand euros to bring someone back from a war zone. As a result, the family and friends of an individual wanting to return to France must raise the money.

Tracfin collects intelligence on questionable transactions in the accounts of those close to individuals who are active in war zones. These transactions can take several forms. Most often they are cash withdrawals of the proceeds of the sale or a car or house, or the cancellation of a life insurance policy. Reporting entities pay heightened attention to the family and friends of individuals who have already been the subject of an information request based on the suspicion that they have left for a war zone.

The number of returnees is relatively low; for this reason, Tracfin has noted very few cases of financing the return to France of jihadists. Nevertheless, Tracfin has investigated the gathering of funds to bring combatants home using money collection websites. A link to the call for donations on the website is spread using social media. By exercising its right to information vis-à-vis the host of the website, Tracfin was able to learn the identity of the person who had set up the request and identify the donors.

INTERNATIONAL NETWORKS OF MONEY COLLECTORS

Areas conquered by Isis provide the organisation with its primary source of funding, via war booty, extorting local populations, exploiting natural resources, taxing trade flows and trafficking. Now that Isis is suffering military losses, the territory it controls is shrinking and its financial resources are dwindling. The movement is attempting to partially offset these losses in revenue through increased reliance on outside funding. These international financial flows can help reveal the movement's possible geographic redeployments.

THE ROLE AND THE ORGANISATION OF NETWORKS OF COLLECTORS

The primary architects of the foreign financial flows gathered on behalf of Isis are called collectors. They are financial go-betweens who offer a variety of services, including:

– Holding the money of foreign combatants travelling to and from war zones in order to reduce the risks involved in crossing borders with sums in cash
– Safeguarding the amount owed to a smuggler by a combatant, by paying the money once the border has been crossed
– Receiving money on behalf of a beneficiary who does not have a valid ID or for whom the risk of revealing him- or herself would be too great
– Bringing money directly to a war zone for the benefit of a combatant
– Sending money to a war zone using a hawala-type compensation system

To organise the transfer of the funds, French members of Isis use mobile apps to send their friends and relatives in Europe the name of the collector and the means to transfer the money (commissions, money transfer companies, etc.). Money gathered from a combatant's entourage is used to defray daily expenses on the ground.

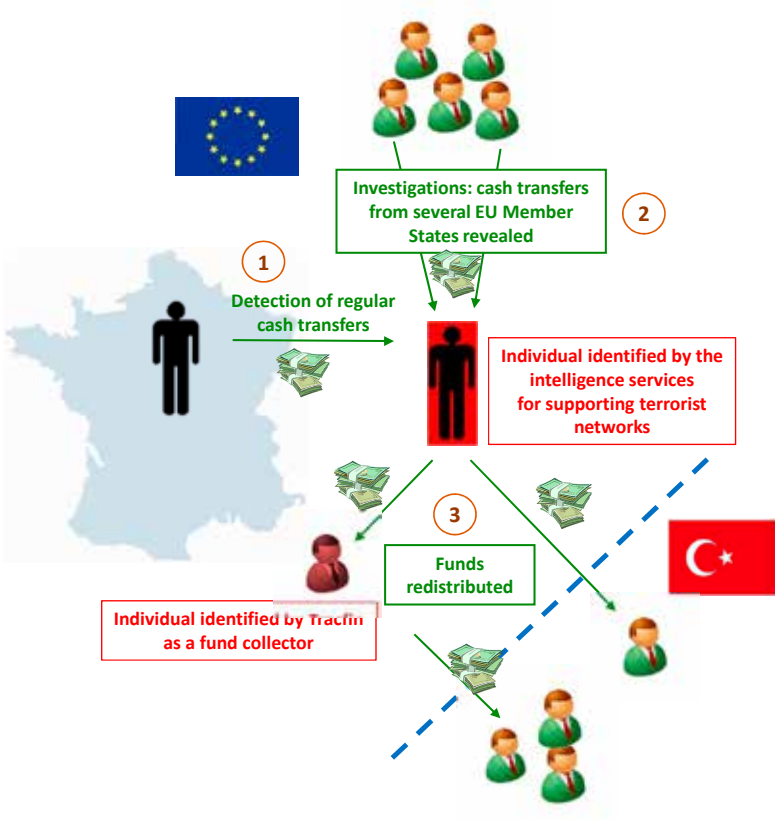
In 2016, Tracfin launched a large-scale investigation, and analysed several thousand cash transfer transactions in a bid to uncover the networks of collectors. The data analysed – the result of information requests by Tracfin to the primary money transfer firms – showed similar modus operandi for transferring money to

collectors. These shared characteristics have allowed the Unit to identify a typology:

– Those sending funds gather the money using several micro-financing sources
– In most cases, they then send the money in one single shipment (or very few). Most often, the transfers are made to countries bordering war zones in the Middle East.
– The collectors thus receive a number of transfers from a variety of individuals with no connection or motivation between them and from a number of countries, mostly European.
– The final destination of the money is Middle Eastern countries in which there are war zones.

Case study no. 18: Discovery of a network of money collectors

Tracfin was alerted to a series of cash transfers between individuals living in two separate EU countries. One of them was known to the intelligence services for his involvement in networks sending combatants to Syria and for providing logistical support for Isis. An analysis of this individual's financial transactions revealed that he was the beneficiary of a number of cash transfers from a number of European countries, which he then redistributed to third parties, some of whom were living in Turkey. Another one of these third parties, a resident of an EU country, was already known to the Unit for his role as a collector of funds being sent to Turkey.

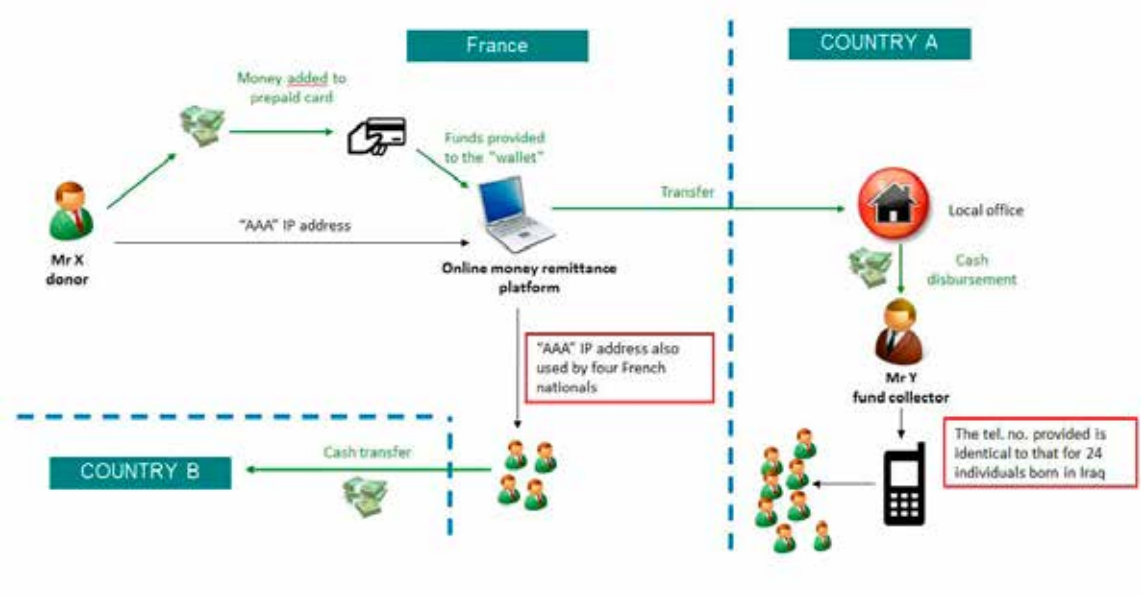


Case study no. 19: Prepaid cards used to channel money to a network of money collectors

Mr X purchased a prepaid card, which he reloaded by cash on three occasions. Using the number of the prepaid card, he made an online money transfer to Mr Y located in conflict zone, who withdrew the funds from a local office. The telephone number that Mr Y gave when withdrawing the money was the same one used by 24 other individuals, all of them born in the country A, located in conflict zone.

Furthermore, the IP address that Mr X used to make the online transaction had also been used by four other individuals to make money transfers to beneficiaries in the country B, bordering a conflict zone.

The multiple identities connected to a single telephone number in country A and to a single IP address in France is likely an indication of the use of false identities for the purposes of discretion. Prepaid cards are particularly susceptible to being used for identity fraud.



Case study no. 20: M's network

At the end of 2015, the anti-terror division of the Paris Public Prosecutor's Office opened a preliminary investigation based on information received from Tracfin. It concerned the activities of Mr M, a money collector for Isis, who was charged with:

- Conspiracy to commit a terrorist act (Article 421-2-1 of the Criminal Code)
- Terrorist financing (Article 421-2-2 of the Criminal Code)

Mr M collected money from a number of European countries via money transfer companies and then turned the funds over to Isis jihadis.

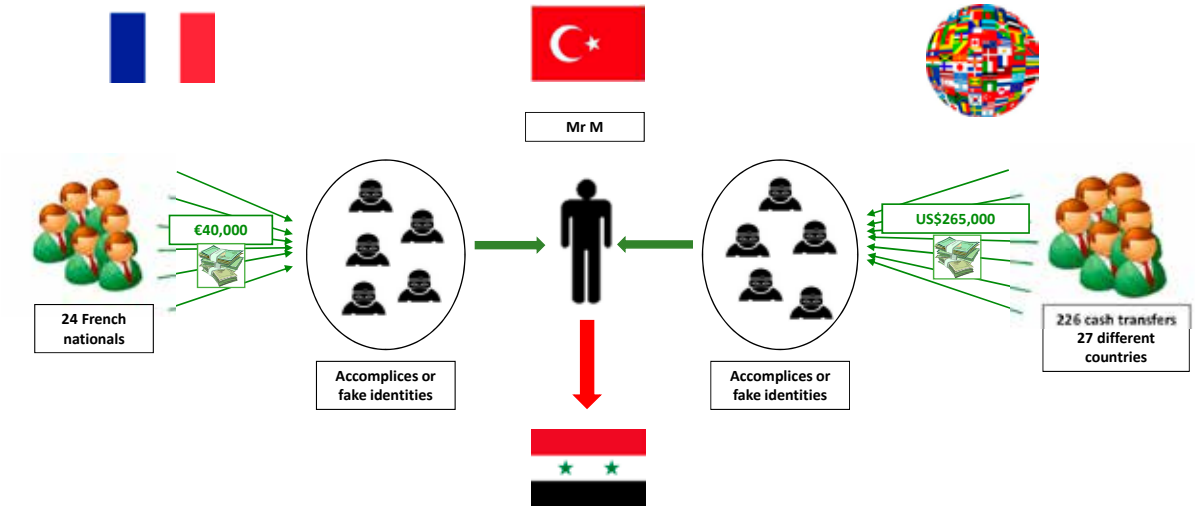
Between May 2014 and August 2015, 24 French citizens sent a total of 40,300 dollars.

Mr M developed his network with the help of a number of accomplices and through the use of false identities. His impact, which was significant throughout the European networks, was a decisive factor in a number of intelligence services taking action with respect to collectors.

Mr M's activities as a jihadi go-between were confirmed by the testimony of those sending funds and by the seizure of computer equipment. The transfers were made by Mr M or his associates, who travelled between Turkey and Syria on a regular basis, taking a 4% commission on each transaction.

Outside of France, Tracfin noted the existence of 226 transfers from 27 different countries for a total amount of 265,000 dollars, which netted Mr M some 11,000 dollars in a year's time.

Mr M is now on the sanctions list of the Office of Foreign Assets Control (OFAC), and his case was the impetus for several European initiatives, which were helped along by the involvement of Interpol.



DETECTING NETWORKS OF MONEY COLLECTORS HAS BOLSTERED A CROSS-CUTTING SPIRIT OF COOPERATION

Efforts to map money collector networks are the fruit of effective inter-departmental collaboration and improved cooperation with private-sector stakeholders.

Institutional partnerships

Within the intelligence community:

Through monitoring networks of collectors and detecting French citizens sending funds, Tracfin has played a role in understanding terrorist threats, which has benefited France's intelligence community. The Unit contributed to an inter-departmental working group that pooled intelligence within the Directorate General for Domestic Security (DGSI).

With the courts:

New ways to collaborate have strengthened the partnership between Tracfin and the courts. In 2016, in an effort to facilitate investigations by the public prosecutor office into ongoing cases, Tracfin introduced standardised information reports.

h Tracfin's international counterparts:

At international level, approaches to this type of micro-financing are still quite heterogeneous within FIUs. France and Belgium have developed an exchange policy in this area. Concurrently, Tracfin relies on the network of FIUs to relay sensitive information to its partners.

Reporting entities

Specific partnerships were launched during 2016 so that our private partners could respond quickly and accurately to Tracfin's requests. The major stakeholders in Paris's financial centre have benefited, sometimes in conjunction with our institutional partners, from an assessment of specific threats to the initiative underway.

In addition to Tracfin's right of information, these entities have been able, through their STRs, to raise new suspicions. New financial routes were thus identified.

NON-PROFIT ORGANISATIONS SUSPECTED OF TERRORIST FINANCING

Tracfin's analysis of STRs concerning terrorist financing has spotlighted certain non-profit organisations as points of convergence for financial flows intended to finance jihadist networks. Based on information received by the Unit, three types of organisations are involved:

– **Humanitarian organisations:** they provide food, medicine and equipment in deprived areas and war zones. Officially, their actions consist of sending individuals (doctors, nurses, humanitarian workers), goods and money abroad.
– **Cultural organisations:** their actions are varied. They involve purchasing books, organising conferences or setting up language courses and support for schoolchildren.
– **Religious organisations:** their stated aim is the management and construction of places of worship.

The organisations suspected of involvement in terrorist financing are mainly located in the Greater Paris region, but they are also in the Provence-Alpes-Côte d'Azur and Rhône-Alpes regions, as well as from the east of France. Financing primarily comes from donations provided by individuals from the community that is the focus of the organisation's efforts. With respect to regional-level organisations, the individuals are generally from the local population.

Financing from abroad is occasionally noted in connection with the accounts of non-profit organisations that manage places of worship known for being home to radical elements.

Some organisations receive public financing in the form of subsidies granted in connection with their official activities.

Examination of the bank accounts of these types of organisations reveal a lack of transparency in how the funds are used, particularly with respect to humanitarian organisations carrying out missions abroad. The accounts are used to compensate individuals and legal entities located abroad without it being possible to establish a link with the humanitarian action in question. Similarly, arguing that there is no reliable banking system in a given area, organisations will withdraw large amounts of cash: tens of thousands of euros or even more.

Organisations will use several methods to conceal the financial circuits they employ:

– The use of payment platforms located abroad
– Interconnecting financial flows between organisations in France and abroad
– Practices involving breach of trust

Case study no. 21: Financing of a place of assembly via an organisation frequented by radicalised individuals

A property investment company managed by Mr A sought and was granted a loan for a real estate purchase. The balance of the transaction was not settled by the investment company, but rather by Organisation B, which is active in educational, social and cultural projects with young people who are part of a specific community. Organisation B's resources are primarily derived from membership fees, donations and public subsidies. However, certain members of non-profit organisation B are known to the intelligence services for their involvement in radical movements. Prior to the real estate purchase, the bank accounts of Organisation B were credited with several hundred thousand euros in the form of bank transfers, cheque deposits and cash deposits, most of which came from its members. Bank transfers also came from Mr A through the intermediary of a third non-profit organisation and a commercial firm. The purchased property could be used as a place of assembly for radical groups.

Case study no. 22: Logistical and financial support for Isis under the guise of humanitarian assistance provided by a money collection website

A non-profit organisation F, chaired by Mr X, had a stated goal of providing humanitarian assistance and development aid in developing countries. Mr X and his board, all from a Slavic country, were suspected of being supporters of a Salafist movement that advocated the reestablishment of the Caliphate. Under the guise of humanitarian assistance, Organisation F would provide financial and material support for Isis in the Middle East. It collected funds via a money collection website that was linked to a bank account that had been opened in Mr X's country of origin. The money collected came from that country, and was withdrawn only in cash.

THE FIGHT AGAINST CORRUPTION, TAX EVASION AND SOCIAL SECURITY FRAUD RAISES HIGH EXPECTATIONS

Combating corruption, tax evasion and social security fraud is one of Tracfin's long-term priorities. In the current context, both domestic and international, this combat elicits high expectations:

- *In terms of corruption, in light of the distressed state of certain countries that have been the victims to predatory practices, media coverage of high-profile events and the work of the OECD, which is preparing to celebrate the twentieth anniversary of the signing of the Anti-Bribery Convention in 1997.*
- *In terms of tax evasion, given the need to achieve fiscal consolidation and to combat large-scale transnational tax evasion, particularly with the introduction in 2017 of automatic information exchange between tax authorities.*
- *In terms of social security fraud, in order to maintain the financial equilibrium of France's social security bodies, and hence their long-term sustainability.*

ANTI-CORRUPTION EFFORTS: INTERNATIONAL CASES SHOULD NOT OVERSHADOW SPECIFIC RISKS TO FRANCE

Combating breaches of probity is driven by an international context that focuses on bribery in foreign business transactions:

- The OECD's dedicated working group – which was set up in the wake of the 1997 Convention and which is tasked with monitoring signatory countries' anti-corruption systems – focuses on bribery in international business transactions (primarily active and passive bribery and influence peddling).
- In France, Act 2016-1691 of 9 December 2016 (known as Sapin 2) was partly created for reasons relating to international trade. It was promulgated to provide France with an anti-corruption mechanism comparable to those of other Western European countries, so that those with the most extensive legislation can no longer use the weakness of French legislation as a pretext for prosecuting French companies.

And yet, France is also vulnerable to domestic breaches of probity committed by persons exercising a public function: elected officials[1], individuals in charge of public authority and those entrusted with a public service mandate. In addition to the offences of corruption and influence peddling, these breaches include favouritism, unlawful taking of interest and misuse of public money.

Tracfin, which processes some fifty cases each year, is taking concerted action in both directions, both internationally and domestically.

ACT NO. 2016-1691 OF 9 DECEMBER 2016 (THE SAPIN 2 ACT)

The Sapin 2 Act introduced several innovations, including:

- Creation of the offence of active and passive influence peddling with respect to a public official in a foreign State
- Expansion of the territorial and extra-territorial effect of French criminal law
- Exemption from criminal liability for whistleblowers
- Sanctions for those failing to comply with the compliance programme (para-criminal penalties imposed by a dedicated agency: the French Anti-Corruption Agency).
- Judicial agreement in the public interest

It creates an anti-corruption compliance obligation that is territorial and extraterritorial in scope, in line with the expansion of the territorial and extra-territorial effect of French criminal law. The Act allows for the sanctioning of an offence committed under criminal law and which is the jurisdiction of the French criminal courts, irrespective of whether the offence is committed entirely or partly in France, or entirely outside the territory. This makes prosecution of foreign companies easier.

1 The Fourth Anti-Money Laundering Directive, which was enacted into French law by Order 2016-1635 of 1 December 2016 extends the concept of Politically Exposed Person (PEP), which had heretofore only applied to foreign individuals, to include French PEPs.

The Sapin 2 Act calls on companies to set up systems to combat corruption (Anti-Corruption Compliance Obligations – OCA) and created the French Anti-Corruption Agency (AFA), which is tasked with ensuring that these systems are properly applied. Companies affected by OCAs are companies or groups that have their registered offices in France, and that meeting at least one of two criteria: they must have more than 500 employees and/or a turnover of over €100 million[1].

The anti-corruption obligations impose eight measures on the companies concerned (Article 17 of Act 2016-1691):

- A code of conduct integrated into the company's in-house procedures
- A dedicated internal alert system, since the Act creates a status for whistleblowers
- Corruption risk mapping in the form of formal, up-to-date documentation for the purpose of identifying, analysing and prioritising risks
- Procedures for assessing customers, leading suppliers and intermediaries within the scope of risk-mapping efforts
- Internal and/or external accounting control procedures
- A training system for staff, particularly managers
- A disciplinary system to sanction employees who violate the company's code of conduct
- An internal monitoring and evaluation system for the measures implemented

1 These two criteria should be clarified, both in terms of how employees are counted and in the definition of what constitutes turnover. In addition, corruption is not confined to large companies. Small companies are also involved, either acting autonomously or as shells for larger firms.

INTERNATIONAL PUBLIC AND PRIVATE CORRUPTION

Corruption of a Foreign Public Official (APE)

The offences related to corruption of foreign public officials are defined in Articles 435-1 to 435-4 of the Criminal Code. They stem from the Act of 30 June 2000, which entered into force on 29 September 2000, which enacts the main provisions of the OECD Convention into French law. They were clarified by Act No. 2013-1117 of 6 December 2013 and Act No. 2016-1691 of 9 December 2016.

Using bank account records, correspondent banking-related activities, audits and account certification, reporting entities pass on substantiated STRs to Tracfin. These help the Unit become an excellent resource for detecting these infringements.

Case study no. 23

A French SME manufacturer sought to sell sensitive equipment to a public-sector customer in West Africa. The company transferred €2 million to the country, into the bank accounts of unidentified legal entities who did not appear on the company's books as suppliers.

The transaction set off warning bells:

- The total amount transferred (€2 million) was extremely high compared with the French company's total turnover of €5 million.
- None of the transfers exceeded €150,000, past which the signing authority with respect to the company's bank accounts would revert to the CEO.
- The recipients of the funds did not appear in the African country's databases of commercial firms. They were not listed in the exporting French company's accounts payable.
- The transactions were booked over a year's time and appeared unusually complex, assigning the amounts to different accounts in the chart of accounts that are normally not used for these types of transactions.

The French company's explanations were not very convincing. It explained that the fund transfers were in connection with the sale of communication equipment. The agreements that the company produced had not been implemented and appeared to be fakes. There was no trace of them, either in the company's customs declarations or in its banking transactions. The investigation concluded that these payments were used to compensate intermediaries.

Use of a subcontractor by a large firm

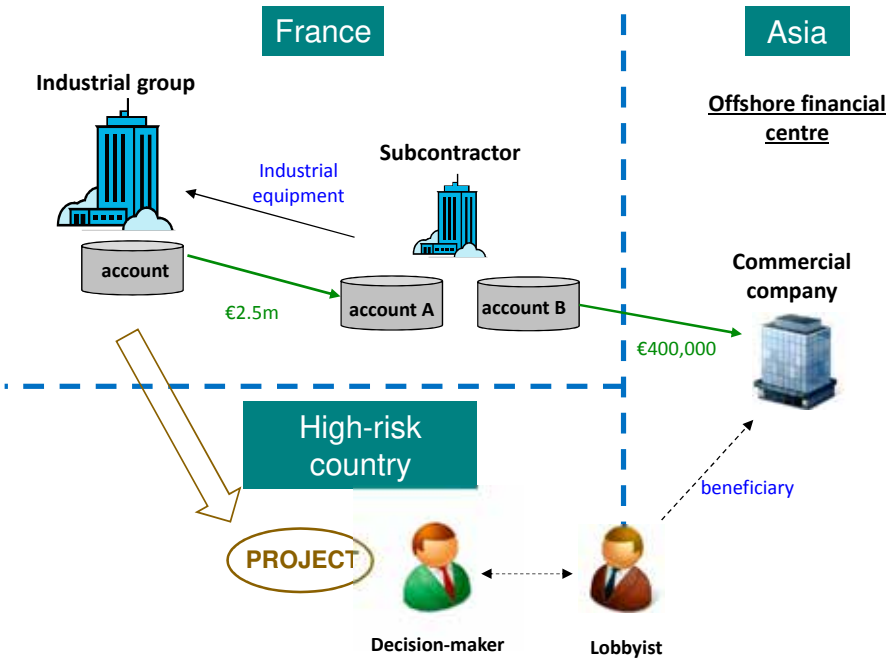
Large companies that are subject to commercial restrictions in certain high-risk countries may seek to outsource bribery transactions to lower-profile subcontractors, over which they have de facto control.

Case study no. 24

A French manufacturing firm was setting up a project in a country that presented a risk in terms of corruption. The company turned to a subcontractor that specialised in manufacturing certain parts. The subcontractor invoiced €2.5 million for its service, which seemed overpriced. The subcontractor then paid 17% of the invoiced amount (€425,000) into the account of a commercial firm located in an Asian tax haven. This company was managed by a national of the country in which the project was located.

Warning signs:

- Discrepancies in the financial circuit through the use of an Asian company for a transaction unrelated to Asia.
- The parts manufacturer used one set of bank accounts to receive the money from the French company and another to transfer a portion of it to the Asian tax haven.
- The 17% paid over to an Asian company represented a higher-than-average commercial margin for this sector. This led to a suspicion of over-invoicing.
- The profile of the manager of the Asian company that received the money was that of a lobbyist involved in a variety of sectors, rather than a technical specialist capable of supplying an industrial service for the project in question.



BREACHES OF PROBITY BY INDIVIDUALS EXERCISING A PUBLIC SERVICE MANDATE

Even more than for corruption abroad, Tracfin's informants have helped make the Unit an effective means for combating breaches of probity on French territory by individuals exercising a public service mandate. Tracfin has investigated many cases of corruption, influence peddling, unlawful taking of interest, favouritism and embezzlement, as well as breach of trust. A great many cases involve non-profit organisations, big and small, financed in whole or in part by public money. The legal framework governing these organisations is particularly flexible under French law, and thus represents a significant area of risk in the AML/CFT system.

Unlawful taking of interest by an elected official

Case study no. 25

The deputy mayor of a mid-sized city was in charge of social action and the elderly. At a time the city was developing a project to build a retirement home, this official was, over a three-month period, the recipient of €1 million that had been wired into the account of a consulting firm, as well as €600,000 transferred to a real estate company in which he was a shareholder.

The money had been paid by a property developer and manager of a retirement home, partly by using a property holding company as an intermediary, and partly directly to the real estate company.

To justify these sums, the official produced invoices for assistance and consulting services he had provided, including the search for a building plot, the bringing together of the developer and the owners, assistance with the project design and the creation of the various permit applications.

Warning signs:

- Duties as deputy mayor
- Setting up of two simplified limited companies (SASs) and management of their bank accounts. The swift arrival of these large bank transfers, justified by finder's fee agreements, is almost the only activity in the accounts
- Links between the deputy mayor and one of the partners in the intermediary property holding company that had transferred funds to the consulting firm.
- The official had used part of the money to purchase a life insurance policy and to make a private real estate purchase.

Breach of trust, by elected officials or individuals exercising a public service mandate to the detriment of non-profit organisations financed by public subsidy

Case study no. 26

Mr X was a local official in a small seaside municipality. His wife headed up a non-profit organisation that promotes the town's port fair. Mr X chaired the organising committee of a large annual carnival that is held in a mid-sized community in the region. The couple also chaired several other non-profits, such as one that provides support for retired carnival workers.

The primary customers of the fairs organised by Mr and Ms X were the social welfare committees (COS) in the region's various municipalities, along with a few works committees. These committees would purchase blocks of tickets for rides and attractions and then distribute them to their beneficiaries (staff in the various municipalities, employees and residents).

Apparently, a portion of the profits from these lucrative ticket sales were diverted to the bank accounts of the non-profit organisations run by the couple, and even directly to their personal bank accounts or those of a property holding company they ran. These various bank accounts were associated with a number of suspicious transactions, particularly cash deposits.

Over a three-year period, two non-profit organisations run by the couple were credited with a series of payments totalling €290,000, mostly from the COS and the works committees, that were completely unrelated to these associations' purposes. Part of the money was redistributed into the couple's personal bank accounts or those of family and friends.

Across all of these accounts, Tracfin found a total of €240,000 in unjustified cash deposits, €160,000 of which were deposited directly into the couple's personal accounts. The remainder was deposited into accounts belonging to family, friends and non-profit organisations. Mr and Ms X led a lifestyle that was much more luxurious than what their declared income would have permitted. Their bank accounts showed evidence of leisure travel and the purchase of high-end cars.

Case study no. 27

Mr Y was a local government manager for a large French city, and as such managed the city's social services, including the municipal social service centre (CCAS). At the same time, he managed two non-profit organisations that helped people enter the job market, both fully financed by the CCAS. He was also a partner in a food distribution company, along with Mr Z. Mr Z's name was listed in the organisation charts for three other non-profits offering job-seeking support and vocational training. Mr Y had power of attorney over the bank accounts of all three.

In two years' time, the various non-profit organisations run by Mr Y and Mr Z received nearly €260,000 in public money, primarily via agreements signed with the city's CCAS.

However, the use of these funds was inconsistent with the organisations' aims, since most of them were withdrawn in cash, through PayPal withdrawals and even in the form of cheques made out to Mr Y.

Case study no. 28

A non-profit organisation helping job-seekers offered accommodation for people in difficulty in three hostels. Over three years, it received €4 million in public support, primarily from the Regional Council. During the same period, however, there were a number of anomalies in the organisation's accounts:

- €470,000 in cash withdrawals, with no apparent destination for the money
- €225,000 wired to a property holding company (SCI) owned by the organisation's chair and treasurer, of which €120,000 was sent from the SCI's account to the personal account of the chair's parents
- Numerous transfers and cheques issued by the non-profit organisation for the benefit of other such organisations, which were active in fields of vocational training or the management of holiday centres, and whose organisation charts included the chair, the treasurer or their relatives.

COMBATING TAX EVASION – TRACFIN HONES ITS TECHNICAL SKILLS AND GATHERS DECISIVE INTELLIGENCE FOR THE TAX AUTHORITIES

In 2016, Tracfin sent 350 information notes to the tax authorities (DGFiP). Eighty-five percent of them had to do with individuals' private assets (under-declaration concerning the wealth tax, inheritance taxes or stamp duty), or cases involving undocumented flows between a legal entity and its director. The remaining 15% involved tax offences by legal entities, primarily in the area of VAT fraud[1].

STRs relating to individuals cover a wide range of fraudulent activities. The most frequent topics include the possession of bank accounts in countries bordering France or in tax havens, undeclared professional activities, the fraudulent organisation of insolvency and abuse of rights (exemption from capital gains tax, disguised donations, etc.).

The average sums involved are trending upward: from €1.33 million in 2015 to €1.41 million in 2016. Tracfin focused on high-value cases, often with international dimensions that meant additional processing time.

Nevertheless, to make better use of STRs involving smaller amounts, in Q2 2017 Tracfin launched "flash" reports – a stepped-up method for processing simple cases being passed on to the tax authorities.

UNDECLARED FOREIGN ASSETS

Thanks to international cooperative efforts between FIUs, Tracfin has the ability to identify undeclared foreign accounts, which is particularly of interest to the tax authorities. Beginning in 2017, the tax administration benefited from the introduction of automatic tax information exchanges between all OECD countries[2].

Trusts and the applicable tax rules

The 2011 Supplementary Budget Act no. 2011-900 of 29 July 2011 introduced into French law a specific tax regime for trusts held abroad. According to information received by Tracfin, certain settlors or beneficial owners of trusts are still attempting to circumvent or only partially apply these provisions.

Case study no. 29

Mr. Y was a resident of France for tax purposes from 2002 to 2014. During this period, he did not report any assets or income from foreign assets, and he only reported a small amount of assets liable for the wealth tax. He and his wife have two children, who remained French tax residents after 2014.

Intelligence gathered by Tracfin revealed that Mr Y was in possession of:

- A trust domiciled in the Channel Islands, of which he and his children were the beneficial owners, with assets of €35 million. Each year, this trust paid out hundreds of thousand euros to the members of the family who were beneficial owners.
- A number of overseas bank accounts (North America, the EU, the Channel Islands)
- Shortly before changing his tax residence, Mr Y and his wife sold the shares they held in a French company, for a total of €100 million. They placed the proceeds in bank accounts opened in several EU countries.

This being said, Mr Y was in breach of several tax provisions.

- Overseas bank accounts:

Under the provisions of Article 1649 A of the General Tax Code (CGI), any accounts, whether opened, in use or closed, must be declared at the time of filing income tax returns. Failure to do so will result in a tax fine and the taxation of the sums in question.

- Failure to declare investment income:

Under the provisions of paragraph 9 of Article 120 of the General Tax Code, income distributed by a trust as defined in Article 792-0 bis, regardless of the type of assets or interests placed in the trust, are considered taxable income.

1 In addition, tax offences are also evoked in most of the disclosures sent to public prosecutors' offices. These are tangential to other, primary offences, such as undeclared work, fraud, misuse of company assets and breaches of probity.

2 The Common Reporting Standard (CRS), developed in response to the G20 request and approved by the OECD Council on 15 July 2014.

Moreover, Article 123bis of the General Tax Code stipulates that when a French tax resident owns at least 10% of a trust or equivalent established abroad, and when the assets of this legal entity consist of current accounts or securities, the profits generated by this legal entity shall, with regard to the tax resident in question, constitute investment income[1].

- Filing amended trust returns:

Mr Y left France at the end of 2014. In 2015, he filed forms 2181-TRUST1 (constitution of a trust) and 2181-TRUST2 (inventory of the net value of a trust's assets) for the years 2012 to 2014. He stated that the trust would cease to have any connection with France at the end of 2014, and therefore did not make any filings for 2015. Mr Y's children issued statements of temporary waivers at the end of 2014.

Article 1649 AB of the French General Tax Code provides that the administrator of a trust whose settlor or at least one of the beneficial owners is domiciled in France for tax purposes, or which includes assets or interests situated in France, must declare any constitution, amendment or termination of the trust as well as the content of its terms.

Mr. Y has been a non-resident since the end of 2014. However, his two children, who are beneficial owners of the trust, are still French tax residents. Thus, issuing a temporary waiver with respect to the trust could be intended to obtain an exemption from this reporting obligation. The temporary waiver is for tax purpose only.

- Lowering the wealth tax:

Since 2012, under the provisions of Article 885 G ter of the French General Tax Code, assets placed in a trust, including capitalised income, are considered part of the settlor's taxable wealth.

- Failure to file an exit tax return:

Article 167 bis of the French General Tax Code provides, *inter alia*, that the transfer of tax domicile outside France shall entail immediate taxation of income and of social contributions on unrealised capital gains on securities, subject to the extent of shareholdings, receivables arising from a price supplement clause and certain capital gains carried forward.

However, Mr and Ms Y did not file such a return. And yet, when they sold the shares they held in a French company for €100 million, the share sale agreement stipulated that the price could be subsequently be increased based on certain criteria defined jointly by the parties. The possible amount of a price supplement defined in this manner should have been listed in the exit tax return.

1 Article 123 bis of the French General Tax Code: "1. Where an individual domiciled in France holds, either directly or indirectly, at least 10% of the shares, units, financial rights or voting rights in a legal structure – legal entity, organisation, trust or similar institution – established or constituted outside France and subject to a preferential tax regime, any profits or positive income derived from that legal structure shall be deemed to constitute investment income earned by said individual [...] wherever the assets or property of the legal entity [...] primarily consist of securities, receivables, deposits or current accounts."

The "Lombard Loan", an instrument to repatriate undeclared foreign assets

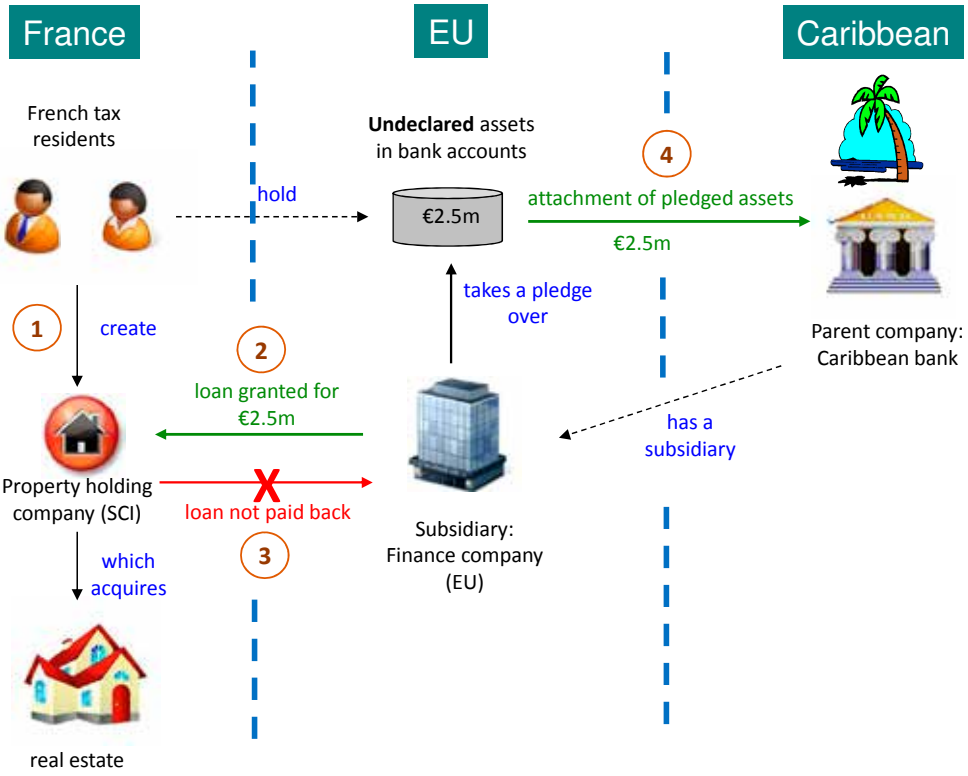
The use of a Lombard Loan pledged on undeclared assets for the purpose of repatriating them, is a well-known tax evasion concealment technique and is still in use.

Case study no. 30

A couple of French tax residents set up a property holding company (SCI) to make a real estate purchase. To finance this, the SCI borrowed €2.5 million from a financial firm registered in the EU, a subsidiary of a discreet Caribbean bank. The loan is called a "Lombard" or a "back-to-back" loan, in the sense that it is pledged on securities held in an account in another European bank, but undeclared with respect to the French tax authorities.

At the end of a year, the Caribbean bank noted the non-payment of the loan instalments, declared the loan in default and seized the pledged securities. As the price of these services, the bank charged the beneficiary family a commission of 3% on the amount of the loan.

The Lombard Loan allowed the beneficiary family to repatriate €2.5 million in undeclared foreign assets tax-free.



ABUSE OF RIGHTS: MISUSE OF A SHARE SAVINGS PLAN (PEA), INTER VIVOS GIFTS FOLLOWED BY DISPOSAL

Misuse of a share savings plan to convert taxable compensation into exempt capital gains

Under the Share Savings Plan (PEA) scheme, French tax residents can assemble a portfolio of shares in European companies. Any capital gains earned are, under certain conditions, tax exempt. This legal framework is often circumvented by some taxpayers, who do not comply with the restrictive exemption conditions.

They purchase shares in their own company from their employer at very preferential rates, put these shares in a PEA and then sell them back to their employer after a few months at twenty or thirty times the price they paid. The idea is to conceal compensation under the guise of a transaction involving the purchase and sale of securities, which are exempt from capital gains tax. French case law views this as an abuse of rights.

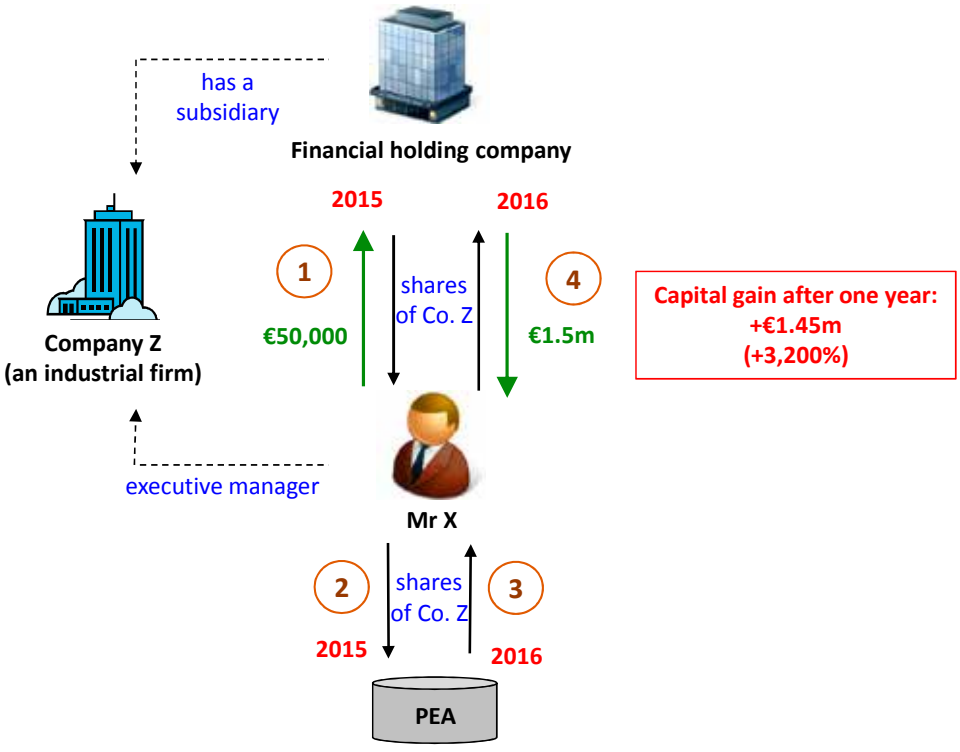
Case study no. 31

An Italian company Z, an industrial parts manufacturer, is unlisted and owned by a foreign holding company. Mr X, an executive in the French subsidiary of Company Z, purchased ten shares in Company Z from the foreign holding company for €45,000, placed them in his PEA, and then sold them twelve months later to the same holding company for €1.5 million.

Mr. X presented the capital gains generated as tax-exempt, since they were earned within the framework of his PEA. However, the sequence of events suggested that fraud was committed:

- Purchase of the shares by members of the management of the French subsidiary
- Purchase and sale of the shares carried out between the same parties – the initial seller of the shares being also the end purchaser
- A 3,200% increase in the value of the shares over a twelve-month period, at a time when the Company Z's turnover was falling off and profits were stable.

This transaction was understood as disguised, tax-free compensation through the use of the PEA's special legal framework. Under French case law, transferring a disguised compensation into a PEA is considered to be abusive, and the tax authorities can challenge the transaction as an abuse of rights, as provided for in Article L64 of the Book of Tax Procedures.



This type of abuse can also be observed within the context of leveraged buy-outs (LBOs). An investment fund offers to acquire a company by involving the company's executive management in the capital transaction. The purchase is primarily debt-funded, with the debt included in the company's balance sheet. The company has to repay the debt by improving its operating capacity in order to generate sufficient cash flow. At the end of the process, the buyers are in possession of a significantly debt-free and better-valued company, which they then seek to sell or list on the stock exchange. The value of the small share of equity that the buyers had originally invested has increased exponentially.

The company's executives who had invested in the transaction may be tempted to place the stock they purchased in a PEA to benefit from the capital gains exemption.

Case study no. 32

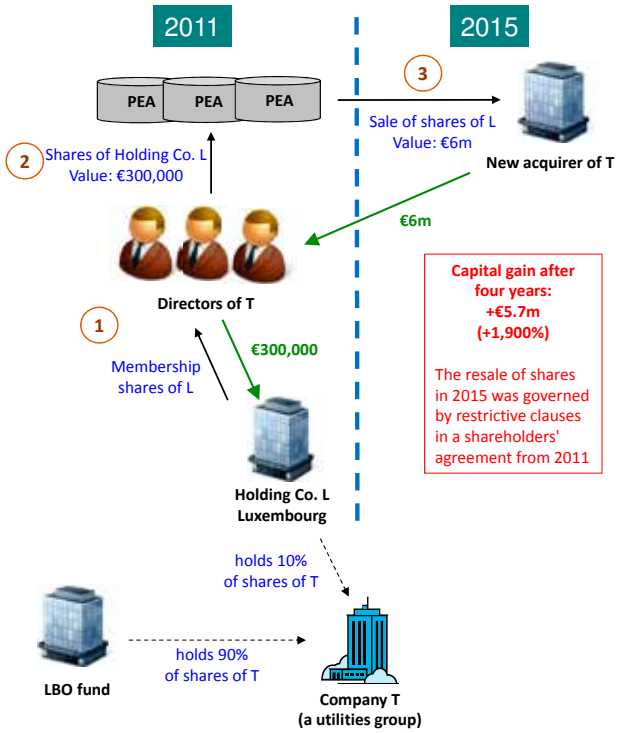
Company T, which provides services to local authorities, was the subject of two successive LBOs in 2011 and 2015, both involving an investment fund and the company's executive management. To take part in these capital transactions, members of the executive management set up Holding Company L, based in Luxembourg, to hold shares in Company T.

These managers used their PEAs to buy and sell Holding Company L's shares. These shares, which sold for €300,000 in 2011, were resold for €6 million in 2015, representing capital gains of 1,900% in four years. The capital gains generated were invested in life insurance policies.

However, the conditions under which the shares in Holding Company L were bought and sold do not appear to be part of a free exchange, with regard to both the purchase price and the restrictive share sale conditions.

The purpose of these transactions appears to be to compensate the company's senior management, tax-free, through the abusive use of the PEA's special legal framework.

In September 2014, the *Conseil d'État* stated that when shares are allocated under preferential conditions with respect to the status of the employee or corporate officer, without any financial risk, or in return for a modest investment, the resulting gains constitute a taxable benefit in the category of salaries and wages[1].



1 *Conseil d'État* ruling no. 365573 of 26 September 2014.

The technique of inter vivos gifts followed by disposal

Gifting prior to disposal has become an aggressive tax planning tool for eliminating unrealised capital gains. Nevertheless, this technique can be challenged as abuse of rights under the terms of Article L64 of the Book of Tax Procedures[1].

The case law of the *Conseil d'État* consistently challenges gifts following which the donor re-appropriates part of the proceeds of the disposal.

Case study no. 33

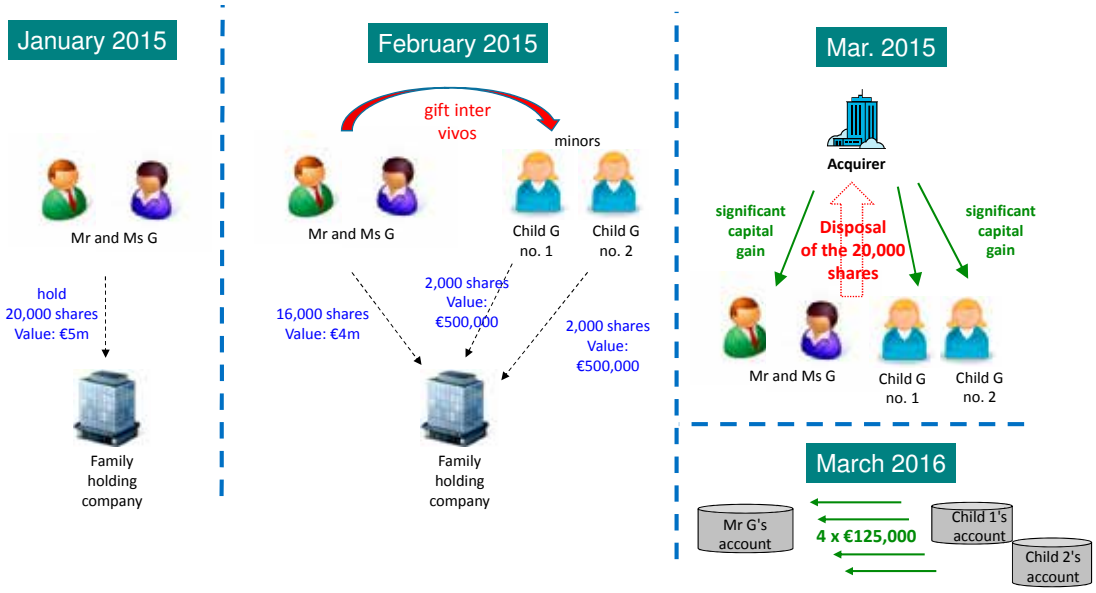
Mr and Ms G owned 20,000 shares in a family holding company. Each share had a par value of €250, making the shares worth €5 million.

They gifted each 2,000 shares in this holding company to their underage children, or a per-child gift of €500,000. Mr and Ms G retained 16,000 shares. Of this gift, a total allowance of €200,000 was granted, pursuant to Article 779 I of the French General Tax Code.

One month later, all of the members of the family sold their shares to a third party company, still at the par value of €250 per share. The disposal of Mr and Ms G's shares generated significant capital gains, to which an allowance was applied due to the length of ownership. The couple duly filed form number 2074 concerning the calculation of capital gains.

One year later, Mr G made four bank transfers of roughly €125,000 each from his children's bank accounts into his own. In this way, Mr G appeared to re-appropriate the money received by his underage children from the disposal of the shares that had taken place the previous year.

The case law of the Advisory Committee for the Elimination of Abuses of Law has established that a gift/disposal transaction can be challenged if the gift is not real and does not lead to a permanent dispossession of the donor. In the present case, the challenging of the gift followed by disposal led to the immediate taxation of the capital gains on the shares that were gifted to the children, which had previously benefited from a total allowance of €200,000.



1 Art. 64 of the Book of Tax Procedures: "The tax administration shall have the right to disregard transactions that constitute an abuse of law, whether these are fictitious or whether, by seeking the benefit of a literal application of provisions or decisions, in opposition to the initial objective pursued by their authors, these transactions were inspired by no other reason than to avoid or reduce the tax burden which would have normally been borne by the taxpayer, due to his or her situation or real activities, had those transactions not been entered into."

COMBATING THE CHANGING FACE OF SOCIAL SECURITY FRAUD THROUGH HEIGHTENED CROSS-DEPARTMENTAL COOPERATION

Tracfin is taking determined action to fight social security fraud. Article 129 of the 2012 Social Security Budget Act no. 211-1906 of 21 December 2011 makes social protection bodies eligible to receive information notes from Tracfin. On 1 March 2012, Tracfin and France's primary social protection bodies (ACOSS (URSSAF), CNAMTS, CNAVTS, CCMSA, CNAF, Pôle Emploi and RSI) formally agreed to build close working relations.

In 2016, these bodies received 165 information notes from Tracfin, a 51% increase over the previous year. The number of information requests submitted by Tracfin to these organisations increased by the same proportion. The total amounts involved came to €140 million. The primary recipient was the ACOSS (Central Agency for Social Security Bodies). Given the overwhelming percentage of STRs involving the use of undeclared labour, the construction sector was by far the sector that received the most attention.

There was little change in the main types of social security fraud observed:

- Unpaid social contribution fraud
  - Undeclared work and use of undeclared labour
  - Understatement of the base for calculation of social contributions by concealing a proportion of professional activity
- Frauds concerning unduly received benefits
  - Carrying out regular undeclared work while at the same time collecting benefits
  - Residence fraud
  - Suspicion of diverting pension benefits via "collection accounts"
  - Defrauding supplementary mutual funds and fraud by healthcare professionals

PENSION BENEFITS COLLECTION ACCOUNTS – DETERMINED, LONG-TERM ACTION PAYS OFF

Since 2013, the National Anti-Fraud Office (DNLF), the National Pension Fund (CNAV) and Tracfin have jointly focused on the issue of pension benefits collection accounts. Although the risk remains high, the number of cases observed has fallen off. The 31 information notes passed on by Tracfin between 2013 and 2016 allowed the CNAV to carry out audits of hundreds of individual cases. Some 15% of cases involving non-residents turned out to involve fraud. There is still a high risk of this type of fraud: the principal case in 2016 concerned large amounts of money.

Individuals who have worked in France receive social benefits, including pension benefits from the CNAV, regardless of whether they are French residents. The benefits are paid into the French bank accounts of the beneficiaries.

In the case of non-resident beneficiaries, the fraud consists in not reporting the death of the beneficiary so that third parties can continue to receive benefits. These are sent, by bank transfer or cash transfers, from the beneficiary's French bank account to a small number of centralising accounts. The funds are then transferred abroad, mainly to the Maghreb.

Tracfin has identified collection accounts fed by dozens, sometimes hundreds of pensioners' accounts, and catalogued the intermediaries, known as "collectors". The cash flows show that pension benefits have been misappropriated. Cases of document fraud have been identified in the identity papers used to open accounts and file for power of attorney, corroborated with information from the CNAV.

Some collectors are intermediaries within larger pyramid organisations. They are then themselves objects of collections at higher levels. In other cases, collection is followed by purchases of miscellaneous consumer goods in France which are then shipped to the Maghreb.

This type of fraud involves large and well-established import-export companies in France.

Warning signs:

For the CNAV:

- Multiple pension funds paid into a single bank agency
- An abnormally high proportion of very old beneficiaries
- Contradictory documentation submitted for the same case: a death certificate sent by certain family members and proof of existence submitted by third parties
- The benefits recipient is not the holder of the bank account into which the benefits are paid

For banks:

- Bank account opened using false documents
- Presence of a proxy for the account, who is collecting the money paid out by the pension fund
- Fund movements: the benefits received are the subject of regular and large-scale cash withdrawals or bank transfers, either within France or abroad

Although this type of fraud can be stemmed by determined, long-term cooperation between the public bodies concerned, the growth of the collaborative economy once again raises the issue of social security fraud.

SOCIAL SECURITY FRAUD IN THE COLLABORATIVE ECONOMY

The rise of the collaborative economy is fostering the emergence of a new type of fraud, particularly in the sector of private hire vehicles (VTC). Some companies misuse the status of freelance entrepreneur to avoid paying social security contributions, even though there is a proven relationship of subordination between the company and its drivers.

Case study no. 34

Company K was a public passenger transport firm. In its first year of activity, the company's bank accounts revealed cash inflows of €2.5 million, the bulk of which consisted of transfers from a major private hire vehicle (VTC) platform.

Outflows consisted of bank transfers and cheques to individuals and to companies in the automotive sales and leasing sector. The individual beneficiaries were the subject of advance hiring notices (DPAEs) by the company K.

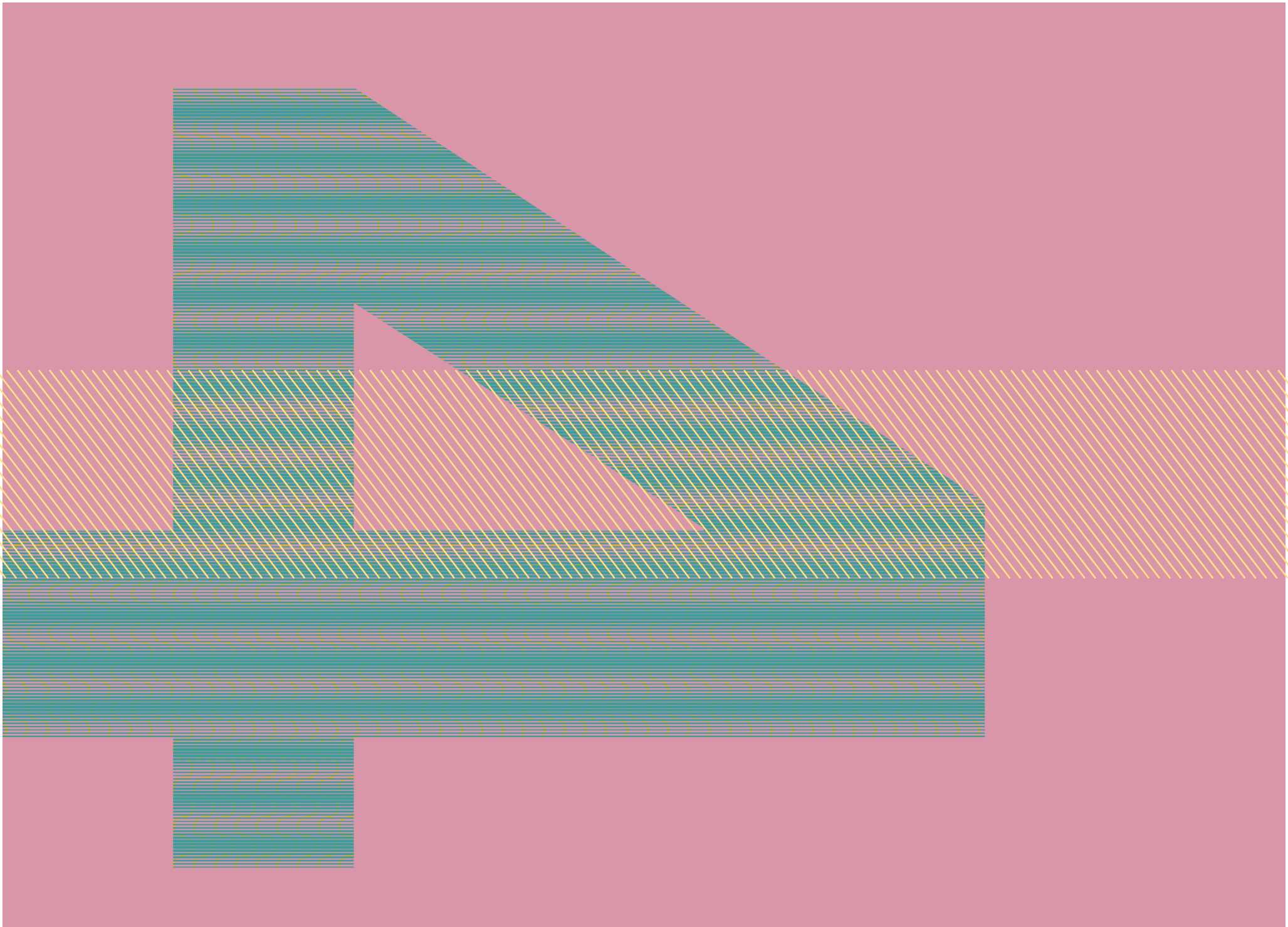
Company K reported to URSSAF (the Social Security and Family Benefit Contribution Collection Office) that its total wage bill was €315,000 for 35 employees, even though it had issued 230 DPAEs. In the following year, there were a number of inconsistencies between the relatively stable amounts of wages paid and the number of declared employees, which fluctuated widely.

These discrepancies between the wage bill and the number of employees were due to the use of drivers who were freelance entrepreneurs. At the end of their probationary period, most drivers recruited as employees ended up choosing freelance entrepreneur status. Company K thus had some thirty stable employees on average over a year's time. The bulk of the workforce was made up of a high turnover of drivers. The company did not use fixed-term or open-ended employment contracts, but rather advance hiring notices which were not converted into one of these types of contracts at the end of the probationary period.

The use of freelance entrepreneur status was abusive, since the drivers remained bound by a relationship of subordination to Company K:

- Company K was their only employer, which alone dictated the drivers' trips.
- It provided them with their working equipment, i.e. the vehicle. Company K owned at least fifty vehicles, some of them purchased with its own assets and others that were leased. The relationship of subordination was also underscored by how rates were set and by the instructions given to drivers about how they should carry out their duties.
- The company set the rates and told the drivers how they should do their job.

Thus, to avoid paying social security contributions on a large portion of its staff, Company K declared that it had only thirty employees, whereas the genuine average number of drivers was at least fifty.



THE ONGOING FINANCIAL SERVICES TECHNOLOGICAL REVOLUTION IS SET TO DISRUPT THE SECTOR – AND AML/ CFT REGULATIONS MUST ADAPT

FinTech firms[1] use the technological innovations of the digital revolution to offer easy-to-use, quick and less costly financial services. Their offer has primarily developed in payment services and account management. The emergence of new payment service providers (PSPs) is disrupting the traditional banking sector. These changes are likely to gather pace as the global web giants or mobile telephone operators enter these markets.

The combination of new technological solutions limits the effectiveness of existing AML/CFT systems by diluting the compliance checks performed by authorised operators. Regulators are endeavouring to adapt to these changes in the sector, but this trend is only in its nascent stages.

THE GROWING NUMBER OF NEW PAYMENT SERVICE PROVIDERS MAKES FINANCIAL FLOWS MORE DIFFICULT TO TRACE

PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS ARE PROLIFERATING, WITH SUPPORT FROM EU DIRECTIVES

The new payment service providers (PSPs) come in several forms, including:

– online payment management platforms, which can be likened to infrastructure usable by other PSPs or directly by retailers or end customers
– other service providers (payment services apps, crowdfunding platforms, payment card issuers) who act as intermediaries between the end customer and the digital platform that manages the financial flows

PSPs offer their clients e-money "wallets" that can be reloaded by transferring funds from: (i) bank accounts, (ii) other e-money wallets, or even (iii) physical devices such as prepaid cards or vouchers. These operators interact with one another via APIs[2], which allow their IT systems to communicate smoothly.

These players take advantage of the EU's 2015 Payment Services Directive (PSD2), which was transposed into French law in August 2017[3]. This Directive officially recognises new providers from the FinTech sector. These new players are mainly payment institutions and electronic money institutions, as well as account aggregators and payment initiation service providers[4]. PSD2 ended a form of monopoly held by banks on payment services, offering substantial commercial leeway to new payment service providers.

1 FinTech is a contraction of financial technologies.

2 An API is an application programming interface.

3 Directive (EU) 2015/2366 of 25 November 2015, enacted into French law by Order no. 2017-1252 of 9 August 2017, along with related decrees and orders (see the Official Journal of the French Republic, dated 10 August and 2 September 2017). The deadline for enacting PSD2 into national legislation for all EU Member States was 13 January 2018.

4 AISPs (Account Information Service Providers) and PISPs (Payment Initiation Service Providers).

FINANCIAL FLOWS ARE BECOMING HARDER TO TRACE

The emergence of these new operators makes financial flows harder to trace. PSPs act as an intermediary between a client and his/her bank. The client registers his/her bank account details or bank card with a PSP, which in turn manages payments to third parties. The PSP thus divests the bank of a portion of the data required to carry out an in-depth analysis of the client's transactions. From the bank's standpoint, the PSP is the sole counterparty for financial flows involving the client's account.

To operate as a business, PSPs must receive authorisation from a banking supervisor, which requires them to implement AML/CFT due diligence measures. Under French law, they can notably elect for the status of payment institution (PI) or electronic money institution (EMI), issued by the Prudential Supervisory and Resolution Authority (ACPR)[1]. Pursuant to Article L.561-2 of the French Monetary and Financial Code (CMF), PIs and EMIs are subject to the AML/CFT system, which requires them to fulfil customer due diligence obligations[2], as well as Tracfin reporting obligations.

However, the AML/CFT system has weaknesses given its functional and geographic scope of application.

On a functional level, an effective scheme must apply to all relevant stakeholders. AML/CFT regulations should be focused on the stakeholders that have the best knowledge of the end customer. Yet authorised financial institutions (such as banks, PIs and EMIs) sometimes have less customer data than other increasingly active payment sector stakeholders, such as the major Web 2.0 players or mobile telephone operators. The latter are not currently subject to the AML/CFT system.

From a geographic perspective, AMT/CFT requirements should be uniform across countries. Yet not all countries have the same level of requirements in terms of issuing authorisations or monitoring operators. Within the European Economic Area, the Free Provision of Services (FPS) regime, made possible by the European passport, curbs the supervisory powers of national regulators (see part 5 below). Distortions from one country to the next reduce the effectiveness of the AML/CFT system. Strengthened cooperation may not be sufficient without considerable harmonisation of the actual authorisation and supervision process.

1 Crowdfunding players have the status of "crowdfunding intermediaries" or "crowdfunding advisers".

2 Identify their client and check his/her identity (Article L.561-5 of the CMF); characterise the business relationship (Article L.561-5-1 of the CMF) throughout the client relationship; and make sure that the client's transactions are coherent (Article L.561-6 of the CMF).

THE MAJOR WEB PLAYERS ARE TACKLING THE MONEY TRANSFER AND MOBILE PAYMENT SECTORS

A DECISIVE ADVANTAGE: CONTROL OF BIG DATA

The major web players have driven the digital revolution and gained dominant positions. Now they are pushing new business models based on the use of data. Combining financial strength and wide-scale support from consumers, these players have unparalleled firepower to penetrate the financial services industry. They could considerably reshape the payment services sector.

Thanks to their technological expertise and skill at collecting and analysing big data, they can compete with banks on several traditional banking segments such as means of payment or loan offers. Their capacity to track and anticipate consumers' online purchases can make them alternatives to banks for some products and services thanks to their better customer knowledge.

In turn, the major web players draw on numerous startups. They benefit from the innovations developed by startups, while offering immediate growth prospects; this alliance of services is especially effective.

Solutions that are already developed and available involve international money transfer services, instant payment services via the Internet or mobile phone, as well as lending to companies.

THE CHINESE MARKET IS A FORERUNNER

China is a forerunner in the payment services digital revolution. The Chinese leaders in e-commerce, mobile telephony and the Web 2.0 began to conquer the financial sector about a decade ago – providing strong inspiration for their Western peers. This head start is notably attributable to China's weight in global e-commerce ($672bn in 2016, i.e. 40% of global e-commerce, which is expected to come to $1,600bn in 2018), along with a sizeable potential customer base (some Chinese social networks have up to 550 million users) and a local banking system that is struggling to adapt to the economy's digital transformation. Chinese web leaders have a broad offer that covers all banking services: payment systems, e-money wallets, online banking, savings products.

Some of these players, having achieved a dominant position on their local market, are expanding outside China into Southeast Asia and also Europe. In 2016, one of these Chinese heavyweights signed a partnership with a French bank to offer French retailers an easy payment solution for Chinese tourists. Targeting high-spending customers, this solution consists of contactless mobile payment from an e-money wallet belonging to the Chinese consumer, who credits the wallet from his/her bank account in China. This system allows the customer to spend up to €40,000 per transaction, and to carry out as many transactions as desired. However, although the French partner bank carries out compliance measures, these only involve the retailers who receive payments. The French bank therefore has no information on the payer, the origin of the funds, or how the account was credited. The AML/CFT due diligence for the issuer depends on the Chinese company's compliance department.

Relatively similar solutions are being developed by Western players in both mobile payments and instant web payments. These services, when combined with prepaid cards, make financial flows more opaque. They can become very popular among users extremely rapidly.

CROSS-FERTILISATION BETWEEN MAJOR WEB PLAYERS AND STARTUPS

Certain web players reach a huge audience of consumers, opening up opportunities for immediate growth for innovative startups.

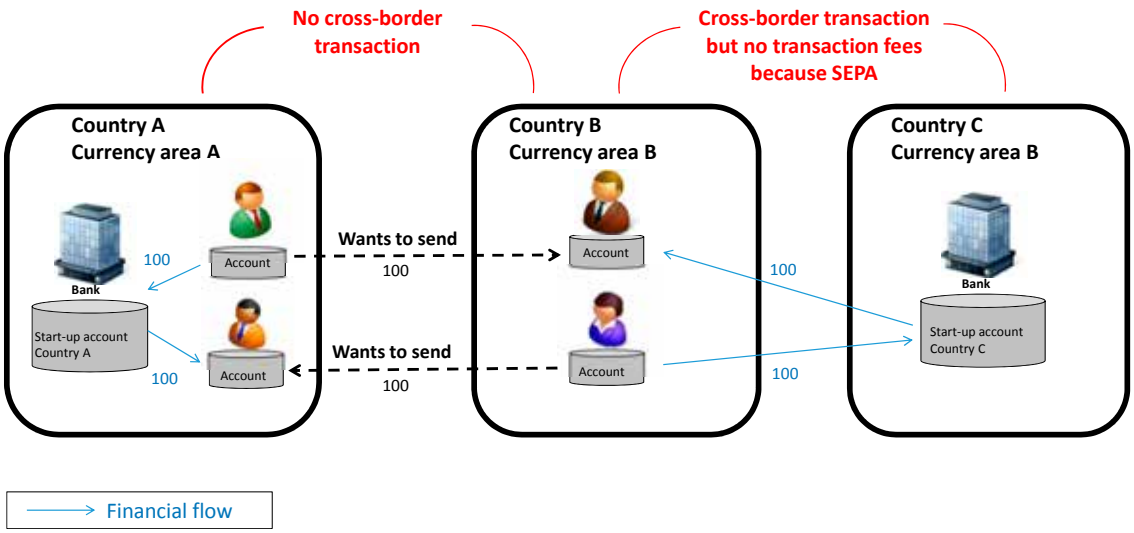
Case study no. 35

One of these startups offers international money transfers with currency conversion. This service uses cross-settlement to avoid clients having to pay the cost of international bank transfers and forex fees. The cross-settlement mechanism, breaking with basic accounting principles, interrupts the traceability of a financial flow. This places a special responsibility on the operator in order to reconstruct this traceability and to fulfil its AML/CFT obligations.

Moreover, this startup has no cap on the amounts that can be transferred.

In France, this firm operates with a European passport under the FPS regime. It does not need to have offices in France. The transactions reviewed by Tracfin involve flows to/from Western countries or developed Asian countries. These transactions are mostly initiated by expats or retirees who use this service to send money home or to carry out property investments. However, the use of these services can give rise to suspicious transactions in some cases, involving sizeable amounts of money.

The success of this kind of offer appeals to Web 2.0 players. Recently, a major web firm added a feature to its online chat that allows users to access this startup's international money transfer service. Simply by indicating a recipient's first and last names and e-mail address, users of the same network can send money. As none of the firms involved with this service are registered In France, it is very difficult for Tracfin to track these transactions without making a formal request to foreign FIUs.



PROMOTING ANONYMITY: OVERLAPPING NEW TOOLS THAT COMBINE E-MONEY, VIRTUAL CURRENCY OR COMMODITIES

Tracfin has noted cases that combine the use of electronic money and virtual currency in a single transaction: sending funds jointly to prepaid cards and virtual currency trading platforms; payment accounts used for transactions on online marketplaces... The use of overlapping payment instruments generally indicates a desire for opacity. There is a growing number of tools available to achieve such opacity.

BLOCKCHAINS DEVELOPED SPECIFICALLY FOR PURPOSES OF ANONYMITY

The bitcoin blockchain, while initially regarded as a powerful vector for anonymity, actually only offers partial anonymity. While the bitcoin blockchain is currently accessible without any KYC procedure and an individual can open any number of wallets without giving his/her identity, traceability is nevertheless a key characteristic of the bitcoin blockchain[1].

A bitcoin transaction is equivalent to a payment made under a pseudonym. The pseudonym in this case is the public key used to acquire or dispose of units of value. Each user can only carry out transactions using his/her public key. As long as a public key is linked to the identity of an individual, the bitcoin blockchain enables all transactions involving this user to be traced back. A blockchain operator – e.g. a bank, a retailer or government authorities – that knows both an individual's identity and his/her public key can cross-check its own client data with the transactional data from the blockchain. As the use of the bitcoin blockchain becomes more widespread, transaction analysis software solutions are being developed.

This is why the experts who want total anonymity are attempting to develop other blockchains. Some blockchains have been especially designed to make transactions untraceable and to facilitate opaque trade.

The methods for preserving anonymity are based on various complex cryptographic technologies.

One of these blockchains is built using a method known as zero-knowledge proof. This technique involves breaking the data about a transaction down into a large number of small pieces that are then mixed up, using a principle similar to clouding, so that the transaction is untraceable.

Another blockchain uses a technique known as one-time ring signature. In this system, public keys are grouped together in a ring so that the issuer of a transaction cannot be specifically identified during the validation. Likewise, by using a one-time address instead of his/her public key, the recipient of a payment avoids being identified. The transaction is totally opaque.

However, identification becomes possible again when a user wishes to transfer his/her holdings out of a blockchain and into real currency or to another more transparent blockchain.

REAL CURRENCY PAYMENT CARDS BACKED BY BITCOIN ACCOUNTS ("BITCOIN DEBIT CARDS")

Since their inception in 2013, payment cards backed by bitcoin (BTC) wallets, known as bitcoin debit cards, are expanding rapidly. The balance on the card is the real currency equivalent of the amount of bitcoins held. These cards allow users to pay a mortar-and-bricks or online retailer in real currency, or to withdraw cash from ATMs in the Visa and MasterCard networks (so-called "cash out"). Criminals use "cash out" to convert the profits from illegal activities from bitcoins into cash. These profits are usually from the sale of contraband items on the dark web (e.g. drugs, weapons, fake identity papers or stolen bank details).

These bitcoin debit cards raise a similar problem to prepaid cards that can be reloaded with cash. They offer a high degree of anonymity, together with

1 See Laurent Leloup, *Blockchain, la révolution de la confiance, Eyrolles*, 2017, pp 50-55.

maximum portability. The AML/CFT risk cannot be curbed unless card issuers maintain a high level of compliance with due diligence obligations – but this is not a foregone conclusion for the issuers identified so far. There are at least 20 bitcoin debit card operators established abroad (in the Americas, Asia and Russian-speaking countries). Half of these use the same EMI, which is registered in a Mediterranean offshore financial centre.

Some bitcoin debit card operators have agreed to cooperate with the authorities. Others are less open and use their guaranteed anonymity as a key sales argument. Although their general terms of use indicate that identification measures are in place above certain financial thresholds, in reality, they apply poor compliance measures.

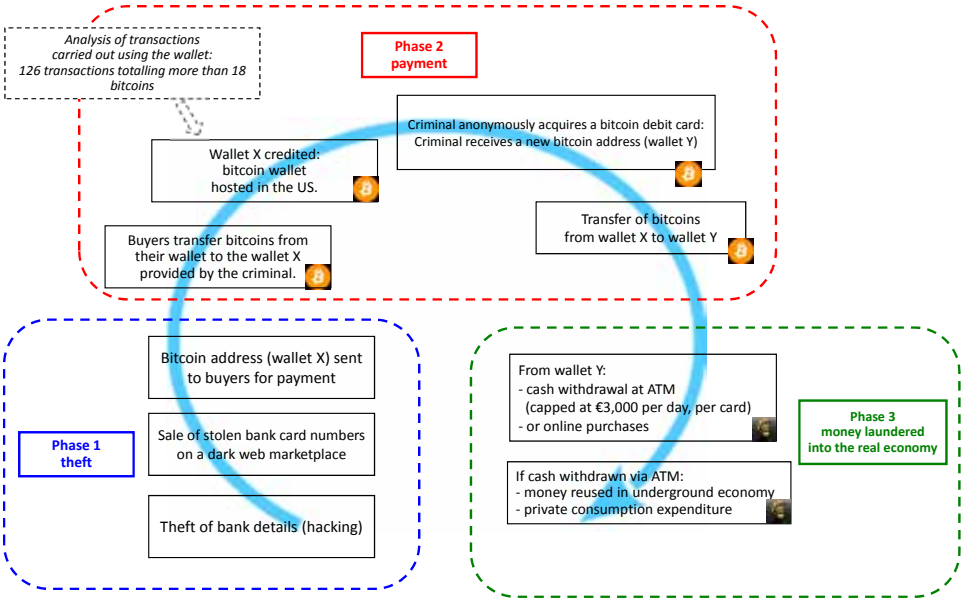
A cybercriminal can choose a bitcoin debit card that provides complete anonymity for the cardholder. In addition, the thresholds for loading the card, making payments or withdrawing cash can easily be thwarted by opening an unlimited number of accounts. Investigators struggle to identify cardholders, all the more because the latter often take every precaution by using the Tor anonymity network and virtual private networks (VPNs).

Case study no. 36

The National Gendarmerie's Central Department for Criminal Intelligence (SCRC) has a specialised criminal investigation unit, the Centre for Fighting Digital Crime (C3N). C3N and Tracfin collaborate on digital crime issues. Over the past two years, C3N has conducted several legal cases involving the use of bitcoin debit cards.

On 17 February 2016, C3N arrested a French cybercriminal who was selling stolen bank card numbers in exchange for bitcoins on the dark web. The proceeds of these sales were transferred to a bitcoin wallet connected to a bitcoin debit card issued in a foreign country. These funds were then withdrawn in cash at an ATM or used to purchase IT equipment on the Internet.

- The funds do not transit through the traditional banking system.
- Transactions and ATM withdrawals are only detectable by requisitioning the card issuer, the real currency/virtual currency exchange, or the EMI that manages the e-money wallet.
- By using several different cards, an individual can circumvent e-money regulations.
- Identifying the transactions does not always mean that the perpetrator can be identified. The perpetrator can resort to techniques for acting anonymously, both on the Internet (VPN, TOR) and for possible deliveries of any physical goods purchased on line ("drop-shipping").
- Identifying the bitcoin debit card does not always mean that the effective beneficiary can be identified. The basic version of the card can be subscribed to anonymously.



PAYMENT CARDS BACKED BY COMMODITIES

Launched in 2013, a service designed by a precious metals trader enables users to purchase gold, silver or diamonds as savings that is liquid, tangible and outside the banking system. The precious metals and gems are held in a bank vault in Switzerland. In exchange for these assets, the client is given a prepaid card whose balance is indexed on the physically-held commodities[1].

The prepaid card is issued by a PSP registered under UK law and is backed by the MasterCard network. The PSP operates in France under the FPS regime. The contract binding the company that markets the card and the PSP is regulated by the Financial Conduct Authority.

According to available documentation, this payment card does not appear to have a balance cap. This is contrary to the French Monetary and Financial Code, which sets the maximum balance for e-money on a physical payment device at €10,000. By default, payments are capped at €500 per day, but this ceiling can be raised if the client requests so.

This service must comply with its AML/CFT obligations on French territory, such as recording the identity of its users and reporting suspicious transactions. The company that markets the card also keeps a register of all transactions. However, this system is not fail proof, and incidents of document fraud or bank card fraud have been observed.

Tracfin has observed that this kind of card was used by an individual suspected of travelling to the conflict zone in the Middle East.

1 For diamonds, the fact that there is no official market price, together with the difficulty of listing gemstones on a market, raises the same valuation issue referred to in Section 1.1.4.1 of this report.

COMMODITY TRADING PLATFORMS THAT ACCEPT CRYPTOCURRENCY

An e-commerce platform registered in an EU Member State enables users to buy and sell precious metals such as gold, silver, platinum or palladium. It accepts payments in virtual currencies including bitcoin, ether and ripple.

A foreign FIU notified Tracfin that an individual residing in France had laundered bitcoins earned from carding activities (i.e. selling stolen bank details) by converting these bitcoins into precious metals via this platform.

Precious commodities such as gold or diamonds are known money-laundering vectors. Any technology that facilitates the conversion of such commodities into means of payment, be it e-money or virtual currency, is a factor for higher risk of money laundering.

PEER-TO-PEER INTERNATIONAL MONEY TRANSFERS: CREATING "DIGITAL CASH"

Some platforms have also taken advantage of blockchain technology to offer international money transfers at lower cost.

Case study no. 37

A US-based platform lets individuals transfer money internationally in real currency, using only a telephone number for identification. The platform converts the client's funds into bitcoins, then uses the Bitcoin blockchain to carry out a peer-to-peer transaction, with the funds being converted back into the recipient's actual currency. The conversion into virtual currency is seamless for users; they do not need to manage a virtual currency wallet on their own.

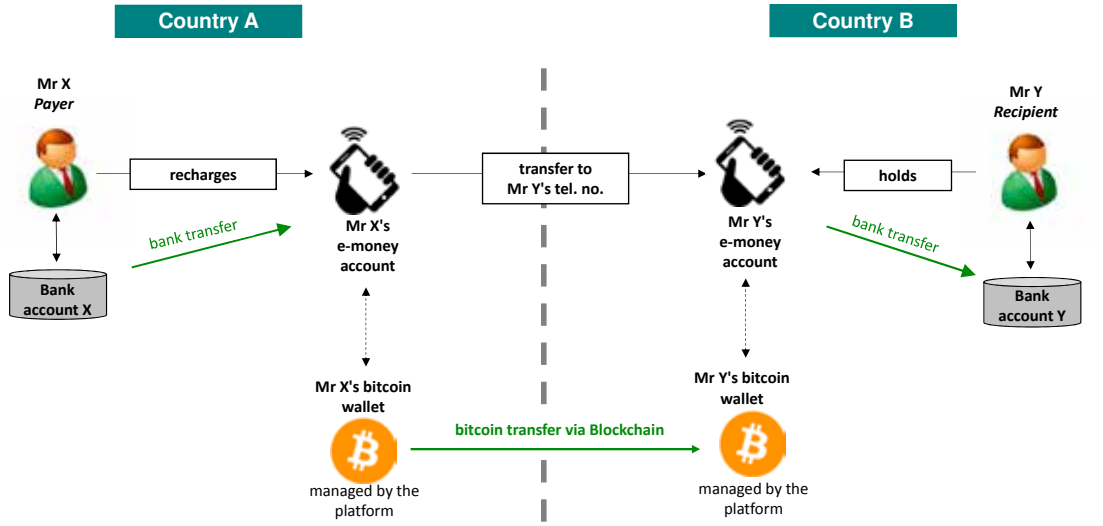
Tangibly speaking, a user who wishes to transfer money overseas has several options:

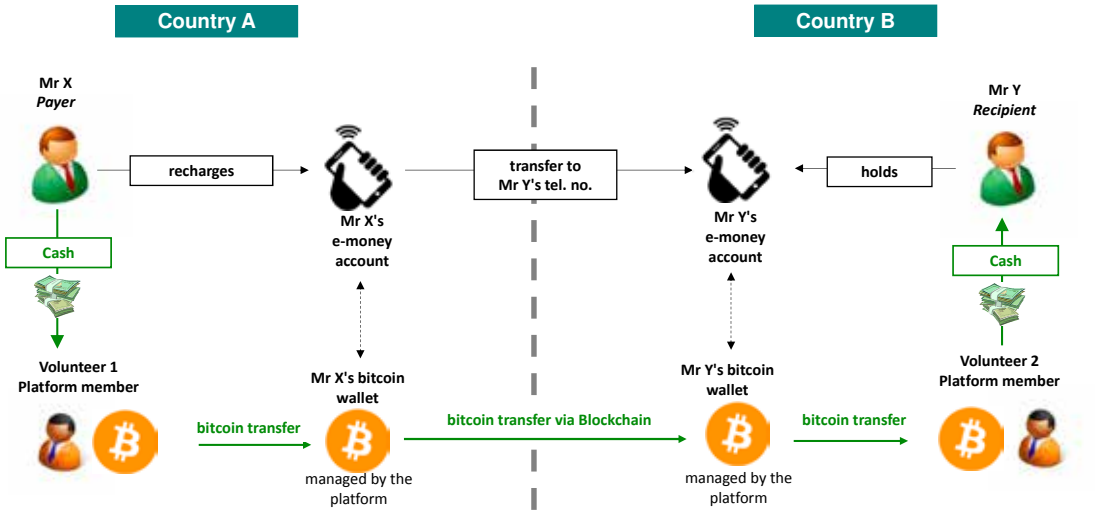
- The users on both ends (remitters and recipients) must already have an e-money account with the operator.
- While opening an account, the platform creates a bitcoin wallet and generates the necessary cryptographic keys. The public key corresponds to the address of the bitcoin wallet used for a client's transactions. This public key will be linked to the e-money account and telephone number of the client. The telephone number will be the only way for the other community members to identify the client.

- The account can be loaded in two different ways:
  - either from a bank account by way of a bank transfer to the e-money account on the platform
  - or directly in cash, with other platform users acting as intermediaries (these users can be located in the same way as a driver on a ridesharing platform). Users can volunteer to act as forex brokers: in exchange for cash, they credit an equivalent amount of bitcoins to the bitcoin wallet of another user
- The user then communicates the recipient's telephone number, and the funds arrive on the recipient's pre-established account.
- He or she can transfer the amount onto his or her own bank account, or receive it in cash using the same principle of exchange between volunteer community members.

Thus, when a transfer is sent as cash and received as cash, its anonymity is ensured by the bitcoin conversion and largely preserved. Only the telephone number and public key are known to the platform. The cash on both sides of the transaction is "digitalised" thanks to the conversion into virtual currency.

This platform is not yet available in Europe – but it could become available quickly.





IDENTITY FRAUD AND DOCUMENTARY FRAUD: A MAJOR FLAW

While technological innovations tend to facilitate anonymity, the leading factor of anonymity in payment services is achieved through documentary fraud and identity fraud. The magnitude of this phenomenon currently represents a serious flaw in KYC procedures, especially for online payment services. Either over the Internet or through a criminal outfit, it is easy to obtain fake identity papers whose authenticity is hard to verify by an operator, more so because the client identity checks carried out by some payment service providers are not very effective.

The use of fake identity papers converges with the use of new technologies that facilitate anonymity:

- In the field of virtual currency, Suspicious Transaction Reports submitted to Tracfin indicate a growing number of cases involving the use of falsified or stolen documents to access platforms for exchanging real currency and virtual currency. This is an indication of fraudulent intent. By using fake identity papers, sometimes combined with a VPN to hide the user's IP address, users can carry out their transactions completely anonymously[1].
- In the field of crowdfunding, Tracfin has also observed attempts to use fake identity papers on crowdfunding platforms. Payment service providers that manage platform accounts and are authorised by French regulators are informed of these risks: when they detect identity fraud, they refuse to open a payment account.

Crowdfunding platforms are also vulnerable to the fraudulent use of stolen bank cards, which are frequently reused on such platforms. Payment accounts linked to fundraising websites are used as transit accounts to convey funds from stolen bank cards. There are two typical situations: either the individual creates a payment account without donating to a project and uses this account as a simple transit account, or a fundraising project is created specifically to funnel funds from the stolen bank card.

One case revealed that some individuals use different fundraising websites simultaneously in order to split the amounts and avoid being detected by the payment institution. The amounts are low, seldom exceeding €1,000.

1 VPN: A virtual private network, which allows a direct connection between remote computers without revealing their locations.

NEW TECHNOLOGIES CONSTANTLY BROADEN THE SCOPE OF POSSIBLE FRAUDULENT ACTIVITY

DISTORTED USE OF BLOCKCHAINS FOR FRAUDULENT PURPOSES

An analysis of Suspicious Transaction Reports involving the use of virtual currencies reveals recurring cases of scams: either pyramid scams such as Ponzi schemes, or price manipulations of a blockchain's unit of account.

In this respect, blockchains do not actually create any new methods of fraud, but instead broaden the scope for proven methods.

A simple scam: a fictitious blockchain

In 2016, Tracfin received several Suspicious Transaction Reports involving a "blockchain" that was actually a simple Ponzi scheme.

The creators of this "blockchain" sold units of a virtual currency to investors, but the blockchain had never been developed and did not really exist. It was a simple website. The putative virtual currency was marketed by a company whose registered office was in the Persian Gulf and which held bank accounts in an EU Member State.

The fraudsters successfully collected several tens of millions of dollars worldwide, using a portion of the funds collected to advertise the website. They had recruited a politically exposed person from an EU Member State to promote their site. A complaint was lodged against this person for fraud.

While this case received media attention, Tracfin has become aware of several other similar websites that offer fictitious blockchains.

A subtle scam: manipulating virtual currency prices by gradually taking over the transaction validation processes in a blockchain

The designers of a blockchain implemented a subtle scamming mechanism based on changing the method for validating transactions. This enabled them to manipulate virtual currency prices.

VALIDATING TRANSACTIONS ON A BLOCKCHAIN: THE CONSENSUS MECHANISMS

A blockchain, as a distributed ledger, relies on the transactions being validated by all blockchain members. The process whereby a block (i.e. a series of transactions) is validated is known as "mining". The miner who validates a block is rewarded with an amount of that blockchain's currency.

There are two main methods for validating transactions:

– The most secure method is called proof of work (PoW)

PoW is used on the bitcoin blockchain. It involves solving a cryptographic puzzle. Any participant on the blockchain can attempt to solve the puzzle, and from the outset, everyone has the same chance of being the first to solve it.

When a blockchain is launched, there are few transactions and the PoW is relatively simple. As the network grows larger, the PoW becomes complex.

– Another method is called proof of stake (PoS)

This method uses less computational power. It involves creating a mechanism whereby network nodes are punished if they do not follow the consensus protocol. To have the right to validate blocks, participants bet an amount of cryptocurrency on the expected consensus outcome. If the bet is wrong, the malevolent nodes that bet against the majority consensus lose the amount wagered. Participants who attempt to cheat by validating a block that should not be validated are penalised financially.

However, the PoS method is criticised for two reasons: Firstly, it is considered to be less secure and more vulnerable to attacks; secondly, it provides a permanent advantage to "richer" participants: the probability of being chosen to mine a block depends on the quantity of cryptocurrency already held by the miner.

The PoS method therefore appears to be a proprietary system, privatised by the cryptocurrency holders. Transaction validation is based on those who already have cryptocurrency (or coins), just as the voting rights on the board of directors of a corporate belong to the shareholders.

Source : Stéphane Loignon, *Big bang blockchain, la seconde révolution d'internet*, Tallandier, 2017.

The creators of the blockchain in question initially chose the proof-of-work method. They did the mining themselves and kept 80% of the coins generated on the blockchain. Then, they shifted to the proof-of-stake method. As they held most of the coins generated on their blockchain, they were able to control the validation of transactions.

The designers of this blockchain then implemented a "pump and dump" scheme, i.e. a price manipulation which consists in artificially pumping up the market price of the coins, then "dumping" (selling) them at the highest price before allowing the price to collapse. Indeed, a few accomplices with a certain weight on a given market can collude to carry out a series of transactions aimed at attracting small investors (i.e. followers) by generating trading activity and a rise in the market price of an instrument (or in this case, a cybercurrency unit). The capitalisation – or total value –of this blockchain's coins rose to $32m. The holders then sold the coins for bitcoins. The market price of the coins quickly plummeted, to the detriment of those who bought just before the crash.

It is believed that the founders of such a site managed to sell their coins on time, pocketing some $20m worth of bitcoins. They were then able to convert these bitcoins into real currency by using bitcoin debit cards. This income left no traces and was not subject to any taxation.

When a blockchain's reputation is tarnished by this kind of manipulation, its designers may change its name several times or convert it into other applications, such as using the coins on e-commerce platforms.

For reasons of discretion and technical feasibility, fraudsters tend to favour blockchains with low capitalisations, as well as second-tier market platforms. The bitcoin blockchain, for example, may seem too visible or require too much computational power. However, the runaway surge in the bitcoin price since the first half of 2017 means that we cannot completely rule out the possibility of bitcoin prices being manipulated. Other influential stakeholders (mining coops, well-known developers or industrial players) may, at least in theory, impair the system's decentralisation.

RISKS OF FRAUDULENT ACTIVITY ARE EXPANDING IN CROWDFUNDING AS DEDICATED PLATFORMS BECOME WIDESPREAD

As for virtual currencies, Suspicious Transaction Reports received by Tracfin in 2016 refer to several Ponzi scams that tarnish the reputation of crowdfunding platforms. The non-repayment of loans offered online damages the credibility of the offers of crowdfunding platforms. This is currently an incentive for crowdfunding intermediaries to implement the AML/CFT system and to file Suspicious Transaction Reports.

Tracfin referred a case to the courts involving a platform set up in the UK, managed by a French national, which had raised more than €700,000 from individuals. For the most part, these funds were used by the managing partner and not invested in the purported projects.

Crowdfunding intermediaries have reported other kinds of scams: cases in which small businesses ask for loans based on fake documents (invoices, identity papers, etc.), as well as cases in which loans are not repaid. In one instance, a company requested a loan from a crowdfunding intermediary, and only made three instalments on its repayment plan (out of 24). The company was placed under court-ordered liquidation soon after the loan was granted, and its directors left France for Turkey. The crowdfunding platform suffered a loss of some €50,000.

TRACFIN'S ACTIVITIES INVOLVING VIRTUAL CURRENCIES AND CROWDFUNDING

In 2016, Tracfin received 178 Suspicious Transaction Reports directly related to virtual currency transactions, for a total value of nearly €5m.

In more than half these cases, the purchase or sale of virtual currency is at the root of the Suspicious Transaction Report. A majority of reports were motivated by doubts about the origin or destination of funds, without any specifically characterised suspicions.

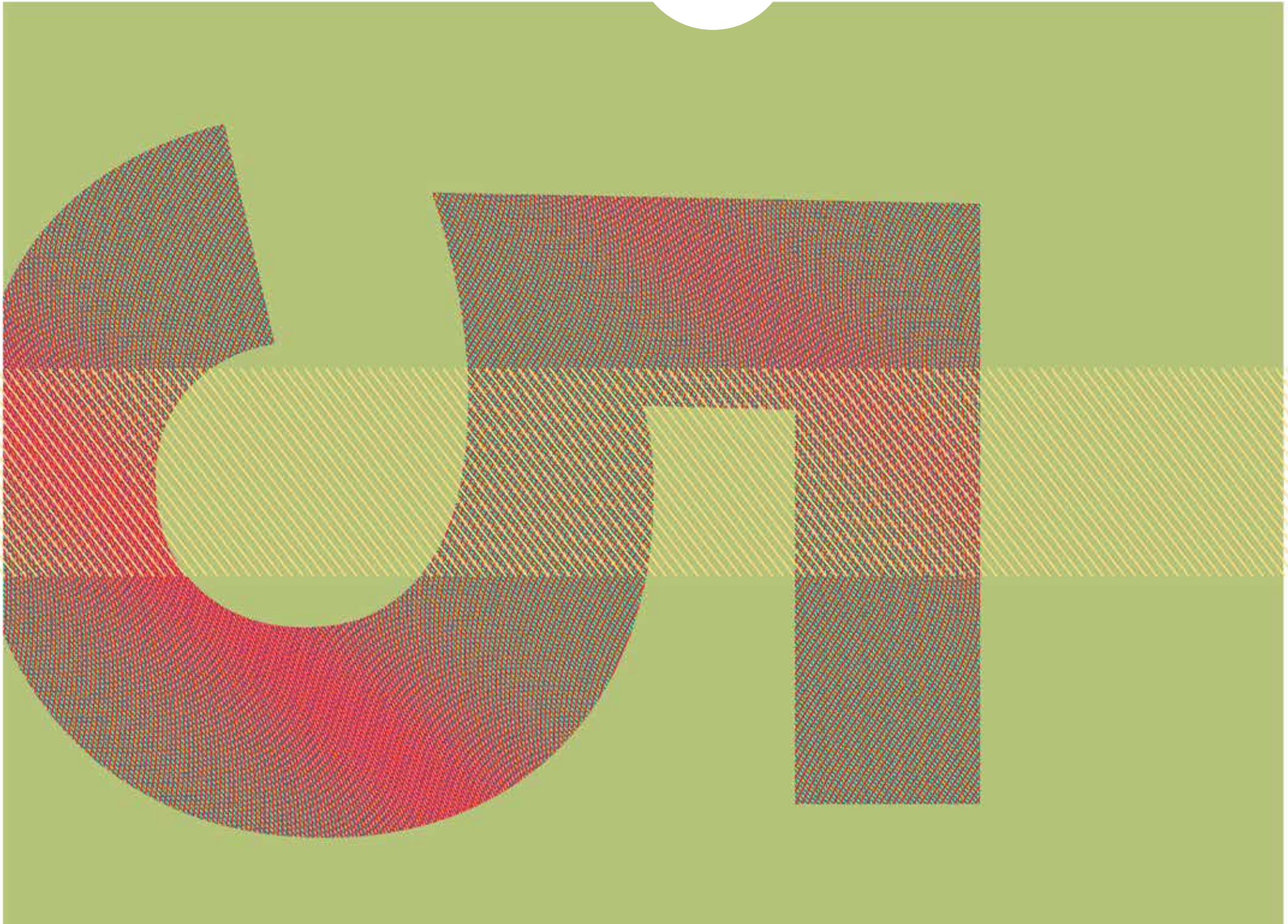
The most frequently-noted situations indicated by reporting entities are cases of individuals acting as intermediaries or illegally exercising a regulated profession[1]. These cases involve individuals collecting funds from numerous other people with the aim of purchasing or reselling virtual currency on behalf of third parties via European trading platforms.

With regard to crowdfunding, Tracfin received 149 Suspicious Transaction Reports involving crowdfunding and online money collection sites in 2016. This figure is up sharply. The increased number of reports in 2016 is due to the fact that a growing number of individuals are using these platforms, while operators are more aware of AML/CFT risks. While the amounts spent on online money collection sites rarely exceed €1,000, individuals' investments in crowdfunding platforms can come to several tens of thousands of euros.

An analysis of Suspicious Transaction Reports submitted in 2016 reveals a wider array of typical cases than in 2015. This reflects the growing number of platforms and users. The simplest way for an individual to use a crowdfunding platform for money-laundering purposes is to invest via the platform in projects that he or she initiated. In one instance, a payment institution detected an individual that had used this method to put more than €250,000 into circulation. Cases of suspected financing of terrorism have been on the radar screen since 2014 and are increasing in number.

The payment institutions and electronic money institutions that partner with crowdfunding platforms appear to be particularly active and aware of the risks that can impact their reputation if their platforms are used for fraudulent purposes.

1 In this case, the regulated profession is that of Banking Transaction and Payment Service Intermediary (IOBSP).



RISK-MITIGATION MEASURES: FRENCH AUTHORITIES ARE ADJUSTING REGULATIONS WHOSE EFFECTIVENESS DEPENDS ON THE QUALITY OF INTERNATIONAL COOPERATION

2016 SAW CONSIDERABLE LEGISLATIVE AND REGULATORY ACTIVITY, NOTABLY TARGETING E-MONEY AND PREPAID CARDS

French legislators took decisive action in 2016 to better regulate the issuance of e-money and the use of prepaid cards[1]. Given the current risks of terrorism, French lawmakers took a step ahead of the EU's AML/CFT legislation when they issued several legal texts aimed at better regulating the use of e-money.

– Since 1 January 2017, all e-money payments carried out in France, either via a card or from a server, are capped at €3,000[2].

– The enactment of the Fourth Directive into French law reduced the anonymity of e-money:

- Now, anyone using a traceable means of payment (i.e. a nominative bank account in an EEA country) to load a physical payment device must show ID for reloads of more than €250 per month. Cash refunds without ID checks are capped at €100.
- Anyone using a non-traceable means of payment (i.e. cash or anonymous e-money) to load a physical payment device must show ID regardless of the amount and for each reload. The sole exception is for "branded" cards usable only in France for the purchase of a limited range of goods and services; these cards can be reloaded with cash without ID checks up to €250 per month[3].
- For online payment services, operators are not required to check ID for online payments made using an EEA bank account to another EEA bank account, for transactions of less than €250, and up to an annual cumulative cap of €2,500[4].

– The use of prepaid cards was restricted under the Act of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing[5]. A decree capped the amounts usable on prepaid cards[6]:

- The maximum amount that can be loaded on a card is €10,000
- Cash reloads are capped at €1,000 per month
- Cash withdrawals or refunds are also capped at €1,000 per month

In addition, e-money providers are legally required to keep records of client information related to activating, loading and using e-money cards or other physical devices[7].

The adjustments made to the e-money legal framework are gradually curbing the inherent risks of prepaid cards. In 2016, the AML/CFT system was also strengthened with Order no. 2016-1635 of 1 December 2016, which enacted Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the so-called Fourth Directive) into French law[8].

While this strengthened legislation is still too recent for its full effects to be measured, this is probably only a first step. The AML/CFT system will remain vulnerable until regulatory requirements and professional practices are strengthened and harmonised at European and international levels.

1 For a detailed presentation of these measures, please refer to Appendix 1.

2 Decree no. 2016-1985 of 30 December 2016, amending Article D.112-3 of the French Monetary and Financial Code (CMF).

3 Article R.561-16 of the CMF.

4 Article R.561-16-1 of the CMF. Articles R.561-16 and R.561-16-1 of the CMF may be amended soon to lower the €250 cap.

5 Act no. 2016-731 of 3 June 2016, known as the "Urvoas Act", and notably its provisions amending Article L.315-9 of the CMF.

6 Decree no. 2016-731 of 3 December 2016, enacted in Article D.315-9 of the CMF.

7 Article L.561-12 of the CMF. As of end June 2017, this provision was not yet clarified in a decree.

8 See Appendix 2.

INCREASED ACCOUNTABILITY FOR THE NEW ENTRANTS IN THE PAYMENT SECTOR IS INDISPENSABLE

The creation of AML/CFT compliance channels within banking institutions gathered pace in the late 1990s/early 2000s. These channels took around five to ten years to become relatively effective. Now, this process has begun for new entrants in the payment services sector. These payment service providers (PSPs), officially recognised in PSD2, do not have the same money laundering risk culture as banking institutions do, and in some cases, they even use the lifting of regulatory constraints as leverage for their development.

NEW PAYMENT SERVICE PROVIDERS: A COMPLIANCE CULTURE THAT NEEDS TO BE STRENGTHENED

Building accountability for new payment service providers on AML/CFT issues is necessary for the AML/CFT system to be effective and coherent. Efforts at regulatory supervision of these new providers must continue.

Payment institutions (PIs) and electronic money institutions (EMIs) must comply with AML/CFT vigilance rules, just like all other reporting entities. The ACPR has already sanctioned certain institutions for (among other reasons) non-compliance with due diligence and customer identification obligations[1].

These obligations are particularly important for PSPs that use networks of agents (for payment services) or distributors (for e-money). Each PSP must ensure that the members of its distribution networks comply with their obligations. These distribution network members are not financial professionals, and are not sufficiently aware of the AML/CFT risk.

For example, the cash sale of prepaid tickets or vouchers to reload electronic wallets sheds light on the limitations of provisions to combat the anonymous use of e-money. Some e-money distributors may give a broad interpretation to the concept of "limited network" for a payment card, so as to avoid having to identify their clients.

Also, competition among PSPs could encourage them, in their dealings with agents and distributors, to prioritise their commercial development over compliance with AML/CFT obligations. In this respect, multi-brand agents and distributors are the most sensitive.

VIRTUAL CURRENCY TRADING PLATFORMS: A COMPLIANCE CULTURE THAT MUST BE CREATED

Trading platforms allow for the conversion between real (fiat) currency and virtual (crypto) currency. These platforms have an important responsibility in terms of client identification. They can decide whether or not to facilitate anonymous transactions in virtual currencies, based on how stringent their client identification procedures are.

Trading platforms and wallet providers are major suppliers of public and private keys for users. These stakeholders bear the same responsibility in terms of client identification as a PSP that offers to open an e-money wallet for a client.

The trading platforms currently established in France collect a varying amount of client information depending on the amount of transactions. For small transactions, platforms identify the client by collecting a name, postal address and bank account information (IBAN or account number), but ID checks are not systematic. For larger transactions, ID checks (i.e. the client must show ID) become systematic based on thresholds that vary for each trading platform.

French legislators have sought to involve these stakeholders in the fight against money laundering and

1 See Sanctions Committee Decision no. 2014-10 of 16 October 2015, and Decision no. 2016-05 of 3 March 2017, accessible on the ACPR's website in the "Sanctions > Jurisprudence" section (some decisions are available only in French).

terrorist financing. Since Order no. 2016-1635 of 1 December 2016, trading platforms registered in France are subject to the AML /CFT system (see paragraph 7°bis of Article L.561-2 of the CMF)[1]. Therefore, they must implement identification and verification procedures, as well as adequate due diligence measures.

On this point, French lawmakers were a step ahead of the EU. This obligation is not included in Directive (EU) 2015-849 (the Fourth Anti-Money Laundering Directive). Talks are currently under way in Brussels to revise the Anti-Money Laundering Directive. This amended Fourth (or Fifth) Directive is likely to encompass virtual currency operators in all EU Member States.

However, subjecting these professionals to the AML/CFT system in France is only a first step. Regulatory supervision of these players is incomplete insofar as they are not subject to any authorisation procedure. So far, no supervisory authority has been designated for this sector. Lastly, the system will still lack effectiveness until similar regulations are implemented internationally.

1 Paragraph 7°bis of Article L.561-2 of the CMF defines virtual currency trading platforms as: "Any person who, in the normal course of its business, acts as a counterparty or intermediary, for the acquisition or sale of any instrument containing non-monetary units in electronic format that may be kept or transferred in order to acquire a good or service, but which does not comprise a receivable held over the issuer."

SUPERVISION OF NEW ENTRANTS IS LIMITED BY THE EUROPEAN PASSPORT AND COMPLICATED BY SECTOR TRENDS

The emergence of new payment sector players, the use of e-money and virtual currencies, and the absence of geographic boundaries are all challenges to the regulatory framework. An effective supervisory scheme must cover the entire chain of stakeholders. Any break in this chain – in geographic terms (i.e. an operator located in a non-cooperative country) or functional terms (i.e. an operator not subject to AML/CFT obligations) – represents a structural weakness in the supervisory scheme.

THE EUROPEAN PASSPORT AND THE FREE PROVISION OF SERVICES REGIME LIMIT SUPERVISION AND CONTROL OF NEW PAYMENT SERVICE PROVIDERS

Considering the digital revolution, French authorities are aware that the effectiveness of the AML/CFT system will remain limited unless it is developed internationally.

Even at EU level, the system's effectiveness is limited by the European passport, which enables operators to distribute their products throughout the EEA if they are authorised in only one Member State. However, the common European framework is not applied uniformly by all Member States. Regulatory authorities of the various EU Member States do not oversee the implementation of AML/CFT obligations for operators with the same degree of effectiveness.

The European passport enables an authorised undertaking from one EEA Member State (i.e. the home country) to offer its services in another Member State (i.e. the host country):

– either on a Freedom of Establishment (FOE) basis, using a permanent establishment (e.g. a branch or an agency) in the host country as a base, and/or by resorting to agents or distributors;
– or as Free Provision of Services (FPS), without being established in the host country, by offering online services.

Under FOE, financial institutions are subject to national regulations for AML/CFT and client protection. In France, establishments that use e-money agents or distributors must name a permanent correspondent, whose role is to be in contact with Tracfin and the ACPR[1].

French supervisory authorities are competent to ensure compliance with these provisions. The ACPR monitors and can sanction branches operating as free establishments, and since 2016, it carries out checks of networks of agents and distributors.

Conversely, under FPS, national supervisors are not competent to monitor foreign establishments operating on their national territory. In this case, the foreign establishments must comply with the regulations of their home countries. When there are doubts, host country authorities can alert their counterparts in home countries. However, the latter are not always cooperative or reactive.

Therefore, FPS constitutes a major risk. At the end of 2016, there were 594 payment or e-money institutions operating in France. Of these, 54 were authorised by the ACPR, 48 were operating under FOE, and 492 were operating under the FPS regime. It is becoming indispensable for the various EEA supervisory authorities to harmonise their level of requirements.

1 Article L.561-3(VI) of the CMF.

	ACPR authorisations	FOE	FPS	Total
PIs	47	34	381	**462**
EMIs	7	14	111	**132**
Total	54	48	492	594

Source: ACPR data as of 1 January 2017

Outside the European Economic Area, the AML/CFT system will remain vulnerable until regulatory requirements become more stringent internationally.

OUT OF ALL STAKEHOLDERS THAT OFFER FINANCIAL SERVICES, AML/CFT REGULATIONS MUST FOCUS SPECIFICALLY ON THOSE WITH THE BEST KNOWLEDGE OF CLIENTS

On 31 August 2017, the Basel Committee published a consultative document on the impact of emerging FinTech firms on the banking market[1]. This document presents five different scenarios for the future of banking, ranging from the best-case to the worst-case scenario. One likely scenario points to incumbent banks being restricted to a role of providing IT and administrative services, to the benefit of major web players which would capture the customer interface.

AML/CFT regulations, if poorly calibrated, could eventually become wasteful and ineffective, creating competition distortions to the detriment of authorised financial institutions. New web players and mobile telephone operators would continue to expand outside the scope of banking regulations and would hold the bulk of customer knowledge data. Conversely, banks and authorised PSPs would bear the obligations of AML/CFT compliance and due diligence, albeit without having enough information available to carry out a detailed analysis of financial flows.

1 Basel Committee on Banking Supervision, *Sound Practices: Implications of fintech developments for banks and bank supervisors*, August 2017.

APPENDIX

APPENDIX 1
MEASURES IMPLEMENTED IN 2016 TO STRENGTHEN THE E-MONEY REGULATORY FRAMEWORK

ALL E-MONEY TRANSACTIONS CAPPED AT €3,000

Since 1 January 2017, all e-money payment transactions have been capped at €3,000.

Six months after the terrorist attacks of January 2015, a simple decree lowered the cap on payments made in cash or in e-money to €1,000 for French residents[1]. This decree encompassed electronic payments, because at that time, anonymous prepaid cards were largely unregulated.

Since then, regulations of prepaid cards were strengthened in 2016 (as explained below). Thus, on 30 December 2016, the cap on e-money payments was raised to €3,000[2]. This decree took effect on 1 January 2017.

AN END TO ANONYMITY

• La règle : la fin de l'anonymat

The rule is that e-money issued and distributed in France can no longer be anonymous, except in specifically defined cases.

Any EMI that wishes to distribute its products in France must comply with Articles L.561-5 and L.561-6 of the CMF. These articles require:

– Identification of the client and the effective beneficiary
– A check of their identities
– Constant monitoring of the coherence of each client's transactions throughout the entire business relationship

Thus, anyone using a non-traceable means of payment (i.e. cash or anonymous e-money) to load a card must show ID regardless of the amount and for each reload.

A payment card loaded using traceable means of payment (i.e. a bank card or via a bank transfer from nominative bank accounts in an EEA Member State) requires an ID check for reloads of more than €250 per month, and for any withdrawal or cash refund of more than €100.

• Very limited exceptions

The exception laid out in Article R.561-16 5° of the CMF provides that e-money devices may depart from the provisions of Articles L.561-5 and L.561-6 of the CMF, i.e. ID checks are not required, if it complies with all of several restrictive conditions:

– It can only be used to pay for goods and services (not to transfer funds or change currencies)
– It can only be used within France
– It cannot be loaded with cash or anonymous e-money (unless its use is restricted to a limited network or a limited range of goods, services or brands)
– Its maximum balance is €250
– Payments are also capped at €250 per month
– Cash withdrawals or refunds are capped at €100 per transaction

Thus, the only cards that can be reloaded by cash without ID checks are those cards issued by certain brands, usable only in France in a predetermined network of stores, for the purchase of a limited range of goods and services, for a maximum monthly amount of €250.

The preparatory work for the amended version of the Fourth Directive lowers these various caps, thus laying out more restrictive conditions for dispensing e-money issuers from fulfilling due diligence obligations.

1 See Decree no. 2015-741 of 24 June 2015, in application of Article L.112-6 of the CMF.

2 See Decree no. 2016-1985 of 30 December 2016, amending Article D.112-3 of the CMF.

• Restrictions for all prepaid cards – even non-anonymous ones

Act no. 2016-731 of 3 June 2016 (strengthening the fight against organised crime, terrorism and their financing, known as the "Urvoas Act") established two provisions to strengthen regulations of prepaid payment cards:

– EMIs must keep records of client information for five years (Article L.561-12 of the CMF): e-money providers are legally required to keep records of client information related to activating, loading and using e-money cards or other physical devices for five years.
– Prepaid cards, even non-anonymous ones, are subject to certain caps (Article L.315-9 of the CMF): a decree stipulates the caps on the maximum amount that can be stored on a card, as well as the amounts that can be loaded, refunded or withdrawn in cash or anonymous e-money.

Decree no. 2016-1742 of 15 December 2016, enacted in Article D.315-2 of the CMF, set these caps. To be marketed in France, an e-money physical device must now fulfil the following conditions:

– The amount that can be stored on a physical payment device (maximum balance) is capped at €10,000.
– Loading a device with cash or anonymous e-money requires an ID check regardless of the amount, and is capped at €1,000 per calendar month in all cases.
– Cash withdrawals are capped at €1,000 per month.
– Cash refunds of the card balance are also capped at €1,000 per month.

• Declaration of cash or cash equivalents transferred into or out of the country

Pursuant to Article L.152-1 of the CMF, reiterated by Article 464 of the French Customs Code, the holder of prepaid cards storing more than €10,000 and entering or leaving a European Union Member State is – in the same way as an individual carrying cash or gold – required to file a customs declaration of cash or cash equivalents.

APPENDIX 2
MAIN PROVISIONS OF ORDER NO. 2016-1635 OF 1 DECEMBER 2016, ENACTING THE FOURTH DIRECTIVE INTO FRENCH LAW

In 2016, the EU's Fourth Directive on AML/CFT was fully enacted into French law with the publication of Order no. 2016-1635 of 1 December 2016. This order strengthens the AML/CFT system by incorporating several provisions into the French Monetary and Financial Code:

• Broadening the scope of the AML/CFT system (Article L.561-2 of the CMF)

– Professionals with the status of Banking Transaction and Payment Service Intermediary (IOBSP) are fully subject to AML/CFT regulations (see paragraph 3° of Article L.561-2).
– Estate agents, who were previously subject to AML/CFT regulations for transactions involving the purchase or sale of properties, are now subject to these regulations for rental activities (see paragraph 8° of Article L.561-2).
– The definition of dealers in precious goods subject to the system has been further specified (see paragraph 11° of Article L.561-2).

Especially, French legislation moved a step ahead of EU talks by incorporating new stakeholders of the digital transformation into the AML/CFT system:

– Crowdfunding platforms that offer loans or collect donations ("crowdfunding intermediaries" or "crowdfunding advisers"; see paragraph 6° of Article L.561-2)
– Virtual currency trading platforms (see paragraph 7° bis of Article L.561-2)

• Enshrining a risk assessment scheme

Each reporting entity must, at its own level, set up a risk analysis process that is appropriate for its business, the kind of products and services it offers, and its client base.

The link between risk analysis and due diligence measures has been strengthened. Risks identified as high must lead to specific due diligence measures, whether these risks involve financial products (e.g. the cap on prepaid card uses) or clients (e.g. with the search for effective beneficiaries).

• Identifying effective beneficiaries and setting up special central registers

The Trade and Companies Register must specify the holders of shares or ownership interests in legal entities.

The Act of 6 December 2013 established a "public register of trusts", which, under terms laid out in a decree, enable free access to various personal data regarding the settlors, trustees and beneficiaries of trusts (see paragraph 2 of Article 1649 AB of the CGI).

According to the Conseil d'Etat, in its Decision no. 400913 of 22 July 2016, later confirmed by the Constitutional Council's Decision no. 2016-591 QPC of 21 October 2016, this register of trusts will only be accessible to the competent authorities. The second paragraph of Article 1649 AB of the CGI was deemed to be unconstitutional because it did not provide the necessary protection for personal freedom.

Enlarging the concept of politically exposed person (PEP) to include national PEPs

• Strengthening Tracfin's capacity to investigate and take action

– Tracfin's right to information has been expanded to include car rental companies, CARPAs (financial settlement funds for lawyers), and all crowdfunding platforms that are not subject to the AML/CFT system.
– Its right of opposition has been extended to ten days, renewable once; this strengthens the possibilities for cooperating with foreign FIUs in order to stop illegal funds from escaping.
– Partnerships between authorities have been enhanced, with a larger list of recipients for Tracfin referrals (including the French Government Audit Office and Regional Audit Offices, the High Authority for Transparency in Public Life, the French Anti-Corruption Agency, the Strategic Information and Economic Security Department, etc.)
– The confidentiality of Suspicious Transaction Reports is protected.

Tracfin

Unit for intelligence processing and action against illicit financial networks

Publication Director: Bruno Dalles
10 rue Auguste Blanqui 93186 MONTREUIL - Tel: +33 1 57 53 27 00

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

Maquette : Studio graphique SIRCOM