2017–2018
MONEY LAUNDERING AND TERRORIST FINANCING RISK TRENDS AND ANALYSIS

TRACFIN
TRAITEMENT DU RENSEIGNEMENT ET ACTION CONTRE LES CIRCUITS FINANCIERS CLANDESTINS

MINISTÈRE DE L’ACTION ET DES COMPTES PUBLICS
CONTENTS

CUTTING OFF SOURCES OF TERRORISM FINANCING IDENTIFIED IN FRANCE 9
DEPARTURE AND RETURN OF COMBATANTS 11
MONEY COLLECTION NETWORKS FOR JIHADi GROUPS 12
MONEY COLLECTION NETWORKS IN FRANCE 12
USING NEW ONLINE PAYMENT SERVICE PROVIDERS 13
"NO MONEY FOR TERROR": AN INTERNATIONAL CONFERENCE HELD ON 25-26 APRIL 2018 14

INCREASING THE TRANSPARENCY OF NON-PROFIT ORGANISATIONS 17
HOW THE NON-PROFIT SECTOR OPERATES 18
A LACK OF TRANSPARENCY IN THE MANAGEMENT OF SOME NON-PROFIT ORGANISATIONS 19
AN INOPERATIVE NATIONAL REGISTER 20
STRENGTHENING THE LEGAL, FINANCIAL AND ACCOUNTING FRAMEWORK FOR NON-PROFIT ORGANISATIONS 21

PREVENTING MONEY LAUNDERING THROUGH BANKING CHANNELS 23
CONSPIRACY TO DEFRAUD: METHODS ALREADY IDENTIFIED BY TRACFIN STILL PERSIST 25
FALSE TRANSFER ORDERS: VOLUMES APPARENTLY DECLINING BUT RISKS STILL HIGH 25
FOREX, DIAMOND AND RARE EARTH TRADING: A SECOND WAVE 26
THE CRYPTO ASSET SPECULATIVE BOOM IN LATE 2017 SPARKED A WAVE OF FALSE CRYPTO ASSET INVESTMENT OFFERS 26
WHITE CERTIFICATE (CEE) FRAUD: TIGHTER REGULATIONS FORCE FRAUDSTERS TO CHANGE TACKS 27
SEPA DIRECT DEBIT FRAUD: SECURITY FLAWS PERHAPS NOT AS BAD AS FEARED 30
TAX EVASION, SOCIAL SECURITY FRAUD, ACCOUNTING FRAUD OR CUSTOMS FRAUD COMMITTED BY COMPANIES THAT HAVE A LEGITIMATE ECONOMIC ACTIVITY 30
SHELL COMPANY NETWORKS REMAIN THE MAIN MEANS FOR MONEY LAUNDERING THROUGH BANKING CHANNELS 31
TWO SECTORS WITH HIGH MONEY LAUNDERING RISK: CONSTRUCTION AND VEHICLE TRADING 33
CONSTRUCTION SECTOR SMES 33
VEHICLE TRADING 35
STEMMING THE STEADY INCREASE IN RISKS RELATED TO ONLINE PAYMENT SERVICE PROVIDERS

PAYMENT AND ELECTRONIC MONEY SERVICE PROVIDERS (PS/EMSPS) ARE INCREASINGLY PART OF MONEY LAUNDERING CIRCUITS

THE USE OF PS/EMSPS IN SHELL COMPANY NETWORKS USED TO LAUNDER MONEY

ONLINE CREDIT CARD PAYMENT COLLECTION SOLUTIONS USED AS A SCREEN TO CONCEAL THE TRACEABILITY OF FLOWS

PREPAID CARDS ISSUED BY PS/EMSPS REVEAL FLAWS IN HOW REGULATIONS ARE APPLIED

THE ONLINE FUNDRAISING PLATFORM SECTOR ALSO Requires PS/EMSPS TO PERFORM AML/CFT DUE DILIGENCE

AML/CFT RISKS IDENTIFIED BY TRACFIN WITH RESPECT TO ONLINE FUNDRAISING

PS/EMSPS RESPONSIBILITIES IN DETECTING AML/CFT RISKS RELATED TO ONLINE FUNDRAISING TRANSACTIONS

PAYMENT INITIATORS, AS DEFINED IN THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2), MAY CURB KYC EFFORTS BY ACCOUNT CUSTODIANS

HOW EUROPEAN AND FRENCH PUBLIC AUTHORITIES SHOULD REACT IN ORDER TO BETTER MANAGE PS/EMSPS RISKS

STRENGTHEN THE ABILITY OF NATIONAL SUPERVISORS TO MONITOR PS/EMSPS

EXPAND NATIONAL CENTRALISED BANK ACCOUNTS REGISTRATION (FICOBA IN FRANCE)

ENACTING DIRECTIVE (EU) 2018/843

HARMONISING NATIONAL LEGAL SYSTEMS AND THEIR IMPLEMENTATION WITHIN THE EU

REGULATING CRYPTO-ASSETS AT DOMESTIC AND INTERNATIONAL LEVELS

PROVEN AML/CFT RISKS OF CRYPTO-ASSETS

A SHARP RISE IN TRACFIN’S CRYPTO-ASSET-RELATED ACTIVITIES

THE MAIN RISKS IDENTIFIED BY TRACFIN IN LIGHT OF STRS RECEIVED

COMBINED PAYMENT SERVICES IN LEGAL TENDER AND THOSE IN CRYPTO-ASSETS

THE RAPID GROWTH IN ICOS: THE NEED FOR A REGULATORY FRAMEWORK

TRACFIN IS ADAPTING ITS ORGANISATION AND RESOURCES TO BETTER MONITOR THE CRYPTO-ASSETS SECTOR

A DEDICATED TEAM OF ANALYSTS

DISCUSSIONS WITH REPORTING ENTITIES ABOUT RISK CRITERIA

CONVERGENCE OF INTERNATIONAL DISCUSSIONS TOWARDS INTRODUCING APPROPRIATE REGULATION
DEVELOPING AML/CFT DUE DILIGENCE IN THREE SECTORS:
FINANCIAL MARKETS, THE ART MARKET AND LIFE INSURANCE MARKET

MONEY LAUNDERING ON SECURITIES MARKETS: MANIPULATION
OF THE SHARE PRICES OF LISTED COMPANIES;
LAUNDERING THE PROCEEDS OF INSIDER TRADING

PRICE MANIPULATION ON ORGANISED SECURITIES MARKETS
LAUNDERING THE PROCEEDS OF INSIDER TRADING

THE ART MARKET IS STILL HIGHLY VULNERABLE TO MONEY LAUNDERING RISKS
A THRIVING MARKET CHANNELLING NUMEROUS RISKS
ONLINE AUCTIONS AND SALES: A GROWING RISK
BOLSTER THE OVERSIGHT OF PROFESSIONALS: AUCTIONEERS, VOLUNTARY AUCTION HOUSES,
ANTIQUES DEALERS AND GALLERY OWNERS
RECAST THE LEGAL ARRANGEMENTS FOR THE INVENTORY REGISTER (LIVRE DE POLICE) AND ORGANISE
FOR IT TO BECOME PAPERLESS
CONSOLIDATE THE REPORTING OBLIGATIONS OF
THE NON-LIFE INSURANCE SECTOR

EXPLICITLY DEFINE POLITICALLY EXPOSED PERSON (PEP)
in French law to bolster the fight against corruption
LAUNDERING IN FRANCE OF THE PROCEEDS OF THE MISAPPROPRIATION
OF PUBLIC FUNDS COMMITTED ABROAD
CORRUPTION OF A FOREIGN PUBLIC OFFICIAL
AS PART OF MAJOR INTERNATIONAL CONTRACTS
THE DEFINITION OF DOMESTIC PEPS SHOULD BE MORE SPECIFIC

CONTRIBUTING FIGHT TAX EVASION, SOCIAL SECURITY FRAUD
AND CUSTOMS FRAUD: A CORE TRACFIN ASSIGNMENT
TRACFIN’S VALUE ADDED IN FIGHTING TAX EVASION
LEGAL ENTITIES: VAT FRAUD BY FORGERY (DEDUCTIBLE VAT)
INDIVIDUALS: ABUSE OF RIGHTS REGARDING THE TAXATION OF INVESTMENT INCOME
AND DEATH DUTIES
AVOIDANCE OF TRANSFER DUTY
PERSISTENT SOCIAL SECURITY FRAUD
CONTRIBUTIONS FIGHT CUSTOMS FRAUD

SUMMARY OF THE MAIN RECOMMENDATIONS
ACRONYMS
Every year, Tracfin assesses the main risks of money laundering and terrorist financing observed in France based on the information it receives.

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, which encourages all Member States to take appropriate steps to assess the risks of money laundering and terrorist financing affecting them. The EU has carried out its own risk assessment, which it published in July 2017.

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 reference materials 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 anyone interested in AML/CFT (students, researchers, journalists, etc.).

This “2017–2018 risk trends and analysis” report builds on the prior reports published in 2015 and 2016. It endeavours to provide a more in-depth look at certain key topics (including risks related to NGOs, shell company networks, the build-up of new payment service providers and cryptocurrency market regulations), to shed light on certain business sectors (such as construction, vehicle sales, financial markets and the art market) and to remind readers of Tracfin’s core remit (combating the financing of terrorism, fighting corruption, and tackling tax, social security and customs fraud). This report lays out a series of ten recommendations.

It coincides with the interministerial national risk analysis process, which the AML/CTF Advisory Board (COLB) has spearheaded since late 2016 in coordination with all relevant government departments and supervisory authorities.

Tracfin’s successive reports and the COLB’s work are paving the way for the FATF to carry out its audit of France. The auditing process is scheduled to begin in late 2019. The FATF’s auditors will carry out an in situ audit in 2020, with a final audit report to be presented for approval during a plenary meeting of the FATF in 2022. The FATF audit is a crucial event for France’s entire AML/CFT system, and Tracfin will devote considerable resources to this process.

\[\text{Directives (EU) 2015/849.}\]
CUTTING OFF SOURCES OF TERRORISM FINANCING IDENTIFIED IN FRANCE
Since 2015, the fight against terrorism and its financing has changed scales. Tracfin has continued its efforts, proving the importance of financial intelligence within a comprehensive anti-terrorism system. Tracfin rapidly provides detailed, factual information about relevant individuals or entities of various profiles.

In 2017, the Unit processed 1,379 declarations involving suspicions of terrorism financing, i.e. a 17% increase from 2016. At the other end of the processing chain, 685 cases were outsourced, vs. 396 in 2016, i.e. a 73% rise. Of these 685 cases, 459 were referred to intelligence services (primarily to a dedicated inter-agency unit) and 226 notes were set to the courts or to the criminal investigation departments tasked with fighting terrorism. With regard to the judiciary, Tracfin has a close working relationship with the anti-terrorist section of the Paris public prosecutor’s office.

The main threats detected by Tracfin in France have not changed substantially and remain quite serious. These threats involve enemy combatants travelling to or returning from the war zone in the Middle East, as well as money collection networks in France benefiting Jihadi groups. Tracfin also notes that certain non-profit organisations with radical ties may carry out suspicious financial transactions (such as cash transactions or misappropriation of funds).

**DEPARTURE AND RETURN OF COMBATANTS**

Following the Islamic State’s losses of territory in the Iraqi-Syrian war zone, the number of Jihadi fighters leaving for the Middle East has declined. However, Tracfin continued to handle important cases throughout 2017.

**Case study no. 1: A Jihadi fighter leaves for the war zone**

A bank identified one of its clients as fulfilling several warning signs for radicalisation and a risk of terrorist financing. This client, a male less than 30 years old, had suddenly changed his way of dressing and taken trips to high-risk countries abroad, then purchased tickets for Turkey and withdrawn almost the full balance from his account. The bank also determined that this client had, in the past, ordered two bank transfers to a non-profit organisation that was later shut down by the authorities, with its assets frozen.

Observing a cash withdrawal in a country neighbouring the war zone, Tracfin immediately alerted its partners in the intelligence community. A connection was established between the French bank’s client and a foreign fighter travelling under a false identity who had recently arrived in a training camp in the Middle East.

The financial investigation confirmed ties between this individual and two other terrorists, both members of a terrorist cell dismantled in the 2000s who were given ten-year prison sentences.

Logically, the terrorist risk should focus on the “returnees”, namely, French nationals who have gone to the war zone and wish to return to France. Their return to France depends on several parameters that are not easily predicted. For the time being, the number of returnees observed has been limited: around 30 in 2016, around ten in 2017 and about the same number in autumn 2018. Several of these cases involve families with minor children.
MONEY COLLECTION NETWORKS FOR JIHADI GROUPS

In its 2016 “risk trends and analysis” report, Tracfin highlighted the risks pertaining to money collection networks. The Unit focused considerable efforts on detecting and identifying these networks in 2016 and 2017. These networks are still active in France. They are in constant flux and they use various modes of payment.

Money collectors act as middlemen or financial facilitators. They use money transfer companies to centralise cash in Europe, and then transfer it to countries bordering the war zone. The transferred funds are then withdrawn in cash and carried across the border to the final recipient.

Some money collectors are residents of France. Sometimes they run businesses that serve as a cover for terrorist financing transactions.

MONEY COLLECTION NETWORKS IN FRANCE

Case study no. 2: Identifying a money collection network in France

A reporting entity identified transfers of funds from several countries including France to a certain “Mr Y”. This individual is known to intelligence units and has been identified by the United Nations Security Council as a representative of an extremist religious organisation with ties to Al-Qaeda, tasked with channelling fighters to the Middle East war zone. He has been banned from entering France.

According to the information in Tracfin’s possession, “Mr Y” has collected a total of $45,000 over four years through some 50 transactions from 12 countries.

A portion of this individual’s network in France was mapped by using the Systematic Communication of Information (COSI) system, along with data gathered from payment institutions, banks and credit institutions, and Tracfin’s foreign partners.

Tracfin identified a dozen donors in France, particularly in eastern France and in the Paris region. All of these donors had police and gendarmerie records for various kinds of offences: foreign nationals living in France without proper documentation, illegal firearm possession, theft and handling stolen goods, undeclared work, etc. One of these individuals was on probation for conspiracy to commit a crime in relation to a terrorist undertaking. The map of financial flows revealed that these individuals were acting as middlemen: they collected small sums from their family and friends, and then remitted these amounts to “Mr Y”.

Amongst these intermediaries, Tracfin identified a married couple living in a mid-sized town. They were already known to law enforcement for having carried on an undeclared business involving the buying and selling of vehicles and the use of sizeable amounts of cash. The husband was working as a driver. Over three years, the couple’s bank accounts recorded deposits of cheques totalling €160,000, plus €70,000 in cash deposits. The couple declared very low income on their tax returns.

A portion of the money from their undeclared business was sent via money transfer to a second money collector, a certain “Ms X” living in a country bordering a combat zone in the Middle East. “Ms X” was acting as an assistant to “Mr Y”. Tracfin’s investigations revealed that at least $26,000 had been sent to “Ms X” over three years.
Investigations: cash transfers from France and other EU Member States revealed

Mr Y
identified as a member of an Al-Qaeda-linked organisation

Ms X

Friends and family

$45,000

Friends and family

$26,000

$45,000

Friends and family

USING NEW ONLINE PAYMENT SERVICE PROVIDERS

Money collectors may also use various online payment services, as well as crowdfunding platforms and online money collection sites. Many international payment service providers allow money to be sent easily, quickly, and in some cases, with a certain degree of anonymity. These services can complicate the supervisory tasks of national authorities. These risks, described in detail in Chapter 4 of this report, are particularly relevant in cases of terrorism financing. International cooperation among financial intelligence units (FIUs) is the first step to tackling this issue.

Case study no. 3: Money transfers via a recently-created European electronic money institution, with cooperation among FIUs

Several credit institutions alerted Tracfin about their clients paying for language and religious lessons and making brief visits to at-risk countries. Tracfin processed these alerts and identified an individual with a suspicious profile. He had recently begun to dress differently. The deposits credited to his bank accounts gave no specific information on his occupation or possible employer. On the debit side, there were payments related to stays in a high-risk country.

Tracfin’s financial investigation determined that this individual had been convicted and incarcerated for domestic violence. Following his prison sentence, intelligence services had identified him as belonging to the radical Islamist movement. He was teaching classes in a Salafi Islamic school in the suburbs of Paris.

An investigation of his financial transactions revealed that he had received many transfers from a European e-money institution, totalling nearly €30,000 over 18 months.

Tracfin requested information from the FIU of the country in which the e-money operator was licensed. The information received showed much larger financial flows that could not be detected from France. The individual being investigated had two accounts on the online platform, and had received more than 3,500 payments in four years from more than 500 different individuals, for a total amount of €165,000.

The payment platform used by this individual only records minimal data about those making payments (i.e. their names and e-mail addresses, but not their birth dates or other identifying information). This made an in-depth investigation more difficult.

The findings of Tracfin’s investigation were sent to France’s inter-agency unit dedicated to combating terrorism.
The fight against terrorism and its financing is at the forefront of international law enforcement priorities. The risks identified by Tracfin – such as the use of new payment service providers or the loopholes in French legislation on non-profits – were highlighted during an international conference on combating the financing of terrorism, held on 25 and 26 April 2018 in Paris and organised at the initiative of President Emmanuel Macron.

France’s Ministers of the Interior, of Justice, of Foreign Affairs, and of Government Action and Public Accounts invited their counterparts from 70 countries, as well as executives from nearly 20 international and regional organisations and specialised agencies, to work together to launch a joint action plan against terrorist financing.

Alongside the directors of other agencies in the French intelligence community, the director of Tracfin moderated a roundtable for the CFT experts, members of foreign government delegations and organisations attending the event.

The conference culminated in a final statement in which the represented countries committed to improving intergovernmental cooperation and making financial intelligence more effective. This statement included a ten-point commitment covering financial flow mechanisms, the new methods of funding terrorist organisations, and removing hurdles to international cooperation.
SUMMARY OF THE TEN COMMITMENTS IN THE FINAL STATEMENT OF THE « NO MONEY FOR TERROR » INTERNATIONAL CONFERENCE, APRIL 2018

1) Further reinforcing the domestic legal and operational frameworks to collect, analyse and share information by national authorities (defining the criminal offence, coordination between national agencies and between intelligence agencies and the courts, FIU resources, dialogue with the private sector, etc.).

2) Fighting anonymous financial transactions (undeclared remittance systems, hawalas, cash payments, prepaid cards and other anonymous means of payment).

3) Enhancing the traceability and transparency of non-profit organisations and charitable funds.

4) Anticipating and addressing the risk of new financial instruments being abused (crypto-assets).

5) Partnering with the private sector, especially the tech industry, in the fight against terrorist financing (risks related to online collecting of funds; promoting involvement by the main web platforms and social media networks; adopting robust guidelines for crowdfunding and payment services).

6) Reiterating the usefulness of international and national asset freezing and seizure mechanisms.

7) Bolstering the effectiveness of international cooperation.

8) Supporting the authority, visibility and resources of the FATF and FATF-Style Regional Bodies (FSRBs).

9) Strengthening the collective engagement towards States that fall short of standards or that lack capacity.

10) Maintaining our common mobilisation against terrorist financing.
INCREASING THE TRANSPARENCY OF NON-PROFIT ORGANISATIONS
In the wake of the « No money for terror » conference held in April 2018, it became apparent that rules for non-profit organisations needed to be revised, and notably for legal entities or other organisations whose main activity consists of raising funds and financing charitable, religious, cultural, educational, social or community projects. An examination of the non-profit sector from a financial perspective reveals that the rules for non-profit organisations generally lack transparency with regard to their setup, public disclosures and financial ties. A revision of the rules would offer the advantage of preventing not only the risks of terrorism financing, but also the risks of radicalisation. Non-profit organisations can also present risks of misappropriation of public funds.

HOW THE NON-PROFIT SECTOR OPERATES

The freedom of association is a fundamental freedom acknowledged in the French Constitution and basic laws of the French Republic. The Act of 1 July 1901 and the enforcement decree of 16 August 1901, the two main legislative texts governing non-profit organisations, are chiefly aimed at organising how a public freedom is exercised. They do not set up a binding legal framework in terms of non-profit management. Any individual can set up a non-profit organisation without having to obtain prior administrative authorisation. All individuals can also decide freely whether or not they wish to join a non-profit organisation, and they can choose to leave an organisation at any time.

Undeclared non-profit organisations have no legal capacity. They cannot accept donations or receive public subsidies. Any assets they might hold are the joint property of their members.

Conversely, declared non-profit organisations have legal personality. They can accept donations and receive subsidies. Legal personality can be simplified or complete.

So-called “simplified” non-profits have limited legal personality (they cannot receive inter vivos gifts or bequests; property assets must strictly comply with the non-profit’s purpose).

Non-profit organisations with complete legal personality are public interest organisations. Donations to these organisations give rise to tax breaks (within certain limits) for the taxpayer making the donation. Public interest organisations can also receive bequests and own real estate. As of January 2018, there were 1,890 public interest organisations in France.

There are around 1.3 million declared non-profit organisations in France. These organisations are primarily active in sports, leisure and cultural activities, or to defend special causes, rights or interests. Most non-profits operate with small budgets and rely on volunteer labour, whereas a large proportion of the non-profit sector’s total budget belongs to large organisations that employ staff and are especially present in the sectors of social action, humanitarian or charitable causes, social housing, medical and social work, healthcare, teaching and vocational training.

---

1 According to the FATF’s definition in “Best practices paper on combating the abuse of non-profit organisations (recommendation 8)”, p. 9 – FATF – June 2015.

2 A non-profit organisation is granted – or stripped of – “public interest” status by decree adopted after consultation with the Conseil d’État.
A LACK OF TRANSPARENCY IN THE MANAGEMENT OF SOME NON-PROFIT ORGANISATIONS

The information in Tracfin’s possession reveals a lack of transparency for some non-profit structures. Some non-profit directors use the flexible regulations to turn their organisations away from their initial purpose and carry out suspicious financial transactions, in particular, cash deposits and withdrawals that are unusually large in light of the purpose and size of the organisation, transfers of money to high-risk countries with no identified recipient, or expenses unrelated to the organisation’s purpose.

Therefore, the non-profit sector is exposed to several kinds of risks:

– A criminal risk when funds are misappropriated, notably breach of trust. Breach of trust is one of the most frequently-suspected offences identified in Tracfin’s investigations, leading to around a hundred judicial referrals annually, with breach of trust as the main presumed offence.

– Tax risk when the organisation does not comply with its non-profit purpose and operates in the same conditions as a commercial firm in the market sector. Some non-profit organisations gradually evolve towards lucrative operations as they develop their activity, whereas others are deliberately created as fronts for a commercial activity.

– Labour risk when the non-profit organisation uses undeclared workers and pays its staff without reporting to URSSAF.

– Risk of foreign interference – a risk that cannot be ruled out in the case of certain non-profit organisations that have opaque funding sources.

Case study no. 4

A non-profit organisation purchased a plot of land for €500,000 in order to build a cultural centre. Most of its expenditure was normally for paying for the building works and other operating expenses.

The organisation developed its project and collected money from a number of other non-profits, commercial firms and private donors, involving a high proportion of cash donations of uncertain origin. Thus, this non-profit organisation received more than 40% of its funding from cash donations of unexplained origin which may have concealed money laundering.

The donors included:

• Individuals known to the police and gendarmerie for financial crime and/or ordinary offences;

• companies reported to Tracfin for unusual cash payments in sectors known for presenting a high risk of tax evasion (such as food shops, automobile sales, taxi companies or construction companies);

• certain religious organisations, some of which are known for having ties to the radical Islamist movement.

1 For the definition of the offence of breach of trust: See Articles 314-1 to 314-4 of the French Criminal Code.

2 However, not all of Tracfin’s judicial referrals for presumed breach of trust involve non-profit organisations.

3 Whether or not an organisation is really operating on a non-profit basis can be determined using the “four Ps” method: “Product”, when the products or services of an organisation are equivalent to those that can be found in the market sector (e.g. language courses); “Price”, when the organisation sets prices that allow it to turn a profit; “Personnel”, when the actual activities of its staff correspond to commercial activities; “Publicity”, when the organisation carries on promotional activities such as advertising.
Case study no. 5

A cultural non-profit organisation’s purpose was to deliver online courses on religious traditions to the general public. Over a year, it received cheques and bank transfers totalling almost €130,000 from individuals who wanted to sign up for these lessons. In addition, the organisation launched an appeal on a fundraising website, stating that it wanted to purchase offices.

Its chairman was known to the intelligence services for suspected ties with the radical Islamist movement. He was also known to the police for the offences of armed robbery, theft with aggravated assault, and purchasing an attack dog. His wife was the organisation’s secretary.

An analysis of the organisation’s bank account showed more than €40,000 in personal expenses (in supermarkets, petrol stations, clothing shops, neighbourhood shops, etc.) unrelated to the organisation’s purpose.

AN INOPERATIVE NATIONAL REGISTER

The non-profit organisations suspected by Tracfin or the judicial authorities of having committed money laundering or misappropriation offences benefited from the fact that there is no central register of information about their directors.

When a non-profit organisation registers with the prefecture, it is recorded in the National Register of Associations (RNA). However, this register is not managed effectively. In practical terms, it is not centralised at national level. Each prefecture manages a list of non-profit organisations within its territory. In addition, the identities of a non-profit organisation’s directors can be given on a self-reporting basis only. No checks are made of a chairperson or treasurer’s ability to manage a non-profit organisation.

The register of beneficial owners, mandatory under the EU’s Fourth Anti-Money Laundering Directive and enacted into French law, will not solve this problem. From a legal standpoint, this register is supposed to include the legal representatives of non-profit organisations. Yet in operating terms, it does not appear to be adapted to non-profit organisations. For legal entities other than corporations and mutual funds, the definition of “beneficial owner” is governed by Article R.561-3 of the French Monetary and Financial Code. This definition was initially devised for trusts. It is based on the concept of an individual controlling more than 25% of the legal entity’s assets. This definition is hard to adapt to the non-profit sector and is therefore imprecise.

2 Article R.561-3 of the Monetary and Financial Code refers to a legal instrument signed by the founders that would identify the beneficial owner. However, for a non-profit organisation, this instrument may not exist or may not be public.
STRENGTHENING THE LEGAL, FINANCIAL AND ACCOUNTING FRAMEWORK FOR NON-PROFIT ORGANISATIONS

The current legal framework for non-profit organisations is inadequate given the risks that they are exposed to. To reconcile the freedom of association and transparency of economic life, Tracfin suggests: (i) requiring non-profit organisations to sign up on a single register, (ii) creating new accounting obligations, and (iii) lowering the threshold for non-profit organisations that receive public subsidies to have their accounts certified by including the concept of ML/FT risk.

Require non-profit organisations to sign up on a single digital register

To ensure better supervision of non-profit organisations, their directors and articles of association, it is necessary to create a single dedicated, centralised digital register. Non-profit organisations would be given a SIREN or SIRET number, associated with mandatory items of information: identities of directors and treasurers, articles of association, filings of amended acts, and know-your-client data such as a company registration certificate (kbis).

Under this proposal, the National Association of Commercial Court Registrars (CNGTC) could be the main entry point for managing this register and could charge registration fees tailored to the non-profit sector.

Require publication of annual financial statements

To ensure better tracking of the source of funding and the use of funds, non-profit organisations – especially those that accept public donations and public subsidies – should have to publish annual financial statements. Thus, it would be relevant for these non-profit organisations to publish a balance sheet and income statement on an annual basis, including notes on gifts, bequests and donations above a certain amount (including those from overseas). This information would then be added to the single register.

Lower the threshold for account certification of non-profit organisations

Lastly, under current rules, non-profit organisations only have to have their accounts audited if they receive public subsidies of €153,000 or more. This threshold is too high to ensure proper supervision. Tracfin proposes eliminating this threshold and replacing it with a special legal audit, including AML/CFT checks, which could be defined and applied for all non-profits receiving public money.
According to information received and processed by Tracfin, there are four main sources for undeclared or illegal capital flows in France that may be subject to money laundering through banking channels. These four sources are:

- scams, generally carried out by organised groups of criminals (including fake bank transfers, fraudulent investment websites, white certificate fraud, scams using fake advertisements, etc.)
- tax evasion, social security fraud, accounting fraud or customs fraud committed by companies that have a legitimate economic activity (such as undeclared work, undeclared business activity, under-declaring company turnover, misuse of company assets, imports/exports without filing customs declarations, etc.)
- misleading or unfair trading practices (such as abuse of weakness or breach of trust, often involving home repair services)
- VAT fraud, a cross-cutting offence that is often carried out in combination with one of the three other categories.

The main channels for money laundering are networks of shell companies – or letterbox companies – that collect the illegal or undeclared funds and then rapidly transfer them overseas. Illegal funds collected in France are generally transferred to relay bank accounts in Eastern Europe, then transferred on to Asia, or withdrawn as cash in France using bank cards connected to foreign accounts. Some Western European countries have started to appear as a first relay for illegal funds. Some Middle Eastern countries are emerging as a destination for the second chain of relay accounts.

Dismantling these international networks mainly depends on cooperation between the relevant professionals and government departments, and efficient international cooperation among FIUs.

CONSPIRACY TO DEFRAUD: METHODS ALREADY IDENTIFIED BY TRACFIN STILL PERSIST

Criminal organisations specialised in large-scale scams frequently develop and test new methods of fraud. Despite preventive and law enforcement actions, scams that first appeared in the early 2010s continue to cause substantial economic damage. The most recently-developed scams add to and compound this phenomenon.

Often the same criminal networks are involved in various kinds of scams (e.g. fake bank transfers, diamond fraud, forex and bitcoin fraud). However, no network holds a monopoly because a successful fraud method quickly attracts “interested competitors”.

FALSE TRANSFER ORDERS: VOLUMES APPARENTLY DECLINING BUT RISKS STILL HIGH

False order transfers involve the fraudulent substitution of bank account details so that the fraud victims’ transfer orders go to bank accounts opened by the fraudsters in another country. This kind of fraud may consist of stealing the identity of a supplier or a factoring company by changing its bank account details directly in the fraud victim’s servers (in this case, hacking is also involved) or by sending a letter or e-mail informing the victim of a change in account details. False order transfers generally target entities in the private or public sectors, regardless of their size or business sector. Individuals may also be targeted.

Criminal investigators’ statistics show that the trend in false order transfers has declined over the past four years,

---

1 For a description of false transfer order fraud, see Tracfin’s “2015 ML/TF risk trends and analysis” report, pp. 20-21.
after peaking in 2014 at nearly 900 cases of fraud or attempted fraud, followed by 640 cases in 2016 and 430 in 2017. Tracfin has not observed a significant decline and has received between 70 and 120 reports of such fraud per year since 2014. False order transfers still occur, and sizeable amounts of money continue to be stolen from companies, especially small businesses that may suffer substantial harm. Fraudsters appear to be focusing on smaller-scale transactions, but may be broadening their reach and targeting new victims (such as government accountants, especially in the health sector).

**FOREX, DIAMOND AND RARE EARTH TRADING: A SECOND WAVE**

Since 2015, false advertisements for online investments have been on the rise: forex trading scams (i.e. trading in binary options on the forex market via unauthorised websites), followed by false investment offers for diamonds or rare earths.¹

Despite numerous warnings issued by the authorities (including the AMF, ACPR, DGCCRF, Tracfin and the police), these methods continue to be used. Cases of forex trading fraud have declined, but cases involving fraudulent diamond and rare earth investments continued apace in 2017.

The lifespan of this kind of fraud has been extended by what might be called a “second wave”. In this second wave, fraudsters contact their victims again, claiming to be acting in an official capacity. They tell the victims that they can recover their money after paying a cash advance – in some cases to a non-profit organisation created for that purpose.

– Victims of forex trading fraud, after having invested and lost their money, were contacted again by individuals claiming to represent law firms, government agencies or public-sector entities, including Tracfin. These individuals explained to the victims that their money would be returned immediately but they had to pay an additional amount to cover certain administrative fees.

– Victims of false diamond investments, led to believe that they had made high-yield investments in diamonds that were being stored in a free trade zone to avoid payment of VAT, were then contacted by the fraudsters and asked to pay VAT of 20% on their investment, which allegedly was now owed because of a “new EU Directive”.

The money collected was then transferred through the same money laundering channels as for the initial fraudulent schemes, via bank accounts in Eastern Europe.

**THE CRYPTO ASSET SPECULATIVE BOOM IN LATE 2017 SPARKED A WAVE OF FALSE CRYPTO ASSET INVESTMENT OFFERS**

Forex trading scams appear to have given way to scams involving crypto asset investments. The model is identical: unlicensed investment firms offer individuals an opportunity to purchase crypto assets (primarily the bitcoin, ether or ripple cryptocurrencies).

The fraudsters create a website encouraging individuals to invest in crypto assets – but with no registration with market watchdogs. In parallel, they open bank accounts, often with online banks in European countries such as the Netherlands or the UK, or even in French banks. They conceal the real purpose of their activity from their bank.

Then, they run Internet advertising campaigns or telemarketing campaigns to promote their website, emphasising that their investment products are simple, quick and very profitable.

After retail investors have transferred their money to the designated bank account, they may see some initial return on their investments to convince them that the investments are legitimate (like a Ponzi scheme). However, the website creators rapidly transfer most of the funds overseas and break off all contact. The individuals who have lost their money have no recourse. The lifespan of these websites can be very brief, limiting the possibilities for the banks that hold the accounts to take action.

These simple scams became more frequent with the speculative boom in bitcoin prices in the last quarter of 2017. The Autorité des Marchés Financiers (AMF) issued several warnings, notably on 22 February and 5 July 2018, including the names of the fraudulent websites.

Such scams have also been made easier since 2017 with the development of Initial Coin Offerings (ICOs).

**WHITE CERTIFICATE (CEE) FRAUD: TIGHTER REGULATIONS FORCE FRAUDSTERS TO CHANGE TACKS**

The White Certificate system (CEE) was developed in France in 2006 to give energy sector companies (known as “mandatory participants”) an incentive to carry out energy savings work (or have such work carried out) for companies, social housing providers or private households. The public authorities assign a quota of White Certificates to be obtained (and thus a quota of energy savings work to be carried out) for each mandatory participant based on its activity.

To obtain these White Certificates, the mandatory participants must either carry out energy savings work themselves (e.g. by distributing energy efficient appliances or installing insulation) or have such work carried out by companies known as “delegatees”. Delegatees carry out energy savings work or subcontract such work in turn, then receive White Certificates from the Ministry for Ecology in exchange for the work carried out. Delegatees then sell these White Certificates on to the mandatory participants.

This system was launched in 2006 and has been expanded in successive phases. With each phase, the energy savings objectives have increased, leading to a rise in the volumes of White Certificates issued. Phase III, from 2015 to 2017, saw an increase in cases of fraud involving White Certificates being delivered on the basis of work that was never carried out.

The risk primarily involved the delegatee status, whereby some companies could submit false applications to obtain White Certificates from the Ministry for Ecology. They then sold these White Certificates to brokers or energy sector groups that needed to fulfil their quotas.

Recent regulatory changes have added safeguards to the system:

- The criteria for becoming a delegatee have been tightened.
  - The PNCEE (National Unit for White Certificates) now has greater resources to carry out the necessary investigations before certifying applicants as delegatees.
  - The delegatee status was overhauled on 1 June 2018 to strengthen regulatory requirements, notably in terms of technical and financial resources. Previous delegatees and new applicants for delegatee status had to apply to the PNCEE to keep or obtain this status. Some companies did not reapply.
  - After 1 January 2019, heating oil distributors – who had been targeted by fraudulent delegatees – are no longer mandatory participants. Companies that had obtained their delegatee status only through heating oil distributors will lose their status.

---

1 See Tracfin’s “2016 ML/TF risk trends and analysis” report, pp. 9-14.
The procedure for issuing White Certificates has been strengthened.

- The application form that must be submitted to the PNCEE to obtain White Certificates has been updated so that the entities carrying out the energy savings work are more clearly identified. Phase IV, which began in 2018, is expected to result in stricter controls of information and documentation submitted for the issuance of White Certificates.¹
- The list of eligible projects is being revised to eliminate certain kinds of energy savings work that have proven more susceptible to fraud.
- Penalties against fraudulent companies will now be published in the Journal Officiel.
- Other anti-fraud measures are under consideration: strengthening the PNCEE’s resources and independence with regard to planning and conducting audits; setting up a complaints system for individuals in case work is not done or is done poorly, in order to identify the delegatees at fault; implementing a system to freeze White Certificates in cases of fraud; eliminating caps on fines; ramping up information exchanges amongst the relevant public sector entities, etc.

However, fraud methods are changing in response to these stricter rules. Companies seeking to commit fraud no longer attempt to obtain delegatee status directly. Instead, they set up partnerships or subcontracting agreements with delegatees or mandatory participants.

**Tracfin continues to handle many cases of White Certificate fraud.** While these cases involve past incidents that occurred prior to the PNCEE’s reorganisation, they nevertheless highlight the risks inherent in subcontracting channels that can circumvent the delegatee status.

**Case study no. 6: White Certificate fraud via subcontracting chains used by delegatees**

White Certificate frauds can involve networks of companies using subcontracting chains.

“Company 1” is a small, struggling construction company based in Paris. In 2017, three partners acquire “Company 1” and change its articles of association (company name, corporate purpose and shares) to refocus the business on insulation work. They injected €800,000 in equity from outside investors.

“Company 1” then presented itself as a subcontractor carrying out energy savings work on behalf of delegatees or mandatory participants. Normally, for the PNCEE to approve work as being eligible for White Certificates, the companies that carried out the work must have received the RGE credential (Reconnue Garante de l’Environnement, which ensures their environmental standards). The RGE credential is awarded by five accredited independent entities. “Company 1” claimed to hold this credential in its communications materials.

On the credit side, “Company 1” received €1m from just two clients. These two clients were both delegatees. “Company 1” provided them with the supporting materials so that they could receive a corresponding amount of White Certificates from the PNCEE.

On the debit side, “Company 1” paid out only €500,000 to a company in the same business sector, “Company 2”, which was apparently another subcontractor. Given the markups for businesses in this sector, the €1m in turnover generated by “Company 1” was apparently largely fictitious, especially as its financial accounts do not show any payroll expenditure or purchases of goods.

Moreover, “Company 1” transferred more than €250,000 to various beneficiaries with no ties to its business activity (including a car repair business owned by the same person as “Company 1”, call centre companies paid for fictitious services backed by false invoices, and personal accounts), thus suggesting a misuse of company assets.

The second level of the network was centred on “Company 2”, which more or less followed the same pattern as “Company 1”, but with greater financial wherewithal.

---

¹ To improve evidence of work being carried out, the PNCEE is considering creating an online platform to store photos of work carried out in support of applications for White Certificates. The largest mandatory participants would only purchase White Certificates from delegatees who use this platform.
“Company 2”, as well, was acquired by two partners who overhauled its articles of association and refocused its business on energy savings work.

On the credit side, “Company 2” took in €15m in a few months:
- €10m from five delegatees, thanks to the White Certificates from the PNCEE;
- €5m from a broker as payment for White Certificates on behalf of mandatory participants.

On the debit side, its outgoings were:
- €7m paid to other companies in the business sector, often not RGE-certified and with dubious trade practices;
- €4m to purchase insulation materials from a distributor;
- €2.1m to various beneficiaries (such as call centres, non-profits or individuals), suggesting a misuse of company assets.

A portion of “Company 2”’s business was apparently legitimate. However, to carry out the energy savings work, it used subcontractors with seemingly dubious trade practices. These subcontractors did not have the RGE credential; an analysis of their accounts shows that their tax affairs were not in order and they used undeclared work; a case-by-case review of White Certificate applications shows that the work declared was two to ten times higher than the work actually done.

This setup was then made more opaque with the creation of additional entities that acted as intermediaries between “Company 2” and its clientele of mandatory participants. Thanks to these shell companies, “Company 2” avoided being identified as a very large provider of energy savings work, thereby not attracting the attention of the departments responsible for overseeing the delivery of White Certificates. After receiving the funds, these shell companies were acquired by “Company 2”.

Tracfin’s investigation confirmed doubts about whether these activities were legitimate:

The three partners of “Company 1” had previous convictions (for breach of trust, armed extortion and kidnapping offences). The €800m that they invested in the company originated from individuals but had no economic justification, suggesting it may have come from money laundering by a criminal organisation. This recapitalisation move was aimed at making “Company 1” look more credible to banks as it resumed its activity, but €500m was returned to the investors six months later.

“Company 2” was run by a de facto manager who received €120,000 from the company despite not being a corporate officer or an employee. It was also discovered that this individual had been the creator of several crypto asset investment websites.
SEPA DIRECT DEBIT FRAUD: SECURITY FLAWS PERHAPS NOT AS BAD AS FEARED

In 2015 and 2016, Tracfin had detected a new kind of fraud that targeted security flaws in SEPA (Single Euro Payments Area), which took effect in 2014 and aimed to create a unified payment standard for 34 European countries. The fraud was based on the new rules for direct debit, which eliminated a bank’s obligation to make sure a direct debit authorisation was in place before carrying out a transaction, in exchange for making it easier to dispute unauthorised direct debits. Fraudsters could make unauthorised direct debits, or request refunds of authorised ones, while taking advantage of the processing times so that the financial risk actually fell on the banks.1 Tracfin did not identify any significant cases in 2017 or in the first half of 2018. This suggests that the cases handled in 2016 were actually attempts aimed at testing the security flaws in the SEPA system. It would appear that fraudsters were discouraged by the difficulties creating companies that were credible enough, in economic terms, to justify setting up direct debits or requesting refunds. Banks, on the front line for counterparty risk in cases of direct debit fraud, were obviously vigilant enough to reduce this risk, and the alert issued by Tracfin may have helped prevent such fraud.

TAX EVASION, SOCIAL SECURITY FRAUD, ACCOUNTING FRAUD OR CUSTOMS FRAUD COMMITTED BY COMPANIES THAT HAVE A LEGITIMATE ECONOMIC ACTIVITY

In addition to the aforementioned fraudulent activities, another major source of cash for money laundering comes from the full range of tax evasion, social security fraud, accounting fraud or customs fraud committed by real companies. These cases of fraud include undeclared business, under-reported turnover, undeclared work, misuse of company assets, import/export activities without filing customs declarations, VAT fraud, etc.

In some cases, this kind of fraud can be used to launder money from criminal activities, especially narcotics and human trafficking.

Apart from tax evasion, undeclared work is the most frequent offence in the Suspicious Transaction Reports submitted to Tracfin, and is one of the priority areas for the Unit’s work. These cases mainly involve small construction companies. Other labour-intensive sectors may also be involved: notably private security companies, cleaning and maintenance services, and the hospitality sector.

Tracfin shares the analysis of criminal investigation departments,2 indicating that undeclared work can be a means for laundering the proceeds of other illegal activities. Criminal organisations often generate cash that can be injected into a legitimate business and used to pay undeclared workers or certain suppliers. This undeclared labour can generate additional revenue for the business, which is largely undeclared. Cash profits from criminal activities can be mingled with other businesses carried on illegally (such as metals trading, door-to-door sales, sales at markets, dealing in used cars, etc.). These practices are more common when the underground economy is more developed.

---

1 See Tracfin’s “2016 ML/TF risk trends and analysis” report, pages 14 to 17.
2 Notably the Information, Intelligence and Strategic Analysis of Organised Criminality Department (SIRASCO) and the Central Office for Combating Illegal Employment (OCLITI), which both report to the Central Directorate of the Judicial Police (DCPJ).
Thus, profits from criminal activities can be injected into a legitimate business as follows:

- A narcotics smuggling network collects its revenue in cash.
- This cash is injected into construction companies or private security firms and used to pay undeclared workers or even to purchase supplies.
- These businesses carry on their normal activities and deposit their revenue into their bank accounts. As this revenue is partly from undeclared cash, it cannot be fully declared and a portion of it must be laundered. The companies involved transfer the undeclared portion of their revenue via bank transfer or cheque to a network of shell companies, covered by false invoices.
- The funds are then transferred abroad, either directly via bank transfer (see below), or covered by goods exports. The proceeds from the sale of these goods will then be transferred to the initial owners of the funds.

**SHELL COMPANY NETWORKS REMAIN THE MAIN MEANS FOR MONEY LAUNDERING THROUGH BANKING CHANNELS**

The main ways for money laundering through banks involve networks of shell companies – or letterbox companies – aimed at transferring funds abroad. Tracfin regularly handles large-scale cases of such money laundering schemes. Several significant cases were referred to the courts in 2017 and 2018.

A shell company network consists of several levels:

- At the beginning of the chain are client companies that have money to launder.
- A first level is made up of shell companies in France, with bank accounts in France.
- A second level, known as a “relay”, is made up of shell companies registered in other European countries, usually in Eastern Europe (Hungary, Poland, Bulgaria, Slovakia or the Baltics), but also possibly in Portugal, the Netherlands or the UK. These companies have bank accounts in their home countries and in several neighbouring countries.

Most financial flows ultimately end up in Asia (China or Hong Kong), the Middle East or certain Mediterranean countries (such as Israel or Turkey).

These networks do not use complex financial arrangements. Their effectiveness depends on how well various actions are carried out at the different levels: an increased number of shell companies and bank accounts; recruitment of front managers for shell companies; dividing up and crossing financial flows. The first- and second-level companies carry out a large number of crossed bank transfers to give the impression of real business activity and to make the financial evasion harder to detect. These networks are difficult to map because they constantly open and close legal entities and bank accounts and rapidly carry out large numbers of bank transfers.

Due to the scale and flexibility of these networks, dealing with them is a complex issue for the legal system. Therefore, certain investigative decisions must be made in order to ensure a robust criminal procedure and to manage investigative resources efficiently.
Case study no. 7: A network of shell companies and relay accounts

Tracfin identified eight French companies with legal and financial ties whose business activity was suggestive of shell companies in the first level of a network. In one year, they managed to channel €20m in financial flows.

These eight companies were all owned and managed by the same individuals. They had broad corporate purposes that encompassed the same business sectors: IT consulting, maintenance and outsourcing, cloud computing, call and data centre services, wholesale and intermediate trade (building materials, electronics and IT hardware, food, textiles, appliances, precious metals and ores, etc.), lease-purchase, or renewable energy.

All these companies had been recently created or reactivated, and had been subject to many changes to their articles of association and shareholding structure. They were often set up with SASU status (simplified limited companies with a single shareholder), a very flexible company structure. Their share capital was very low compared to the financial flows into and out of their bank accounts. They used virtual office addresses and false lease agreements. They held accounts with multiple banks over short periods of time, and most of them did not have their tax, social security and customs affairs in order. They had not filed any advance hiring notices and appeared to have no employees. These companies had short lifespans, generally less than 18 months, before being shut down or placed into court-ordered liquidation prior to initial tax audits.

The eight companies identified by Tracfin collected money from a single pool of clients. This client pool comprised dozens of SMEs or very small companies in various sectors: construction, general repairs, sale and maintenance of electronics and IT hardware, vocational training, private security services, food and beverage retail, marketing consulting services and call centres, advertising agencies, home improvement and renewable energy, etc. They either had a legitimate economic activity, or were fronts for fraudulent activities. They often had undeclared workers.

Each client company transferred tens or hundreds of thousands of euros to the “money launderers”. Thus, each money laundering company collected between €2m and €3m in 12 months, for a total €20m in financial flows.
Further down the channel, the “money launderers” transferred the bulk of money to the network’s second level, comprising around 20 companies across Europe. These European companies were recorded as suppliers in the accounts of the French “money launderers”. They were created by the same individuals. They were mainly set up in Austria, Hungary, the Czech Republic and Poland, but also in Germany, the Netherlands and Spain. They claimed to be working in IT services and IT hardware sales.

Tracfin noted glaring inconsistencies between bank flows and a lack of customs declarations or very low operating expenses. The crossed financial flows between companies on each level, as well as the combination of unrelated business sectors, were definitive evidence of the economic inconsistencies of the intermediary companies.

The funds received by the European companies were immediately transferred abroad, primarily to Asia (China and Hong Kong), to bank accounts belonging to companies or individuals.

As this network involved intermediary companies in France and chains of suppliers in Europe, it could be used for VAT fraud by artificially creating VAT deductions or refunds for the French clients. While a small portion of the financial flows may correspond to actual business activity, these flows are organised in such a way as to avoid paying VAT. The French “money launderers”, which will go into default, artificially house VAT debt corresponding to VAT not paid by their clients (who actually purchased goods).

Tackling networks of shell companies requires a coordinated effort in France and abroad, especially at European level.

In France, all stakeholders must work to detect fraudulent companies at the earliest stage possible: commercial court registrars, commercial registered office providers, commercial banks, Tracfin, the DGFiP, Customs, the DGCCRF, police departments and specialised magistrates. Available information must be shared. In July 2018, Tracfin and the National Association of Commercial Court Registrars (CNGTC) signed a joint action plan to give registrars training about Tracfin’s duties, ML/TF risks and how to detect unusual financial transactions.

At international level, effective cooperation between Tracfin and FIUs in relay countries, especially in Eastern Europe, is crucial. Such cooperation has already achieved notable results in halting certain transactions, recovering diverted funds and identifying network members. However, it can be further developed.

TWO SECTORS WITH HIGH MONEY LAUNDERING RISK: CONSTRUCTION AND VEHICLE TRADING

The construction sector – especially SMEs – and vehicle trading sector are at particularly high risk for money laundering. Many cases handled by Tracfin involve one or both of these sectors. They can easily overlap with the shell company networks described above.

CONSTRUCTION SECTOR SMES

SMEs in the construction sector have a very high risk of money laundering due to their frequent involvement in undeclared work and tax evasion.

---

1 Tracfin’s investigations quickly determined that the individuals with ties with the French and European companies were, in some cases, known to the police for fraud and money laundering offences.
Case study no. 8: A construction subcontractor launders the proceeds of undeclared work and tax evasion by joining a large-scale European money laundering scheme

“Company X”, based in the northern suburbs of Paris, is a subcontractor in the construction sector. It works in all building and masonry trades. Its annual accounts showed turnover of €6m in the form of cheques and transfers from various other companies, generally in labour-intensive sectors.

Its outgoings fall into two categories: bank transfers to French and European companies, some of which match the profile of shell companies used for fund evasion; cheques for small amounts to the order of many individuals. “Company X” declared only one employee and reported no expenses for the purchase of building materials, thus suggesting that it is not really a construction company.

Thus, over a year, “Company X”’s expenses are as follows:

- €5m in transfers, primarily to wholesalers (for household items, cosmetics and clothing) and vehicle trading companies. In particular, “Company X” transferred €700,000 to a Belgian consumer goods wholesaler belonging to British holding companies. The invoices submitted as justification for these payments were falsified.
- €1m in cheques (more than 300 cheques, of which 290 for amounts less than €3,000). None of the individuals receiving these cheques was listed in the company’s advance hiring notices.

“Company X” has not paid taxes despite its significant bank flows.

Tracfin’s investigation determined that “Company X” was the largest of a series of similar companies in the construction and vehicle trading sectors in France. These companies were apparently satellites of “Company X”: they helped collect undeclared funds from various business sectors. They broke the flows down into smaller amounts to avoid attracting attention. Most of these satellite companies had names that were very similar to “Company X”, with just one or two letters different. By playing on these almost identical names, “Company X” could deposit cheques made to their order. “Company X” therefore centralised the pay of undeclared labour.

Combining the funds sent by “Company X” and those sent by its satellites, the Belgian wholesaler collected more than €1.5m (according to Tracfin’s investigations) from France in a year. Of this total, nearly €1m was transferred to Dutch, UK and Polish companies. Continued investigations revealed that this setup was replicated in France and other neighbouring countries, revealing an organised European money laundering network.
Case study no. 9: A construction subcontractor acts as a “cash box” to pay undeclared workers of other construction companies

A company in the Paris region is registered as a subcontractor in the construction sector. From an accounting standpoint, its income looks coherent, with an annual turnover of €7m, mainly from other construction sector SMEs. However, its expenses are unusual for several reasons:

- No purchases of building materials.
- A large number of cheques issued for small amounts, to the order of individuals not reported in advance hiring notices.
- Sizeable expenses with no ties to the business: €700,000 for luxury watches; €260,000 for vehicle purchases in Germany; €750,000 in transfers to Hungary and Cyprus, leading to other financial flows to China.

The investigation, conducted jointly with URSSAF, determined that the manager owned several construction companies, which served other companies in the sector as a “cash box” vehicle to pay undeclared workers, to conceal money from the tax authorities or to generate undeclared cash. His companies were liquidated within 18 months of their creation so that they would not have to file financial statements with the tax authorities. For all of his companies, he allegedly concealed €2m from URSSAF and diverted €2.3m.

VEHICLE TRADING

The Suspicious Transaction Reports submitted to Tracfin very often involve the vehicle trading sector, especially used vehicles. This sector is highly exposed to the risks of money laundering and undeclared business. It is often involved in the money laundering channels described above.

It has two major advantages for money launderers:

- with regard to purchases, vehicles can be bought in cash in European countries that do not place a cap on cash payments;
- for reselling, the market is buoyant thanks to dynamic export channels. Some overseas used car markets generate strong demand, which is met by undeclared imports of vehicles.

Tracfin, alongside criminal investigation departments, frequently handles such cases.

Case study no. 10: Money laundering through European vehicle traders

Two members of the same family, both French nationals, created two vehicle trading companies in a neighbouring country: “Company 1” and “Company 2”. These companies opened bank accounts in France.

The companies’ debits seemed consistent with their business activity: payments went mostly to European automobile dealerships, from which Companies 1 and 2 were purchasing vehicles. While most of the dealerships were in Germany, the largest in volume terms was in Gibraltar.

By contrast, the credits were unusual.

- “Company 1” received deposits totalling €15m in ten months, from French companies that had been recently set up or had failed to comply with their tax obligations. These companies declared business activities ties that were inconsistent with purchasing vehicles on a massive scale (e.g. construction, pallet/packaging material trading, and private security), and did not register any vehicles over the period being investigated.
- “Company 2” recorded €1m in credits to its accounts in a few weeks, from French bank accounts with individual account-holders. Tracfin’s investigation revealed that most of these individuals were elderly and were living abroad. Their French bank accounts showed very few transactions: the only inflows were pension payments, and outgoings were banks transfers to entities such as “Company 2”. No evidence could be found that these individuals were still alive.

In addition, Companies 1 and 2 had no declared operating resources in France: no taxable turnover, no VAT filings, no declared employees, no customs declarations for the import/export of goods, dormant websites.

Lastly, Tracfin received information from the FIU of the country in which Companies 1 and 2 were registered, indicating that two individuals had been stopped by customs officers in possession of €260,000 in cash. These individuals reported that this cash was to be used to buy vehicles from “Company 1”.

These various elements constitute a suspicion of money laundering of the proceeds of tax evasion and social security fraud, committed both by French companies (namely undeclared work, unreported turnover and VAT fraud) and by individuals (pension scheme fraud).

Companies 1 and 2 may have been purchasing vehicles in Europe to sell them on other markets abroad. The proceeds from these sales may have been transferred to undeclared foreign accounts, belonging to the initial French funders or the individuals behind the scheme.
Case study no. 11: Laundering of illegal funds through used car sales for illegal imports to North Africa

“Company Z”, with SASU status (simplified limited companies with a single shareholder), operates in the vehicle trading business. In less than a year, it received €3m in inflows from small construction companies and private security firms. An analysis of the accounts of some of these companies revealed widespread use of undeclared workers and an absence of tax and social security filings.

“Company Z”’s outgoing also totalled €3m in barely one year. More than €2.7m was spent on purchasing vehicles from European automobile dealerships, the largest of which was in Poland.

“Company Z” had not fulfilled its tax obligations. It had not filed a business earnings report even though its turnover was sufficient to require it. It had not filed any VAT returns, while the Polish and German car dealers it traded with declared to their home tax authorities that they had delivered vehicles to “Company Z” under a specific VAT number.

Tracfin examined customs declarations and discovered that over the same period, “Company Z” had exported 120 vehicles to North Africa, for a total value of €4m. However, no financial flows corresponding to these exports were recorded in “Company Z”’s bank accounts.

The criminal investigation brought to light a scheme to launder funds from drug trafficking activities, with funds being remitted via a used car trading activity. Covered by false invoices, “Company Z” collected illegal funds from construction companies or private security firms, which in turn gathered funds from drug trafficking. “Company Z” purchased vehicles, then resold them in North Africa. The proceeds from these sales were then recovered by relatives of the individuals dealing drugs in France.

The official automobile dealership market in certain North African countries is highly regulated to favour local automakers. Imports of new vehicles are prohibited, and there are strict limits on imports of vehicles more than three years old. As a result, consumers turn to vehicle purchases from individuals. Certain individuals (such as veterans) enjoy licences that make it easier for them to purchase foreign vehicles. Several hundred false licences are in circulation. This has fuelled demand on the underground vehicle market. This demand encourages illegal imports from Europe of stolen or trafficked vehicles, or as part of money laundering schemes.
STEMMING THE STEADY INCREASE IN RISKS RELATED TO ONLINE PAYMENT SERVICE PROVIDERS
Since the late 2000s, the EU has provided support for the liberalisation of banking and financial services by developing a legal framework conducive to the emergence of new players: European e-money directives from 2000 and 2009, and the payment services directives from 2007 (PSD1) and 2015 (PSD2). This normative shift, particularly PSD2, has boosted the growth of service providers that offer payment accounts that are easy to open and use.

The category of payment and electronic money service providers (PS/EMSPs) includes establishments that offer:
- Payment services referred to in Article L.314-1 of the French Monetary and Financial Code (CMF). These including cash payments and withdrawals from a payment account, direct debits, bank transfers, card payments, transfers of funds, etc.
- And/or the electronic money services defined in Article L.315-1 of the CMF

These establishments must be accredited to operate.

- In practice, the term PS/EMSP refers to three main types of establishments:
  - Credit institutions (CIs) for the part of their activity that has to do with payment services
  - Payment institutions (PIs)
  - Electronic money institutions (EMIs)

A new generation of PS/EMSPs has distinguished itself, with distribution channels based primarily on digital technologies, the Internet and smartphones.

Tracfin notes that these new PS/EMSPs are multiplying and are increasingly used in money laundering operations, in addition to or in parallel with the standard networks of shell companies. They are now present in most of the circuits described above in Chapter 3.

Supervision of these institutions can be difficult. The vast majority of PS/EMSPs operate in France under the European passport, which allows a company that is authorised in one Member State of the European Economic Area (EEA) to distribute its products in all the other Member States. There are two aspects to the European passport, the freedom of establishment and the freedom to provide services:
- Freedom of establishment where PS/EMSPs have a physical presence on the territory of the host country (branch offices and/or networks of agents for payment services and/or networks of distributors for electronic money). They are then legally subject to AML/CFT regulations and to the monitoring by the host country’s supervisory authorities.
- Freedom to provide services when PS/EMSPs operate in the host country without having a brick-and-mortar establishment there (services are distributed only online). In this case, they remain under the supervision of their country of accreditation. If there are any doubts about AML/CFT compliance, the host country supervisory authorities should contact their counterparts in the country of accreditation.

- Although PS/EMSPs operating in France under the freedom of establishment are legally subject to the same AML/CFT regulations as establishments that are authorised in France, in practice some of them can be difficult to monitor. With regard to the freedom to provide services, some EEA countries are less strict in the area of AML/CFT supervision. In this sense, the European passport – and in particular the freedom to provide services regime – weakens the French AML/CFT system significantly.

These risks, which were already pointed out in Tracfin’s «2016 risk trends and analysis» report, are increasing and require that the resources for monitoring European PS/EMSPs be bolstered.

---

PAYMENT AND ELECTRONIC MONEY SERVICE PROVIDERS (PS/EMSPS) ARE INCREASINGLY PART OF MONEY LAUNDERING CIRCUITS

Money laundering circuits that use shell companies tend to circumvent the traditional banking system. The system is boosting its due diligence efforts, developing alerts and tools for detecting suspicious transactions, and closing transit accounts more and more quickly. Money laundering networks now use online payment and electronic money institutions, where KYC procedures are less stringent and supervision is less well-established.

Over the past two years, Tracfin has seen a surge in the use of payment and electronic money accounts in money laundering circuits abroad. Every type of fraud scheme that use such circuits is affected:

– Laundering of funds derived from fraudulent activities and undeclared work
– Various fraud schemes: false payment orders, fraudulent fake investment sites, white certificate scams, false accessibility assessments, fraudulent adverts for credit offers or real estate rentals, etc.

The following two examples are indicative of this trend.

THE USE OF PS/EMSPS IN SHELL COMPANY NETWORKS USED TO LAUNDER MONEY

Case study no. 12: Opening of payment and electronic money accounts by a shell company in the construction sector that abandoned its accounts

Company X is recently created in the Paris region by two partners. It is a subcontractor in the construction sector (finishing works, solar and energy engineering). It appears to closely follow the money laundering model described in Chapter 3 of this report.

• In one year’s time, the company collects €3 million in the form of cheques and bank transfers issued by other French companies in the construction sector.

• Despite these significant inflows, the company does not file or pay any taxes or VAT.

• The company’s small number of declared employees is incompatible with the volume of activity. It issues a number of cheques to individuals who do not appear in the company’s advance hiring notifications or social security declarations. On the other hand, some of these individuals are listed as employees of other construction companies that have transferred funds to Company X. This set of circumstances suggests the existence of undeclared work.

• It transfers €1.9 million to four foreign companies established in the UK, Bulgaria and Turkey, but managed by French residents linked to the manager of Company X.

One year after it was founded, Company X closes several of its bank accounts to open payment accounts with a payment service provider. Detailed examination of Company X’s transactions allowed Tracfin to identify accounts held at:

• A French payment account service for professionals. This service does business as the payment agent of an electronic money institution approved for operating in France. By relying on the electronic money institution that provides the payment infrastructure, the service does not have to carry out its own AML/CFT due diligence obligations.

• A Luxembourg payment institution doing business in France under the freedom of establishment regime.

• A Belgian payment institution specialising in multi-currency services also doing business in France under the freedom of establishment regime.
• A British electronic money institution operating in France under the freedom to provide services.

Over nine months, nearly £2 million is registered in these accounts, which is then moved to other bank or payment accounts opened abroad, some in the name of the British company – which was already the primary recipient of the outflows issued by Company X – and some whose beneficial owners are difficult to identify.

Tracfin has referred the Company X case to the courts for undeclared work, tax evasion and laundering the proceeds of various offences.

ONLINE CREDIT CARD PAYMENT COLLECTION SOLUTIONS USED AS A SCREEN TO CONCEAL THE TRACEABILITY OF FLOWS

Case study no. 13 : A fraud network using online platforms for collecting card payments

Under French law, all establishments open to the public are obliged to assess the accessibility of their premises to people with disabilities before carrying out any necessary works to bring the establishment into compliance. This obligation is particularly applicable to medical and paramedical establishments.

Tracfin became aware of Company Y, a simplified limited company with a single shareholder (SASU) that was created in Paris. Its broad corporate purpose involved the purchase, sale and import/export of all types of electronic and computer products.

Analysing the transactions for Company Y’s bank accounts, Tracfin established that, over seven months, the company managed to collect at least €600,000 in inflows. Using aggressive canvassing techniques, the company contacted health professionals, and presented itself as mandated by a public or para-public organisation that can help them comply with their regulatory obligations. In exchange for a fee of between €1,000 and €2,000, payable by credit card, the company offered an accessibility assessment. Company Y pocketed the money and disappeared. The assessments were never carried out. The professionals contacted thus seem to be victims of fraud, the so-called «accessibility assessment scam».

To collect the money, Company Y set up an opaque financial network, designed to conceal the traceability of flows between the victims who issue the funds and the beneficial owners. To do so, the company introduced several PS/EMSPs, established both in France and abroad, as intermediaries.
Remote credit card payments from individuals were divided between two payment platforms:

- An online platform for collecting credit card payments. This was initially backed by a European electronic money institution that was in charge of the payment infrastructure. The flows arrived into the bank accounts of this EMI, before being re-transferred to the bank accounts of Company Y. In response to the initial complaints against Company Y, the European EMI severed ties with the collection platform, which then substituted a French electronic money institution.
- A payment service provider accredited in France that offered a secure online payment solution. This service provider received bank flows from individuals and then transferred them to the bank accounts of Company Y. Company Y successively Bank A, then Bank B, and then the payment account of a different EME as the destination account.

Once the funds were collected, Company Y transferred them to a money-laundering network:

- Either to a French company offering telemarketing and call centre services, with the characteristics of a shell company. The shell company then re-transferred most of the funds collected abroad. It also was found to be part of a VAT carousel fraud network.
- Or to a company established in the Balkans, which has been part of other organized fraud schemes, particularly in the solar panel sector.

Tracfin investigated cases of PS/EMSPs whose internal processes raised questions about whether their managers were aiding and abetting fraud networks. For example, a group of trading companies defrauded private individuals via the Internet through fraudulent investment sites. These companies had entrusted the management of their payment flows to a British EMI, whose internal processes had been designed to maintain the beneficiaries’ anonymity. The names of the trading companies never appeared on the transfer orders issued by the defrauded individuals. Credit institutions holding the accounts of individual victims could not see the names of these companies in their computer systems. Even though the trading companies were publicly condemned by supervisory authorities, the credit institutions’ computer alert systems would not have been able to immediately identify these transactions as fraudulent.
PREPAID CARDS ISSUED BY PS/EMSPS REVEAL FLAWS IN HOW REGULATIONS ARE APPLIED

Every year, Tracfin issues alerts on the risks associated with electronic money devices, in particular physical devices such as prepaid cards and vouchers.

In 2016, France tightened its electronic money regulations. As from 1 January 2017, the date of entry into force of Decree No. 2016-1742 of 15 December 2016 (creating Article D.315-2 of the French Monetary and Financial Code), prepaid cards issued in France are subject to various caps:

- **Storage cap**: the maximum value that can be stored in electronic form and used by means of a physical device is set at €10,000.
- **Loading cap**: the maximum amount of cash or so-called anonymous electronic money that can be loaded is set at €1,000 per calendar month.
- **Usage cap**: the maximum amount of withdrawals and cash refunds is set at €1,000 per month.

Yet European and French regulations are limited in that it is possible, for payment and withdrawal transactions in the EU, to use prepaid cards issued by institutions that are not subject to these regulations. Some non-European countries do not have caps, or they are set quite high. This is a significant flaw in the current AML/CFT system.

Within the EU, some institutions are not always in compliance with the regulations in force, particularly the obligation to verify the identity of customers above a certain threshold. Tracfin’s attention was drawn to an individual holding a card issued by a European EME that had a balance of €24,000, without the issuing institution being able to provide the FIU in the country of accreditation with precise identity details about the customer.

Lastly, certain products marketed in France and in compliance with European regulations may be propitious for fraudulent activities, particularly if the operator issuing the products does not perform due diligence.

**Case study no. 14: Marketing of packs of prepaid cards used by fraudsters**

A European credit institution offers packs containing several prepaid cards. The main card can be reloaded by bank transfers or by purchasing vouchers. The other cards are funded only by the balance of the first card, and are used to purchase goods and services or to withdraw cash.

These packs were being used by a network of online ad fraudsters. The scam consisted of posting fictitious ads online, for example for rental properties or job offers, and then asking the interested customer or candidate to put down a deposit to confirm his or her interest.

Fraud networks use this multi-card pack system to:

- Reload the first card in France using bank transfers or vouchers paid for by the fraud victims
- Then use the other cards, in the possession of people in a West African country, to make cash withdrawals

In each of this type of cases that were handled by the Unit, tens of thousands of euros – and sometimes several hundred thousand – were loaded onto the first card.

To issue and market these prepaid card packs in France, the European credit institution partnered with a French payment service company. The company claims to be an «authorised» intermediary in banking transactions and payment services (Intermédiaire en opération de banque et services de paiement – IOBSP). However, exercising an intermediary activity in France is subject to simple registration with ORIAS (France’s centralised registry for insurance, banking, and finance intermediaries), which the company had not done.

In addition, the gang purchased the packs and activated their accounts using assumed names and identities without being detected by the issuing institutions. As a result, Tracfin was unable to identify the real perpetrators.

---

1 I.e., not subject to the obligations of identification and verification of the customer’s identity, pursuant to Articles L. 561-9 and R. 561-16-1.
THE ONLINE FUNDRAISING PLATFORM SECTOR ALSO REQUIRES PS/EMSPS TO PERFORM AML/CFT DUE DILIGENCE

Crowdfunding platforms and money collection websites are the two types of stakeholders in the online fundraising sector.

Crowdfunding platforms provide financing in the form of equity investments, loans or grants. Those offering equity financing have the status of «crowdfunding advisers» (CIP). Those offering financing in the form of loans or grants have the status of «crowdfunding intermediaries» (IFP). Both are subject to AML/CFT requirements by virtue of 4) and 6) of Article L.561-2 of the French Monetary and Financial Code.

Money collection websites are not legally part of the crowdfunding sector, and are not subject to AML/CFT requirements as reporting entities.

The difference between a crowdfunding intermediary exclusively handling donation transactions and a money collection website lies in the concept of a «project».

- Crowdfunding platforms publish projects online. A project is defined by three elements: a subject, a length of time and a set amount that corresponds to its financing needs.
- Money collection websites are about simple events. An event is defined by two elements only: a subject (often a celebration involving family, friends or professionals) and a date. But it does not include a predefined amount. The final amount collected is solely dependent on the generosity of donors.

For Tracfin, these two definitions have no real significance in terms of AML/CFT risks. Both crowdfunding intermediaries and online money collection sites present similar risks, particularly with regard to terrorist financing.

The AML/CFT risks associated with the online fundraising sector were identified early on by Tracfin. The Unit has supported several initiatives to limit these risks in terms of crowdfunding. In 2014, Tracfin advocated the including both crowdfunding intermediaries and crowdfunding advisers in the list of those subject to AML/CFT reporting obligations. In 2016, Tracfin was in favour of including IFPs offering only grants in the list of reporting entities.

Tracfin now recognises the need for money collection sites to be subject to AML/CFT requirements. During work on enacting the Fourth Anti-Money Laundering Directive into French law in 2016, Tracfin emphasised this point. Progress has been made with Order No. 2016-1635 of 1 December 2016, which allows Tracfin to submit requests for information to these sites. The enactment of the Fifth Directive will likely complete these measures.

---

1 As defined in Articles L.547-1 et seq. of the French Monetary and Financial Code.

2 As defined in Articles L.548-1 et seq. of the French Monetary and Financial Code.

3 For example, a humanitarian organisation wishing to raise funds to finance the purchase of a well for a village will request a donation amount calculated to match the total cost of installing the well.
AML/CFT RISKS IDENTIFIED BY TRACFIN WITH RESPECT TO ONLINE FUNDRAISING

The number of suspicious transaction reports (STRs) related to the online fundraising sector more than doubled in a single year. In 2017, Tracfin received 364 STRs relating to this type of transaction, an increase of 140% over 2016.

This sharp upswing is the natural result of these platforms’ success and their increasing use by individuals. Awareness-raising efforts amongst reporting entities about risks facing the sector are also bearing fruit. However, crowdfunding platforms, which recently have become subject to regulation, still submit too few reports (23 STRs in 2017). Most STRs received are submitted by the payment and electronic money institutions (70%) and credit institutions (22%) used by the platforms. Credit institutions seem to be increasingly aware of the risks presented by the sector. In 2017, more than 30 of them submitted reports.

The types of fraud noted in STRs continue to diversify, reflecting the increasing use of these platforms for illicit purposes.

As Tracfin reported in 2016, crowdfunding has opened up new areas for fraud. Every aspect of this type of financing is involved: equity investments, loans and grants. The schemes are most often based on fictitious projects, with varying degrees of sophistication. In this area, Tracfin has processed several cases of pyramid schemes.

Case study no. 15: Investment fraud using crowdfunding platforms

«Mr Z», an entrepreneur, used various crowdfunding platforms to attract investment in an innovative company.

To do so, he created two entities:

- The company that was touted as an innovative SME, which allegedly manufacture and marketed smart objects for the general public. Mr Z held more than 33% of the capital and served as the manager. The company had twelve employees.

- An investors’ club, accessible by co-optation, designed to encourage investment in the company through crowdfunding. Investors were not entitled to shares, but rather to royalties on future sales. The investments were intended to finance the company’s R&D activities. The expected returns were highly appealing and – under the terms of a sponsorship system – increased geometrically if an investor invited others to join the club.

Mr Z collected €500,000 in six months.

Calls for financing took the form of fundraising rounds on two crowdfunding platforms. The first was a known player in the market; the second one, based in France, had been deliberately created by Mr Z to put his plan into action. It had not been registered, as required by law. The funds were centralised in accounts opened with two payment service providers.

One-third of the funds collected (€155,000) was used to pay suppliers for economically justified transactions, another third to pay employees (€165,000) and the final third was wired to bank accounts abroad without no economic justification (€180,000). The beneficial owners of these accounts were found to be Mr Z and the club’s initial sponsors.

Tracfin’s investigations led the Unit to suspect a pyramid scheme. The methods for compensating investors was economically unrealistic, since a geometric progression of returns would have been financially unsustainable for the company. The scheme constantly encouraged investors to find new referrals to join the pyramid. However, only Mr Z and the club’s initial sponsors received the advertised royalties.

Tracfin referred this case to the courts for suspicions of breach of investors’ trust, misuse of company assets to the detriment of the innovative firm, misleading commercial practices and illegal practice of a regulated profession.

---

1 Crowdfunding advisers (CIPs) and intermediaries (IFPs) have been subject to AML/CFT requirements since the entry into force on 1 October 2014 of Order No. 2014-559 of 30 May 2014 on crowdfunding.
In addition, Tracfin continues to note the use of crowdfunding platforms to recycle funds from stolen bank cards. The stolen cards are debited to fund projects placed online by criminal networks. The platforms’ payment accounts are used as collection and transit accounts, which then allow the money to be transferred to other bank or payment accounts.

Cases of suspected terrorist financing, which made their first appearance in 2014, are frequent and mainly involve donation platforms and money collection sites. Tracfin’s various information campaigns and media coverage of the use of this method of terrorist financing have sharpened due diligence efforts by reporting entities.

Finally, crowdfunding platforms’ AML/CFT risks are heightened by the fact that these stakeholders are highly exposed to the use of false documents from both project leaders and funders. Some companies use this type of financing because their profile is too risky to obtain traditional bank financing. They might then be tempted to submit false balance sheets on an online platform.
PS/EMSPS RESPONSIBILITIES IN DETECTING AML/CFT RISKS RELATED TO ONLINE FUNDRAISING TRANSACTIONS

In the online fundraising sector, flagging suspicious AML/CFT transactions is complicated by the fact that KYC and transaction information is split between two stakeholders:

- The fundraising platform itself – whether crowdfunding adviser (CIP), crowdfunding intermediary (IFP) or money collection website – which provides an interface between the organisers, contributors and beneficiaries of projects and events

- An underlying operator, the payment service provider (PSP), which manages the funds pledged by individuals contributing to or benefiting from the projects and events, as well as various related money flows. The PSP is subject to the AML/CFT system.

As a result, the complementary roles of the platform and the underlying operator are such that each possesses partial information that can only be used with difficulty for KYC purposes, unless the two information sources are linked together.

- The platform has information on the nature of the project or event being funded, the online content in support of the project or event, the visitors to the website and the connection data of organisers, visitors, contributors, etc., but it does not have information on the means of payment used by contributors, the origin of the funds or the supporting documentation provided (if any), which are owned/detained by the underlying PSP.

- The underlying PSP, on the other hand, is subject to due diligence obligations, but may lack knowledge of the context of the operation.

- An effective AML/CFT system calls for AML/CFT reporting by both online fundraising platforms and PSPs. As such, Tracfin sees the non-registration of money collection websites as a weak point in the AML/CFT system.

Tracfin supports several measures that should be taken at European level in order to prevent the harmful effects of regulatory competition between Member States:

- Risks should be taken into account at European level:
  - Crowdfunding and money collection sites should be identified as high AML/CFT risks services, justifying the decision to oblige PSPs to step up their due diligence efforts with respect to all these activities
  - Every crowdfunding and money collection site at European level should be subject to the AML/CFT system
  - In addition to Europe-wide compliance, there should be corresponding compliance of all national fundraising platforms, whether for projects or events. PSPs must carry out additional due diligence measures, such as systematically checking the identity of the transaction initiator, as well as obtaining information on the purpose and nature of the transaction.
PAYMENT INITIATORS, AS DEFINED IN THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2), MAY CURB KYC EFFORTS BY ACCOUNT CUSTODIANS

PSD2, which was adopted in 2015 and enacted into French law in 2017, established the existence of account information service providers and payment initiation service providers. Until then, these services had been developed by certain fintechs without being subject to any specific oversight. The enactment of the European directive gave rise to two types of service providers:

- **Account Information Service Providers (AISP):** these provide a consolidated view of all bank or payment accounts that a user holds with one or more PSPs. This service is also called «account aggregation». It does not require approval, but merely registration with the Prudential Supervision and Resolution Authority (ACPR).
- **Payment Initiation Service Providers (PISP):** from a PISP’s website or application, users can directly initiate payment orders to be debited from bank or payment accounts at other PSPs. This activity requires full accreditation as a payment institution with the ACPR.

AISPs and PISPs are known collectively as «third-party PSPs». PSD2 requires banks to make their information systems available to them, via APIs that allow third-party PSPs to access the bank’s customer data and perform payment transactions.

Since the entry into force of PSD2 in early 2018, AISPs and PISPs have expanded considerably in France. By the end of June 2018, the ACPR had given ten stakeholders authorization to offer their services:

- Four French entities accredited as payment institutions with the ACPR, all providing both account information services and payment initiation services
- Six foreign entities registered in EU Member States and operating under the European passport. Two of them operate in France under the freedom of establishment, and the other four under the freedom to provide services.

Before being approved as PISPs, several of these entities had appeared in STRs received by Tracfin as part of their other payment institution or payment institution agent activities. They may have been used by questionable customers for the purposes of fraud, VAT fraud, tax evasion, undeclared work or money laundering in at-risk sectors such as online gambling.

As PISPs, these institutions now have the ability to access their customers’ bank or payment accounts directly and initiate payments. In cases where the flow passes through the PISP account before reaching the final recipient, the PISP reduces the visibility of the credit institution that manages the sender’s initial account. The credit institution loses the ability to analyse and detect suspicious transactions. It is then highly required that PISPs implement their own AML/CFT due diligence obligations, in accordance with the highest standards.

Moreover, it is likely that major global e-commerce firms, which already provide financial services, will consider applying for authorisation as payment initiators. Such an approval would allow them to order their customers’ payments directly at the time of purchase, marginalizing the use of bank cards used up to now. The arrival of this type of stakeholder does not, in theory, present immediate AML/CFT risks, but it does beg the question of credit institutions’ control over KYC in the long run.
HOW EUROPEAN AND FRENCH PUBLIC AUTHORITIES SHOULD REACT IN ORDER TO BETTER MANAGE PS/EMSP RISKS

The European passport scheme generates high AML/CFT risks in the French system, particularly due to the freedom to provide services principle. To limit this, it is vital to provide national supervisors with every necessary means of monitoring the PS/EMSPs that have emerged in recent years. In a given country, entities operating under the freedom of establishment must be subject to the same monitoring as authorised entities. Otherwise, the AML/CFT system would be significantly weakened.

STRENGTHEN THE ABILITY OF NATIONAL SUPERVISORS TO MONITOR PS/EMSPS

In August 2018, the Council of the European Union adopted a technical regulatory standard specifying that a Member State may require PS/EMSPs to appoint a central contact point to respond to requests from the supervisory authorities and the FIU when operating in its territory under the freedom of establishment without a branch office.

At the end of September 2018, the amendment of domestic legislation to conform to the provisions of this European regulation was in progress. It will provide legal security for the regulations in force in France.

EXPAND NATIONAL CENTRALISED BANK ACCOUNTS REGISTRATION (FICOBA IN FRANCE)

In light of the increasing risks associated with the use of multiple PS/EMSPs, the public authorities of each EU Member State must have a national centralised bank account register, which provides exhaustive information on the various bank, payment and electronic money accounts held by individuals and legal entities with authorised institutions within the country or operating on under the freedom of establishment.

- The information must be exhaustive with respect to the scope of the accounts in question

A national centralised bank account register must cover not only bank accounts but also payment and electronic money accounts that individuals and legal entities may possess.

In the case of France, the issue concerns the exhaustiveness of FICOBA, which is managed by the DGFiP. FICOBA would need to be expanded to systematically include all payment and electronic money accounts held by economic stakeholders.

The current national regime is incomplete:

- FICOBA lists only bank accounts, not payment or electronic money accounts (except for two institutions, authorised in France, which have requested to be included in FICOBA).
- FICOBA only contains institutions accredited in France, but not those accredited in another EEA country and operating under the European passport. Although institutions operating under the freedom to provide services need not appear in the French FICOBA, the issue of establishments operating in France under the freedom of establishment needs to be clarified:
  - Institutions operating as branches may issue IBANs starting with FR. However, to date, they do not seem to have been included in FICOBA. Nevertheless, registration with FICOBA should be possible under the current
state of regulations, insofar as they are «institutions or bodies subject to the control of the administrative authority which usually have custody of securities, shares or cash» (Art. 1649A of the French General Tax Code relating to FICOBA).

- Institutions operating in France solely through agents or distributors should – from Tracfin’s point of view – be able to be included, but are not because they do not have an IBAN starting with FR.

**Types of accounts included in FICOBA (as of the end of September 2018)**

<table>
<thead>
<tr>
<th>Type of Account</th>
<th>Approved in France</th>
<th>Approved in the EEA, operating under freedom of establishment (IBAN beginning with FR possible)</th>
<th>Agréé dans l’EEE, exerçant en LPS (IBAN non français)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Institution (CI)</td>
<td>YES</td>
<td>NO even though regulations could allow it</td>
<td>NO</td>
</tr>
<tr>
<td>Payment Institution (PI)</td>
<td>NO (except for one PI that is included, whereas the regulations allow them all to be included)</td>
<td>NO even though regulations could allow it if it had a French IBAN</td>
<td>NO</td>
</tr>
<tr>
<td>Electronic money institution (EMI)</td>
<td>NO (except for one EMI that is included, whereas the regulations allow them all to be included)</td>
<td>NO even though regulations could allow it if it had a French IBAN</td>
<td>NO</td>
</tr>
</tbody>
</table>

- European regimes must be harmonised to facilitate international cooperation

Within the European Union, some countries have yet to introduce national centralised bank account registries. Directive (EU) 2018/843 amending the 4th Anti-Money Laundering Directive has made doing so a priority: it requires all Member States to have national account registers, so that each FIU knows the exact number of bank accounts and payments an individual has within its jurisdiction.

This provision enhances the effectiveness of international operational cooperation between EU FIUs. By querying its counterparts, a FIU in a given Member State will be able to quickly find out the exact number of bank accounts, payments and electronic money available to an individual within the EU. Above all, the counterpart FIUs will be able to quickly issue requests for information to assist in the financial investigation conducted by the FIU that initiated the request for cooperation. When gathering financial intelligence related to suspected terrorist financing, this will ensure efficiency, speed and thoroughness.

**ENACTING DIRECTIVE (EU) 2018/843**

Directive (EU) No. 2015/849 of 20 May 2015 (the so-called «Fourth Directive») represented a milestone in improving the European AML/CFT system. However, the attacks in Europe, and particularly in France in 2015 and 2016, have underscored the need to further strengthen AML/CFT capacity. Another reason for doing so lies in ongoing, rapid changes in the financial system.

Under the impetus of France, among others, the EU has launched efforts to amend the Fourth Directive, which led to the publication on 19 June 2018 of Directive (EU) 2018/843 (sometimes referred to as the «Fourth Directive bis» or the «Fifth Directive»).

This directive must be completely enacted in every EU country by 10 January 2020. The overall effectiveness of the European AML/CFT system will depend on how this directive is applied in the various Member States.
In France, the measures introduced by the 2018 amendment have already largely been integrated into the French Monetary and Financial Code. Efforts to enact the Fourth Directive into French law overlapped with European discussions on how to amend it. When enacting the Fourth Directive by means of Order no. 2016-1635 of 1 December 2016, France anticipated certain amendments introduced by the 2018 directive.

Specifically, to better regulate the activity of PS/EMSPs at European level, Directive (EU) 2018/843 provides for:

– Lowering thresholds applicable to electronic money for which due diligence measures are not required
– Adapting customer identification requirements to new existing technical devices. In particular, it incorporates electronic means of identification provided for in the European eIDAS Regulation.1

**DIRECTIVE (EU) 2018/843, AMENDING THE FOURTH DIRECTIVE, LOWERS CAPS ON THE ANONYMOUS USE OF ELECTRONIC CURRENCY**

Article 12 of the Fourth Directive allowed Member States not to apply certain due diligence measures for electronic money that met various conditions: load and use caps, loading procedures, supervision of use, etc.

Directive (EU) 2018/843 of 30 May 2018 is a reflection of the European Union’s hardening stance concerning electronic money. These conditions have been bolstered (in particular by lowering load and use caps), thus reducing the scope of electronic money benefiting from the easing of due diligence measures.

In its original version, the Fourth Directive allowed electronic money payment instruments to be sold without requesting ID if all the following conditions were met:

- The instrument is not rechargeable, or has a payment transaction limit of €250 per month
- The maximum amount stored on the instrument does not exceed €250
- The instrument is used only for the purchase of goods and services
- The instrument cannot be loaded using anonymous electronic money.

As amended by the 2018 Directive, the storage cap and monthly payment limit have been reduced to €150.

In addition, cash withdrawals and redemption in cash of the electronic money balance were capped at €100. The amended Fourth Directive lowers this ceiling to €50.

Directive (EU) 2018/843 also requires reporting entities to implement due diligence measures for online payment transactions that exceed €50.

Lastly, Directive (EU) 2018/843 provides that Member States may decide not to accept payments made using anonymous prepaid cards within their territory.

---

HARMONISING NATIONAL LEGAL SYSTEMS AND THEIR IMPLEMENTATION WITHIN THE EU

The differences between AML/CFT regulations in the EU Member States – not to mention the varying levels of supervisory compliance requirements – lead to the most rigorous countries being inadvertently exposed to risks introduced by countries that are less strict.

One short- and long-term priority involves harmonising practices for supervision and monitoring compliance with AML/CFT obligations by reporting entities within the EU.

In July 2018, the Commission decided to refer three Member States (Romania, Greece and Ireland) to the Court of Justice of the EU for failure to implement the 2015 Directive. The Commission accused them of AML/CFT failure. Other Member States have also been asked to step up their efforts.

At the same time, the prospect of Brexit is a major unknown. The UK is currently the country of accreditation for many PSPs operating in France and the rest of Europe operating under the European passport. Some of them have been assessed by Tracfin as presenting high AML/CFT risks.

At the end of September 2018, the prospect of the United Kingdom leaving the EU without an agreement (scheduled for 31 March 2019) seemed plausible. The various possible scenarios are subject to uncertainties.

– The UK could successfully negotiate an agreement with the EU to maintain the equivalent of the European passport for the benefit of the financial services sector. There would then be a risk that PS/EMSPs authorised in the United Kingdom could continue to provide services in Europe, whilst at the same time limiting the scope for national supervisors to monitor, if not de jure, then at least de facto.

– The UK could lose the benefits of the European passport, which would require PS/EMSPs that had a British accreditation to move and apply for a licence in another EU country. This can lead to regulatory dumping behaviour on the part of some European markets. In addition, the UK might – in response to the loss of the passport – be tempted to turn isolationist and establish itself as a world-class offshore financial centre, without any of the limitations provided for under European regulations.
REGULATING CRYPTO-ASSETS AT DOMESTIC AND INTERNATIONAL LEVELS
What term should we use – virtual currencies, crypto-currencies, crypto-assets, digital assets? There is an ongoing terminological debate on the nature of these new instruments. According to the Banque de France, the term «currency» should be avoided since these instruments only imperfectly fulfil the functions associated with legal tender. However, French translations of European provisions use the term «monnaies virtuelles», which is a literal rendition of «virtual currencies». For other analysts, the term «assets» is also inexact: these instruments have no use value and no expected income flow. However, it appears that the Business Growth and Transformation Action Plan (PACTE) bill has chosen to use the generic term «digital assets».

In this report, Tracfin uses the term crypto-assets, whether these instruments are used as means of payment (units of account and trading intermediaries) or as speculative assets (store of value). In the specific case of ICOs (Initial Coin Offerings), the term «tokens» may also be used.

The use of crypto-assets has continued to expand, despite uncertainties about exchange rate trends, the concentration of mining activities, the viability of technologies or their energy costs. This can be seen in the growing number of users and the responses of various economic stakeholders. Among other initiatives, a global smartphone manufacturer is proposing to include a wallet app as part of its devices, a mobile bank is offering its customers an interface that allows them to buy, sell and pay in bitcoins directly without recourse to specialised exchange platforms, and investment banks are setting up crypto-asset trading teams.

The high AML risks of crypto-assets have been described in Tracfin’s “2016 risk trends and analysis” report. They mainly have to do with anonymity, especially for blockchains that have been deliberately set up to erase the traceability of transactions. Platforms that exchange one crypto-asset for another (the so-called cryptocurrency exchange platforms) currently play a major role in money laundering circuits, by making it possible to convert crypto-assets based on traceable blocks (Bitcoin, Ethereum) into those based on untraceable blocks, thus ensuring that transactions are anonymous.

In addition, crypto-assets are particularly propitious for a variety of scams: exchange rate manipulation (whose risks increase with the concentration of mining activities), cyberattacks against exchange platforms and users’ computers (ransomware payable in crypto-assets), fake investment sites (scams) and fundraising for non-existent projects.

In light of the risks, the ever-widening use of crypto-assets, the increase in the number of related professions, the development of blockchain projects and crypto-asset fundraising (ICOs) call for stepped-up efforts, both at domestic and international level, to define and implement a regulatory framework, at least in terms of AML/CFT.
PROVEN AML/CFT RISKS OF CRYPTO-ASSETS

The risks inherent in the use of crypto-assets – as previously shown by Tracfin – were confirmed during 2017 and the first half of 2018.

A SHARP RISE IN TRACFIN’S CRYPTO-ASSET-RELATED ACTIVITIES

In 2017, Tracfin received 250 suspicious transaction reports directly related to the use of crypto-assets, an increase of 44% over 2016. Given the results from the first half of 2018, this volume is set to double. The rapid rise in the number of STRs is proof positive of the expanded use of these instruments. In absolute terms, however, the number of STRs submitted remains low and is not necessarily a reflection of the significance of the risks of fraud and money laundering linked to the use of crypto-assets. Most of the information received is submitted by banking institutions.

THE MAIN RISKS IDENTIFIED BY TRACFIN IN LIGHT OF STRS RECEIVED

Several trends emerge from the reports handled by the Unit:

– Laundering the proceeds of tax evasion: this concerns individuals who receive sizeable deposits into their French or foreign bank accounts from exchange platforms, most often based in foreign countries. The individuals may be French tax residents, who state that they have successfully invested in crypto-assets without justifying the funds’ origins. They may also be non-residents who wish to transit money through France or make use of income concealed from their country of residence.

THE TAX REGIME APPLICABLE TO GAINS FROM THE RESALE OF CRYPTO-ASSETS

In its decision of 26 April 2018, the Conseil d’État specified the tax regime applicable to gains derived by individuals from the sale of crypto-assets. The Conseil d’État does not statute on the possible monetary nature of bitcoin and refers to the classification of goods as provided for under France’s Civil Code. It compares crypto-assets to intangible movable property. Three cases are then possible:

– If the individual earns occasional capital gains, they are subject to the capital gains tax on movable property regime as provided for in Article 150 UA of the French General Tax Code.

– If the individual earns capital gains on a regular basis as a «miner», this is considered compensation for a gainful activity that is liable for income tax under the category of non-commercial profits (BNC).

– If the individual engages in the buying and reselling of crypto-assets, these are commonly-earned capital gains that are liable for income tax under the category of industrial and commercial profits (BIC).

1 EC, 26 April 2018, No. 417809.

2 The Conseil d’État’s position differs from that of the tax authorities, who believe that this type of gain should be liable for income tax system under the category of non-commercial profits (bénéfices non commerciaux – BNC). Cf. § no. 1080 of the administrative comments published on 11 July 2014 in the official tax bulletin (BOFiP), updated on 3 February 2016 without change concerning this point. The Conseil d’État’s position results in an effective tax rate of 36.2% (withholding tax of 19% + social security contributions of 17.2%). In many cases, it is not more favourable than the progressive income tax scale as proposed by the tax authorities.

3 With respect to the bitcoin blockchain, «mining» consists of taking part in the proper functioning of the blockchain by providing computer and computational resources to validate transactions electronically. This is done in exchange for compensation paid to the «miners» in bitcoins.

3 With respect to the bitcoin blockchain, «mining» consists of taking part in the proper functioning of the blockchain by providing computer and computational resources to validate transactions electronically. This is done in exchange for compensation paid to the «miners» in bitcoins.
act as crypto-asset brokers for third parties without obtaining prior authorisation.

- Fraud schemes: these consist of fake, unauthorised investment sites, which have been condemned by the Autorité des Marchés Financiers (AMF). The development of such sites picked up in the last quarter of 2017 due to the surge in the price of bitcoins (see Chapter 3 of this report, pp. 26-27).

- Cyberattacks: Tracfin observed financial flows to exchange platforms from French companies which suddenly made isolated bitcoin purchases. These were victims of a ransomware. This type of application, developed by hackers, is introduced into dealing in illegal goods: Lastly, Tracfin deals with financial flows to dark web marketplaces hosting platforms for the purchase or sale of illegal products: drugs, weapons, stolen bank details, false identity documents, child pornography, etc. Transactions on these platforms are carried out in encrypted form to preserve the anonymity of the participants. These illegal platforms must be identified and shut down. In the spring of 2018, after nearly a year of investigation, the National Directorate of Customs Intelligence and Investigations (DNRED) broke up a major dark web operation known as the «Black Hand». In June 2018, the Spanish Guardia Civil, working closely with the Austrian police and Europol, dismantled a dark web network focused on the production and distribution of synthetic drugs on the dark web, profits from which were laundered through the sale of crypto-assets (more than €4.5 million in bitcoin, IOTA and lumens). Among those arrested was a French national.

COMBINED PAYMENT SERVICES IN LEGAL TENDER AND THOSE IN CRYPTO-ASSETS

Tracfin has pointed out the risks of combining payment or money transfer services that use legal tender and the use of crypto-assets, which makes it possible to mask the traceability of flows.

One important risk resulting from the hybridisation of the two types of payment services is legal tender payment cards backed by crypto-asset wallets (so called «BTC-to-plastic»), which Tracfin has already flagged up.

Introduced in 2013, these cards make it possible to make purchases from brick-and-mortar or online retailers and to make cash withdrawals from ATMs. The balance available on the card is the real-currency equivalent of the amount of crypto-assets held by the user. They are marketed and sold by specialised companies that use payment or electronic money institutions to manage payment flows and handle the related regulatory constraints.

BTC-to-plastic cards are widely used by criminal gangs that sell illegal goods online and are paid in crypto-assets. These cards allow them to withdraw the ill-gotten gains in cash.

In early 2018, these cards suffered a setback due to the weakness of their issuers’ AML/CFT provisions. Most of the cards used in the EU, which were sold under various names, were issued by a single electronic money institution, Wavecrest Holdings Ltd, registered in Gibraltar.¹ At the beginning of the year, VISA and MasterCard decided to exclude this EMI from their network for failure to comply with its contractual compliance obligations. All payment cards issued by Wavecrest were then deactivated. The commercial companies involved had to suspend the functionalities of their prepaid cards within the EEA, leaving users with access solely to their crypto-asset wallets.

¹ In France, Wavecrest sold «BTC-to-plastic» payment cards under the freedom to provide services regime.
THE RAPID GROWTH IN ICOS: THE NEED FOR A REGULATORY FRAMEWORK

Crypto-active fundraising operations are called initial coin offerings (ICOs), by analogy with initial public offerings (IPOs). They have developed outside any regulatory framework, as digital tokens offered for sale do not have the legal character of financial instruments. They are not, however, illegal.

Funds raised through ICOs have soared since 2017. More than 2,000 ICOs took place worldwide in 2017, compared to about 60 in 2016. Some were carried by French teams (more specifically by a primarily French-speaking team from France). With 50% of the dedicated market share, Ethereum is the main blockchain used to carry out ICOs, due to its performance in the automated management of exchanges between investors and project leaders (smart contracts).1

As with any entrepreneurial project developed ex nihilo, many blockchain projects that raised funds via ICOs proved to be economically non-viable.

HOW ICOS WORK

An entrepreneur develops a blockchain dedicated to a new project (an online game, cloud services, domain name auction site, etc.) through which he or she issues tokens:

– Tokens are offered for sale to investors, who pay in crypto-assets (bitcoin or ether), although some projects can be financed using legal tender. The transaction is most often carried out on the Ethereum blockchain, which, thanks to smart contracts, secures exchanges between the tokens of the blockchain used for the project and the amount of bitcoins or ethers involved.

– Tokens give investors various rights with respect to the issuing project, such as the right to future dividends on income generated by the project; voting or governance rights, the right to use the project, the right to a service offered by the issuer, etc.

– Once the project owner has collected bitcoins or ethers from its investors, he or she can use exchange platforms to convert crypto-assets into legal tender and finance operations, such as leasing premises, computer equipment, hiring staff, and so on.

1 The term smart contract refers to an automated transfer of values managed by a blockchain and based on mutually-agreed-upon terms between the parties.
ICOs offer a number of possibilities in terms of money laundering and fraud.

Illicit funds may be used to purchase tokens, which can be sold on to other investors and then converted into legal tender. The launderer can then justify the funds by stating that he or she has financed a project and has made a profit. Hence the importance of being able to verify, at the ICO launch, the origin of investors’ funds.

The upsurge in ICOs on an international scale has also created a window of opportunity for fraudsters offering fictitious projects. As reported by experienced investors in specialised fora, many ICOs have turned out to be scams. There are specific websites that list fraudulent ICOs.

ICOs have developed without a regulatory framework. In France, however, a number of stakeholders already understand the importance of verifying the identity of their investors, if only to protect themselves in the event of regulatory changes in this area. Project owners, however, do not have in-depth knowledge of the AML/CFT system and do not always possess the means to take adequate KYC measures.

Very often they employ specialists, known as KYC providers. These providers, who are generally based outside France, provide identity check and verification services. These outsourced services can be expensive for project owners, although they are inadequate. KYC providers do not store data and are not liable if a project owner decides to accept or reject an investor.

A legal framework seems necessary in order to protect investors and encourage economically sound project owners. To this end, in 2017 the AMF launched a public consultation with the various financial stakeholders with an eye to sketching the outlines of a regulatory framework. The goal is not to strictly regulate this new activity, since the transactions so far are quite varied in nature.

The AMF has proposed creating a voluntary system for certifying projects. Any project owner in France who wishes could request certification from the AMF. The AMF would then check that the project provides sufficient guarantees to protect investors, including:

- A white paper that is sufficiently clear and accurate
- Creation of a company – a legal entity that would be responsible for the project
- Creation of an escrow account to protect investors’ funds
- A KYC obligation vis-à-vis investors to factor in the AML/CFT dimension
- Proof that a liability insurance policy has been taken out
- The AMF would audit the computer code used

Financial stakeholders have understood the advantages of such a certification system and are in favour of it. On this basis, investors can more easily distinguish between serious projects and possibly fraudulent ones.

The Business Growth and Transformation Action Plan (PACTE) bill, which was debated in Parliament in the autumn of 2018, could lead to the establishment of such a system. However, it is important to note that a voluntary scheme may not be sufficient to reduce AML/CFT risks.

---

1 For investors, the only information available is the document that the project leader decides to publish, known as a white paper. The content is not standardised and is not required to comply with any legal requirements. It may contain inaccuracies, omissions or unrealistic forecasts. It may also fail to indicate the competent court in the event of a dispute.
TRACFIN IS ADAPTING ITS ORGANISATION AND RESOURCES TO BETTER MONITOR THE CRYPTO-ASSETS SECTOR

A DEDICATED TEAM OF ANALYSTS

To bolster its expertise and improve its investigative capabilities, in June 2018 Tracfin set up a new investigative division devoted to financial cybercrime, and tasked certain investigators with analysing crypto-asset transactions.

This dedicated team has three goals:

- Developing its ability to analyse transactions registered in public blockchains
- Strengthening ties with the leading investigative departments in this area, primarily French Customs (Cyberdouanes) and the French Gendarmerie (C3N)
- Forging international partnerships, since the specific environment for crypto-asset products and the foreign location of many of this sector’s stakeholders require enhanced cooperation with other FIUs
- Tracfin’s specialised analysts are also able to refer to the courts cases of fraudulent introduction and modification of data into an automated system, and obstructing the operation of an automated data system, without prejudice to financial offences.

Case study no. 16: Insertion of a malware and bitcoin mining without the knowledge of computer application users

«Mr X», a computer specialist, sold file copying software, hardware comparators and online role-playing games online. Customers were offered the choice of paying in euros or crypto-assets (bitcoin or nextcoin). In addition to the paid versions of his software, Mr X also offered a free downloadable version. However, one of these applications contained a malware. Once installed, the application used the computing power of the victim’s computer equipment to mine bitcoin without his or her knowledge.

Bitcoin mining is the process by which «miners» electronically validate blocks of transactions in a blockchain, using mathematical combinations. When the right combination is found, the miner receives a reward in bitcoins.1 Bitcoin mining consumes large amounts of electrical energy and requires powerful computing equipment (graphics capacity in particular). By inserting a mining function into his victims’ computers, Mr X saved himself significant operating costs while reaping the benefits of the calculations performed.

Thus, in addition to profits from the sale of his software applications and his own exchange transactions, Mr X earned nearly 50 bitcoins in a few weeks from his mining activities – or about €160,000 at the then current exchange rate. To collect the revenues from the sale of his applications, Mr X used his own addresses (public keys), which were not affiliated with a platform. To conduct his exchange transactions, he used both a French and a foreign platform.

Once the bitcoins had been converted into legal tender, for an identified total of over €200,000, Mr X transferred these funds to bank accounts abroad, which were ultimately seized.

---

1 The Bitcoin blockchain is programmed in such a way that the amount awarded to miners for each validated transaction decreases over time, as the number of bitcoins overall issued on the blockchain increases.
The mining operations described above occurred between 2013 and 2016, at a time when mining was highly profitable for individuals using their personal computers. Since 2016, the decrease of the rewards value and the transformation of crypto-asset production techniques have significantly reduced the profitability prospects of «home-grown» mining efforts. Bitcoin mining is now carried out on an industrial scale by «mining farms».

**DISCUSSIONS WITH REPORTING ENTITIES ABOUT RISK CRITERIA**

Credit institutions are facing increasing use of crypto-assets by their customers. However, banks remain suspicious as for this type of transaction, given the difficulties in identifying the funds’ origins, and in distinguishing between individual use, brokerage/trading activities on behalf of third parties, and illicit uses.

Risk criteria provide guidelines for analysis, helping these institutions better formulate suspicions on crypto-asset-related transactions:
- The history of the customer relationship
- The customer’s profile: age, place of residence, sector of activity
- The economic justification for entering into a relationship with the institution
- The correlation between the amount of flows related to crypto-asset products and the customer’s profile
- The functioning of the account: are transactions to or from exchange platforms occasional or regular? Is the account exclusively devoted to exchange platform transactions?
- In the case of flows to platforms: are they preceded shortly before by transfers of comparable amounts from third parties? In this case, is the justification of the origin of the funds satisfactory?
- In the case of flows from platforms: can they be reconciled with previously issued transfers? Are the funds immediately re-invested?
- The name and location of the exchange platforms used: compliance measures vary in quality
- As far as possible, the nature of the crypto-assets that are the subjects of the transactions: some crypto-assets are known to prioritise anonymity

Professionals in the crypto-asset sector face serious difficulties in their relations with banks, starting with account management. Hence the need for robust regulation that can take into account this new sector’s specific risks, while remaining proportionate and appropriate, to allow for the virtuous development of crypto-asset professionals within France. Overly-rigid national regulations could encourage these stakeholders to establish themselves abroad. When it comes to AML/CFT, stakeholder flight would lead to a loss of visibility concerning this type of asset, due to the lack of reporting entities. A new balance must be struck.
CONVERGENCE OF INTERNATIONAL DISCUSSIONS TOWARDS INTRODUCING APPROPRIATE REGULATION

Regulation of the crypto-asset market has become a top financial priority for international, European and French authorities. Points of convergence are emerging:

- **At international level**, a FATF working group (the Policy and Development Group) is directing its efforts towards revising the 40 recommendations that shape national AML/CFT frameworks to include the issue of crypto-assets. To this end, it is committed to listing all crypto-asset-related activities, in a bid to list those that are comparable to financial services.

- **At European level**, Directive (EU) no. 2015/849 (the so-called «Fourth Anti-Money Laundering Directive») does not address the topic of crypto-assets. France nevertheless began subjecting exchange platforms to AML/CFT requirements starting in December 2016 (see 7° bis of Article L.561-2 of the French Monetary and Financial Code).

- **Directive (EU) 2018/843 of 30 May 2018 amending the Fourth Directive** requires all EU Member States to subject exchange platforms and custodian wallet providers to the AML/CFT framework by 10 January 2020 (see Article 1, 1) c) of Directive 2018/843).

- **In France**, the Business Growth and Transformation Action Plan (PACTE) bill, which was debated in Parliament in the autumn of 2018, contains a section dedicated to crypto-assets, making it possible to introduce a legal framework for sector stakeholders. This section of the bill has several goals:
  - A more exact definition of the nature of crypto-asset services that need to be regulated
  - Designation of one or more competent supervisory authorities
  - Defining obligations for the accreditation or registration of the various stakeholders with the appropriate supervisory bodies
THE SECTION OF THE PACTE BILL DEVOTED TO CRYPTO-ASSETS

In the autumn of 2018, discussions of the PACTE bill could lead to the following proposals:

1/ The creation of a generic concept of «digital assets», which would cover both crypto-assets used as payment instruments as well as speculative assets and tokens issued as part of ICOs

2/ The introduction of a regime for «digital assets» service providers, distinguishing five categories of services:
   - Buying or selling digital assets in exchange for legal tender (by so-called «fiat-to-crypto» exchange platforms)
   - Storing digital assets or cryptographic keys on behalf of third parties
   - Exchanging digital assets for other digital assets (by so-called «crypto to crypto» exchange platforms)
   - Operating a platform for trading digital assets
   - Services similar to financial services but in connection with digital assets (order reception/transmission, portfolio management, underwriting and investment, etc.).

The first two services (fiat-to-crypto exchange platforms and portfolio custody services on behalf of third parties) would require mandatory registration with the supervisor, implying full compliance with the AML/CFT framework.

In addition, for all five service categories, a voluntary approval process with the supervisor is presented as a competitive advantage. Supervisory approval, even on a voluntary basis, would lead to being subject to the AML/CFT scheme.

3/ The bill could also propose, for ICOs, to subject first-time buyers to AML/CFT requirements only upon the issuance of tokens.

Thus, at the end of the initial discussions of the PACTE bill in the National Assembly, the following are planned:

- An optional approval regime for ICOs
- An optional approval regime for many crypto-asset services, such as storage and brokerage, exchange platforms, order reception and transmission, portfolio management under mandate, advice to underwriters, underwriting and investment
- For fiat to crypto brokerage services, mandatory initial registration with the AMF, with approval remaining optional thereafter
- An account entitlement regime for ICOs who have been granted approval and accredited providers
- Finally, an article provides that specialised professional funds (SPFs) may now invest in crypto-assets (cryptocurrencies and ICO tokens), provided that they comply with the other conditions set out in 2° to 4° of Article L. 214-154 of the Monetary and Financial Code, in particular as regards liquidity and valuation.

Discussions are ongoing, in particular with respect to compliance by crypto to crypto exchange platforms, on which the FATF is also working.

The promulgation of the PACTE law could take place in spring 2019.
DEVELOPING AML/CFT DUE DILIGENCE IN THREE SECTORS: FINANCIAL MARKETS, THE ART MARKET AND THE NON-LIFE INSURANCE MARKET
In certain sectors of activity falling within the scope of intermediation in the broadest sense, proven AML/CFT risks have justified compliance by the primary professions concerned. However, the involvement of these professionals in the AML/CFT system should be expanded or strengthened. Faced with lobbying strategies advocating a return to an earlier state of affairs, Tracfin would like to highlight the specific risks associated with three sectors: financial markets, the art market and the non-life insurance market.

The financial and art markets are particularly susceptible to AML/CFT risks. Although the financial weight carried by the two sectors is not comparable, they share common characteristics: volatility in the prices of traded assets, uneven regulation depending on the market segments, technical and specific expertise that create a barrier to entry. These two sectors are currently insufficiently addressed by the French AML/CFT system.

Non-life insurance products, which are the subject of reduced vigilance under Article L.561-9 and 2° of Article R.561-16 of the Monetary and Financial Code, are nevertheless a valuable source of information for Tracfin, often complementary to other reporting entities. The cross-functional nature of these products makes it possible to collect information on many topics: laundering of criminal proceeds (car insurance in particular), laundering of the proceeds of corruption (home insurance) and terrorist financing (property and casualty insurance). Compliance by non-life insurance activities with the AML/CFT framework must be bolstered.

**MONEY LAUNDERING ON SECURITIES MARKETS: MANIPULATION OF THE SHARE PRICES OF LISTED COMPANIES; LAUNDERING THE PROCEEDS OF INSIDER TRADING**

Both Tracfin and the reporting entities still take insufficient account of the risks of money laundering on the financial markets in spite of the fact that particularly large amounts are at stake.

Risk levels vary according to the features of each market: volumes, liquidity, organised or over-the-counter market, home country of the stakeholders and market infrastructure. Regulated markets based in France, for which Tracfin is able to obtain information, seem to be less exposed than international currency and commodity markets. These markets do nevertheless carry risks owing to price manipulation and insider trading on the securities markets.

**PRICE MANIPULATION ON ORGANISED SECURITIES MARKETS**

Tracfin has handled a number of cases involving price manipulation using comparable methods. A typical example is that of a medium-sized enterprise listed on the free market. The majority of shares are owned by a lead shareholder.

– Over a two to three year period, the share capital is frequently restructured with an eye to reducing the par value of the shares to foster price volatility.

– Next, accomplices purchase blocks of securities which pushes the share price up. These sales of securities may be carried out over-the-counter: in this case, the buyer is able to defer payment for the purchased securities and subsequently retract. However, the transaction will have been recorded in the marketplace and have favoured a price rise.

– The upward trend is maintained whilst the lead shareholder sells his/her/its shares at the highest price, often to ill-informed individuals who are contacted by telephone by pseudo-brokers. At the end of the process, the share sale price is vastly over-inflated. The value bears no relation to the company’s economic realities (net assets, number of stores or headcount, etc.).
Case study no. 17: Suspicion of fraud by price manipulation and conspiracy to launder money

“Company Y” was listed on the free market of the Paris stock exchange. It was jointly owned by two parent companies with each having a 35% stake. These companies were themselves held by two shareholders who were individuals.

• Over a three-year period, “Company Y” underwent frequent share capital restructuring to bolster its shareholders’ equity and to substantially increase the number of shares and reduce their par value, which fostered price volatility.

• In 2015 and 2016, both parent companies carried out major stock market transactions by exchanging “Company Y's” securities between themselves to support the share price. The price was around €1 per share.

• In mid-2016, there was a major over-the-counter transaction on a block of 15% of the capital for a price of €1.5. The buyer was an accomplice third part company: “Company Z”. The transaction caused the share price to rise.

• However, a month later, the buyer retracted and returned the shares to the two initial shareholders. As this was an over-the-counter transaction, the buyer was not obliged to immediately pay for the purchased securities and this makes it easier to retract. However, the share price was influenced as the transaction had been recorded on the market.

• In late 2016 and early 2017, the two initial shareholders sold their shares at the highest price (between €3 and €6) to individual investors in France and Europe. When necessary, the individuals were contacted by telephone. As a result of these sales, the two shareholders collected more than €5 million and transferred the majority of this amount to companies and non-profit organisations set up abroad with straw men and which had accounts in a number of European countries (UK, Cyprus, Poland, etc.). The unit price of the sold shares seemed hugely over-inflated in view of the intrinsic value of “Company Y” which only had one physical store, had not reported any earnings for the last two years and had net assets of far less than its valuation. Consequently, as from the end of July 2017, the share had lost 90% of its value at the expense of the various individual shareholders.

Tracfin handled a second case with the same protagonist: “Company Z”. This supported the fact that this was an organised crime network. Through some of its employees, “Company Z” appeared to have links with individuals who were known, and had been sentenced, in France for large-scale financial fraud (forgery and use of forgeries, misuse of company assets) and for money laundering.

Laundering the proceeds of insider trading

Insider trading - and laundering its proceeds - is the other main offence noted on the securities markets.

Cas no. 18: Laundering the proceeds of insider trading and misuse of company assets

A national partner drew Tracfin’s attention to an independent investor, “Mr X”, who was based in Paris and who managed his assets himself. He was known to French and foreign market authorities for major insider trading offences, some of which had led to judicial investigations.

“Mr X” had set up a large number of companies, including “Company F” and “Company G”.

• “Company F” was a holding company registered in Paris. It held shares in around thirty companies operating in different sectors: land and property rental, catering, IT services, business consulting, etc.

• “Company G” was an offshore company registered in a Pacific island.

Both these companies speculated based on insider information. They used securities accounts opened with brokers and linked to bank accounts with credit institutions on the American continent. In this way, the two companies made gains of over $3 million each.

Tracfin’s investigations revealed a number of suspicious transactions involving “Company F”:

• “Company F” received at least €1 million from “Company G” as well as other funds from a broker. It was suspected that these amounts originated from illegal stock market transactions.
Case study no. 18: Laundering the proceeds of insider trading and misuse of company assets

Mr X, co-partner in Company F, a holding company for various activities such as land and property, catering, IT services, consulting, etc. détient a bank account in the Americas (Brokers).

Company F had bank accounts in a number of European countries. It carried out regular transactions between its accounts without the origin of the funds being identified.

Lastly, Company F booked expenses that were unrelated to its corporate purpose: transfer in 2016 of €30 million to a foreign company with no equity relationship, payment of rent for a private residence, works in a holiday home, etc.

Furthermore, Mr X directly owned a French property holding company (SCI) which had bank accounts both in France and in a neighbouring country. This SCI carried out purchase/sale transactions on shares which were part of legal proceedings instituted abroad although the French SCI was not itself implicated. The SCI made a profit of €600,000.

Tracfin’s investigations also brought to light several transactions carried out by a partner of Mr X within Company G. The partner received €200,000 from Company G via the French company that he owned. He had bank accounts in the UK, some of which had not been declared to the French tax authorities. Hundreds of thousands of euros passed through these accounts. In 2014, one of this partner’s companies acquired a villa in the south of France. The former owner was the foreign company that received €30 million from Company F in 2016.

All these transactions could represent laundering of the proceeds of insider trading and misuse of company assets. The case was subject to joint action by a number of relevant national partners.
Violations of stock market law are of particular interest to Tracfin. They represent a major vehicle for money laundering involving substantial amounts and elaborate techniques. Certain stakeholders may have connections with members of criminal networks.

In 2019, Tracfin will strive to expand its detection and investigation capabilities on capital markets:

- By restarting discussions with reporting entities, especially investment companies, investment management companies (SGP) and financial investment advisers (CIF). In the main, reporting by these professions can be vastly improved in light of the stakes. In 2017, Tracfin received 62 suspicious transaction reports from investment companies, 63 from investment management companies and 57 from financial investment advisers.
- By bolstering operational cooperation with the Autorité des Marchés Financiers (AMF), particularly as regards market investigation methods.

THE ART MARKET IS STILL HIGHLY VULNERABLE TO MONEY LAUNDERING RISKS

The global art market is still thriving. According to the Voluntary Auction Council’s 2017 annual report on public auctions, the “art and collectibles” segment of the global market was estimated at €28 billion that year (up 6.1%). France has a 6% market share, putting it in fourth place, far behind China (36%), the US (34%) and the UK (12%). In 2017, in France, all the segments of the public auctions sales sector represented total bid amounts of €3 billion (up 5.2%).

The art market is highly vulnerable to money laundering owing to the lack of transparency of certain practices (price volatility, cash transactions, etc.). Since the conflict in the Levant began, with the attendant looting of museums and archaeological sites, there has been an uptick in the risk of terrorist financing. It should be noted that art market professionals are little implicated in the AML/CFT system and that compliance has only a minor role in the sector’s professional practices. Tracfin is taking action to raise awareness and train but a large proportion of the profession play down the risks.

A THRIVING MARKET CHANNELLING NUMEROUS RISKS

- The international development of flows
By its very nature, the international network of major art auction houses fosters the sidestepping of actions to verify and monitor works placed on the market and the related financial flows. For French professionals, one of the major problems of auctions in France is the lack of European and international market harmonisation. This generates a severe competitive imbalance between incumbent voluntary auction operators, which work at national or regional level, and the major international auction houses. The latter need to have in-depth knowledge of their customer base to avoid damaging their image and reputation.

- The speculative nature of the market
The art market is structurally vulnerable to money laundering risks owing to the highly speculative nature of works of art, particularly modern art, which can be both safe investments and collectibles. On the art market, it may be difficult to determine the value of a work as it may fluctuate significantly (particularly upwards), without obeying economic rationale. For the relevant stakeholders and those in the know, the market has its own internal logic. Professionals need to protect themselves from those who look to play the system to launder financial flows by taking advantage of a sector in which there is headroom for fraudsters.

Appraisal arrangements, which are subject to very varied criteria, can shield certain laundering operations which would otherwise be identified by the delta between the starting price and the sale price. It is in professionals’ interest to encourage higher prices but they have limited scope for unearthing any complicity between buyers and sellers who may manipulate prices for the purposes of money laundering.
With increasing numbers of market segments, virtuous stakeholders should adopt a medium-term strategy to protect themselves against such risks.

– **Cash payments**

As the antiques profession is largely unregulated, dealers readily accept cash payments without establishing the origin of the funds. The profession stresses the competitive distortion caused by the lack of standardised cash payment thresholds within the EU. Some countries, such as Germany, place no limits on the use of cash. Others, such as the UK and the Netherlands have no limits but, in practice, professionals may refuse cash payments in certain circumstances.

– **Terrorism financing**

Since 2013 and the emergence of Islamic State onto the international stage, the looting and trafficking of antiques in the Middle East and North Africa have reached unprecedented levels. The risks of looted antiques being put onto the market are now perceived as high. This is borne out by a number of ongoing customs procedures and legal proceedings in Europe: Seizure at Roissy airport in March 2016 of marble bas-reliefs looted in the Syria-Iraq zone, proceedings in Switzerland and Belgium against one of the leading Geneva-based art dealers for holding and trading in works of art thought to have been looted by Islamic State, and the arrest in Spain in March 2018 of another art dealer and two experts accused of trading antiques that had been stolen from Libyan archaeological sites.

**ONLINE AUCTIONS AND SALES: A GROWING RISK**

In 2017, the total value of online auctions in France stood at €1,158 million, up 18% over 2016.¹ This amount accounts for 37% of auctions using all sales methods.

The rapid rise in the number of works of art offered for sale on the Internet, and the corresponding financial flows, create high ML/FT risks. This is due to the fact that transactions are carried out online and the lack of traceability of both the works and funds in the event of fraudulent operations.

As Internet sales are constantly on the rise, it is becoming even more difficult for auctioneers to conduct customer due diligence. Moreover, payments are handled by intermediary websites. Websites such as “Interenchères” allow online purchases to be made without any verification of the buyer’s identity. Even voluntary auction operators admit that this is a new unregulated channel. Whilst certain customers’ desire for discretion can be understood, it should be mentioned that one of the advantages of the AML/CFT system is its confidentiality which protects the reporting entity.

The requirement of better customer due diligence together with the obligation, since December 2016, of identifying customers for transactions of more than €15,000 means that professionals should necessarily establish an Internet buyers’ file with an identity document having to be provided prior to any involvement in an online auction. However, it appears that nobody has taken any action in this respect.

Online auctions of works of art are arranged by voluntary auctioneers but, outside the framework of auctions, there is also online trading between individuals, or between professionals and individuals. An article offered for sale on the Internet may disappear and reappear a few days later on another website. Furthermore, it is even more difficult to tell a genuine item from a false article online.

---

¹ Total of online sales and e-sales backed by live sales. See Voluntary Auction Council’s 2017 annual report.
BOLSTER THE OVERSIGHT OF PROFESSIONALS: AUCTIONEERS, VOLUNTARY AUCTION HOUSES, ANTIQUE DEALERS AND GALLERY OWNERS

Reporting by auctioneers and voluntary auction houses is still too low bearing in mind this market’s momentum although it did rise sharply in 2016-2017. Auctioneers, who were poorly informed about the AML/CFT system and its guarantees covering the confidentiality and protection of sources, welcomed awareness-raising initiatives rolled out by Tracfin and their professional body. They are starting to send suspicious transaction reports on a more regular basis.

Nevertheless, the voluntary auction houses that record the largest sales are under-represented, or even non-existent, amongst art sector professionals having submitted STRs. The statistics seem to suggest that, as regards AML/CFT, the involvement of professionals is inversely proportional to their turnover.

With the exception of auctioneers, other art dealers (antiques and art galleries) are still resistant to the system. The culture of compliance is largely alien to them. They are also subject to very little regulation. Only a declaration filed at a prefecture is required to practise the profession. Certain people operating on the fringes of the profession obtain licences of sell off goods at trade fairs and exhibitions with a real risk of handling stolen goods. Antiques and artwork trade fairs and exhibitions are an issue in themselves as the legality of neither the transactions nor the prices is verified.

Order no. 2016-1635 of 1 December 2016, which wrote the Fourth AML Directive into French law, laid down a number of arrangements concerning these reporting entities by differentiating between, on one hand, people who habitually trade in antiques and works of art and, on the other, dealers in precious goods.

Furthermore, antique dealers and art gallery owners are not governed by a regulatory authority and are rather informally overseen by professional bodies of which membership is optional. Since these professions had become subject to AML/CFT arrangements in 2001, no supervisory or enforcement authority had been designated. All this changed with the Order of 1 December 2016 which appointed the Directorate General of Customs and Excise (DGDDI) as the supervisory authority for antiques dealers and gallery owners and the National Enforcement Commission as the enforcement authority.

RECAST THE LEGAL ARRANGEMENTS FOR THE INVENTORY REGISTER (LIVRE DE POLICE) AND ORGANISE FOR IT TO BECOME PAPERLESS

Professionals in the art sector are legally required to keep an inventory register. Failure to do so may lead to criminal sanctions. Nevertheless, this register has a number of shortcomings.

The information to be noted is scant and imprecise: no photographs of the items, lack of information about the buyer and the means of payment used. Regulations on making the registers paperless are incomplete. No ministerial order has supplemented Decree no. 2013-287 (amending Article R.321-8 of the French Criminal Code) on the conditions for keeping paperless registers and the technical requirements to be complied with. In light of the foregoing, paperless inventory registers can be kept on an ordinary Excel spreadsheet to and from which information can be freely added and deleted without the data being safeguarded. As a result, paperless registers are even more lax than paper ones for which formal requirements are regulated.

Broadening the scope of the inventory register, especially in its paperless form, would be an effective way of involving professionals and improving AML/CFT arrangements:

- Provide more information in the inventory register to enable full traceability of the article
- Extend the requirement to keep a paperless, secure and enhanced inventory register with, inter alia, photographs of the items being sold, to antique dealers and auctioneers, in addition to auction houses
CONSOLIDATE THE REPORTING OBLIGATIONS OF THE NON-LIFE INSURANCE SECTOR

Since the AML/CFT system was introduced, the entire insurance sector, within the meaning of Article L.310-1 of the French Monetary and Financial Code, has been subject to reporting requirements. It plays a much larger part in these arrangements than the financial and art market sectors mentioned above.

The most common schemes are tax evasion (in particular undeclared gifts and, to a lesser extent, assets held abroad) followed by abuse of weakness. Although they are less widely reported, misuse of company assets and fraud in the healthcare and benefits sector (in particular, through the involvement of fictitious companies) are still topical and raise significant financial issues. There are schemes related to terrorist financing in both the life insurance and non-life insurance sectors.

The 2012 Warsmann Act\(^1\) classified non-life insurance products in the “light vigilance” category provided for in Article L.561-9 of the French Monetary and Financial Code. Since the Act, a number of professionals in the sector consider that non-life insurance could be subject to even lighter AML/CFT regulatory requirements, or even be removed from the system.

In the same way as all French regulatory and supervisory authorities, Tracfin considers these reporting requirements to be necessary owing to their operational value. Certain groups of reporting entities, with significant economic influence on the insurance market, are also in agreement: in 2017, STRs received from the non-life sector jumped by 75.5%.

Submissions concerning non-life insurance present an immediate operational interest, including as regards terrorist financing. Most of the submissions from the insurance industry which were investigated by Tracfin’s Combating of Terrorist Financing Division related to the non-life sector. Non-life insurance products provide details and information on the customers’ environment which are especially relevant for Tracfin’s investigations into individuals suspected of terrorist financing.

These products can also help detect money laundering operations which may be connected with organised crime, in particular via accident reports with complicit witnesses or insurance fraud. The rationale for imposing reporting obligations on the non-life insurance sector is confirmed by the interaction between some areas of the underground economy and certain networks suspected of terrorist financing.

At institutional level, the FATF is currently overhauling its Risk-Based Approach Guidance for the Life Insurance Sector. It has formed a working group comprising representatives of supervisors (including the Prudential Supervision and Resolution Authority, ACPR) and private sector stakeholders. Against this background, discussions are also covering non-life insurance although the sector is not expressly addressed by the 40 Recommendations. This recasting of the guidance should be factored in with an eye to the FATF Mutual Evaluation of France in 2019.

---

\(^1\) Article 72 of Act no. 2012-387 on legislative streamlining and cutting red tape.
Case study no. 19 : Insurance fraud as part of organised crime

An insurance company submitted a report to Tracfin concerning a second-hand car dealership/repair shop which had taken out a professional vehicle insurance policy with a broker. Less than two years after the company had been set up, a suspicious fire in the garage destroyed ten vehicles that had been offered for sale. The inventory register showed that all the vehicles had been purchased for cash. Tracfin’s investigations revealed that the manager belonged to a criminal network operating in a number of areas (extortion by violence, burglary, theft and handling stolen goods, drug trafficking) which generated large amounts of cash. Purchasing the cars, the claim, and its consequence, the repayment, therefore represent two stages, namely placement and layering, of laundering the proceeds of criminal activities via insurance fraud.

Case study no. 20 : Money laundering using accident reports with complicit witnesses

An insurance company submitted a report to Tracfin concerning an individual, “Ms Y”, who had purchased a second-hand vehicle for €9,000 from a third party. Four months later, “Ms Y” declared a traffic accident in which the opposite party, “Mr Z” was at fault. The insurance company paid out €7,000 to “Ms Y”. Her bank subsequently contacted the insurance company to advise it that her accounts were being monitored and that she had paid the entire insurance money over to “Mr Z”. Following investigations vis-à-vis its counterparts, the insurance company discovered that “Mr Z” had already declared two similar accidents, including one with another of the company’s insurees, “Mr W”. It turned out that “Ms Y” and “Mr W”, who were not obviously connected, provided the insurance company with the same bank account number.

Tracfin’s investigations revealed that “Mr Z” had set up a fraud system using accident reports with complicit witnesses.

He was already known to Tracfin for suspected laundering of amounts of unknown origin using sports bets. The insurance company’s STR enabled it to be established that at least part of the “gambled” funds came from the insurance payments made following accident reports with complicit witnesses, in other words, from the proceeds of insurance fraud.
EXPLICITLY DEFINE POLITICALLY EXPOSED PERSON (PEP) IN FRENCH LAW TO BOLSTER THE FIGHT AGAINST CORRUPTION
FIUs have a central role in fighting corruption, either in terms of detection or by supporting judicial investigations. Since 2013, the French anti-corruption system has been significantly bolstered:

- Setting up the High Authority for Transparency in Public Life (HATVP)¹
- Creating the French Financial Prosecutor’s Office (PNF)²
- Ramping up of the French Anti-Corruption Agency (AFA)³

Tracfin has regular contact with the French Financial Prosecutor’s Office. Its work should also overlap with that of the French Anti-Corruption Agency. The latter Agency’s recommendations, which were published in February 2018, set out the initiatives to be rolled out by reporting entities, known as Anti-Corruption Compliance Requirements (OCA), pursuant to Article 17 of the Sapin 2 Act. The French Anti-Corruption Agency’s preventive actions and the French Financial Prosecutor’s Office’s repressive actions are set to complement each other.

In spite of this system, the Unit still only receives a fairly small number of STRs concerning suspected breaches of probity. Although it may be difficult to detect these violations, greater involvement by reporting entities in this field, with Tracfin’s support, could prove to be useful.

Every year, Tracfin sends other government departments between forty and fifty files that are directly related to suspected breaches of the duty of probity. Moreover, Tracfin also sends a great many files concerning tax evasion, misuse of company assets or breach of trust, which a judicial investigation could, ultimately, tie in with acts of corruption.

These files cover a number of areas: laundering the proceeds of corruption by foreign Politically Exposed Persons (PEPs), corruption of foreign public officials in international business transactions, private corruption and embezzlement by public officials in France, in particular, through subsidised non-profit organisations.

LAUNDERING IN FRANCE OF THE PROCEEDS OF THE MISAPPROPRIATION OF PUBLIC FUNDS COMMITTED ABROAD

The leading corruption (and laundering of the proceeds of corruption) risk pinpointed by Tracfin relates to certain foreign PEPs who misappropriate public funds in their home country and invest the proceeds in France. In 2017, almost half the files sent by Tracfin in relation to breaches of probity belonged to this category. The submissions concern the PEPs themselves, or target their inner circle who benefit from the proceeds of misappropriation or who are used to integrate the funds into the French economy.

Case study no. 21: Laundering funds illegally acquired by a businessman with close ties to Heads of State

Tracfin’s attention was drawn to a property purchase for which the origin of the funds used was unable to be determined. The buyer was a property holding company (SCI) which received funds from a bank account in a non-European country. Tracfin’s preliminary investigations revealed that the SCI had acquired two properties in the Greater Paris Region for a total amount of over €11 million. It appeared that the SCI was managed by a straw man.

¹ Act no. 2013-907 of 11 October 2013
² Constitutional Bylaw no. 2013-1115 of 6 December 2013
³ Act no. 2016-1691 of 9 December 2016 (the Sapin 2 Act)
⁴ Breaches of the duty of probity encompass corruption, influence peddling, unlawful taking of interest, favouritism, misappropriation of public funds and extortion by public officials.
Due to cooperation with a number of foreign FIUs, Tracfin discovered that the SCI’s beneficial owner was “Mr X”, an influential foreign businessman. He had acted as a go-between in the negotiation of major international weapons and infrastructure contracts with various countries. He was close to foreign political decision-makers and had been implicated by the judicial authorities of certain countries and by international institutions in acts of corruption and misappropriation of public funds. He was thought to have received kickbacks during the execution of a number of procurement contracts.

Furthermore, Tracfin’s investigations established that “Mr X” acquired works of art for €3 million, almost half of which was paid in cash.

“Mr X” has no personal bank account in France. However, a member of his family does have an account which is regularly credited with transfers from accounts held by “Mr X” in a European country.

**CORRUPTION OF A FOREIGN PUBLIC OFFICIAL AS PART OF MAJOR INTERNATIONAL CONTRACTS**

International cooperation between FIUs is crucial in the fight against corruption.

Tracfin regularly discusses with its foreign counterparts, especially with regard to leading international deals for which certain financial flows may have been conveyed through France. They often involve energy and commodity contracts.

**Case study no. 22: Public and private corruption in the awarding of oil contracts**

Tracfin received a request from a foreign counterpart concerning an international group that specialised in oil-related services (assisting multinationals with exploration-production projects in third countries). The group was undergoing a joint judicial investigation in three countries for corruption of public officials and private corruption. It was thought to have paid bribes to decision-makers in the Maghreb region, the Near and Middle East, and Central Asia in order to secure contracts and receive confidential information.

The group received funds from its backers via false invoices for subcontracting services issued by offshore companies. The funds were then paid over to the decision-makers in the relevant countries or to executives working for competitors who were willing to hand over sensitive information, via equally fictitious consulting services.
The implicated group had an entirely offshore organisational structure with the goal being opacity. The underlying concept was the systematic splintering of a large number of legal entities with each entity being itself splintered between registration in one country, residence in another, and bank accounts held in a third, etc. The aim was to remain elusive by ensuring a low profile for parent companies or operational companies which would put flesh on the group’s bones. The owner family ultimately used a number of international consulting firms and family offices to manage the group.

Tracfin’s investigations revealed that certain of the group’s oil-related foreign companies had bank accounts in France which were used to convey funds between the customer backers and a group entity based in Monaco. Over a three-year period, several tens of millions of euros transited through these accounts.

Moreover, the owner family made private property investments in France. A French limited liability company (SARL), whose shareholders included members of the family, collected over €800,000 from Caribbean offshore companies without supporting documentation. It distributed these funds to two SCIs to partly finance the acquisition of luxury villas in the south of France.

Case study no. 23: International embezzlement and laundering the proceeds of corruption

Similarly, Tracfin played a key role in the European arm of an international public fund embezzlement case at the expense of a sovereign fund. Some of the fund’s investments were financed by the issuance of bonds which were guaranteed by third party institutions. The premiums paid by the fund to these third parties as compensation for the guarantees provided were embezzled and collected by the guarantors’ namesake offshore companies. The total loss was estimated at several billion dollars with the beneficiaries being numerous high-ranking public officials and leading businessmen in a number of countries. The case led to several legal proceedings in different countries, including European countries.

Following a request from a European counterpart, Tracfin was able to discover that one of the beneficiaries of the embezzlement had placed part of the funds in a Caribbean company of which he was the beneficial owner. This company transferred almost €10 million to an account in the EU prior to investing them in the acquisition of a luxury villa in France.
Tracfin’s investigations revealed that the businessman in question was either a direct shareholder or beneficial owner of around fifteen French SCIs, which had been incorporated over a ten-year period, and which held property assets of €130 million.

**THE VULNERABILITY OF THE PROPERTY SECTOR AND THE ACCOUNTABILITY OF NOTARIES AND ESTATE AGENTS**

The corruption cases sent by Tracfin confirm the vulnerability of the French property sector to the risk of money laundering, especially in respect of funds originating from breaches of the duty of probity. This phenomenon was flagged up in the “2015 risk trends and analysis” report (pp. 51 to 54).

This calls for heightened due diligence from the sector’s professionals, particularly notaries and estate agents.

Tracfin would like to draw attention to the involvement of notarial offices in 2017 although the number of STRs received (1,400) is still low when compared to the number of recorded property transactions (One million per year1). Furthermore, Tracfin would like to be provided with more comprehensive information by the profession’s supervisory authorities concerning the sanctions handed down every year against any defaulting professionals.

Tracfin is also striving to increase the involvement of estate agents. On 6 November 2018, new AML guidelines were published jointly by Tracfin and the sector’s supervisory authority, the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF). These guidelines will help the profession understand its due diligence obligations and how to submit an STR to Tracfin. This action is also being helped by the convergent work of the National Enforcement Commission.

---

1 In 2017, 986,000 deeds of sale were drafted for pre-owned property (source: 2017 annual report of the Conseil Supérieur du Notariat (National Association of Notaries).
THE DEFINITION OF DOMESTIC PEPS SHOULD BE MORE SPECIFIC

Directive (EU) 2015/849 extended the concept of Politically Exposed Person (PEP) to include domestic individuals. It had previously only covered foreign individuals. Under French law, the definition of domestic PEPs is still under discussion and should be more specific.

In the French Monetary and Financial Code, PEPs are defined in Articles L.561-10, R.561-18 and R.561-20-2. They are people who hold or have held political, legal or administrative positions on behalf of the government during the year prior to the start of the relationship.

They are identified as being exposed to specific ML/FT risks. Legislation requires reporting entities to take special and additional due diligence measures vis-à-vis these persons.

These heightened due diligence measures also apply to the close acquaintances of PEPs:

- Family relations (Article R.561-18 (II): parents, children, partners, etc.)
- Business relations (Article R.561-18 (III): people having a close business relationship with a PEP)

This strengthened due diligence is legitimate as Tracfin regularly handles cases of breaches of probity committed by individuals holding public office in France. However, the precise scope of the political, legal and administrative positions covered by PEP classification should be specified.

Article R.561-18 of the French Monetary and Financial Code is a direct reproduction of the European definition set out in Article 2 of Directive 2006/70/EC of 1 August 2006, and reiterated in the Fourth AML Directive. In respect of domestic PEPs, the European definition raises many application issues as it does not provide for modulation according to the risks relating to such and such a PEP.

European legislation classifies the members of high-level judicial bodies whose decisions are not subject to further appeal as PEPs. In France this includes members of the Conseil d’État (French Supreme Administrative Court), the Cour de Cassation (French Supreme Civil Court) and the Cour des comptes (Government Audit Office). After over 25 years of detecting suspicious transactions, Tracfin affirms that these individuals carry very low ML/FT risks.

Conversely, the legislation does not stipulate, for instance, that the executive managers of local authorities (not even the largest) or the chairs of semi-public companies, which carry high levels of risks owing to their decision-making powers in managing budgets and awarding procurement contracts, should be considered as PEPs.

The drafting has not been improved by the work to write the Fourth AML Directive into French law. This inadequate definition requires reporting entities to carry out excessive due diligence measures on low-risk profiles. This change could compromise the credibility of the domestic PEP system. The enactment of the Fifth AML Directive into French law could provide the opportunity to review the classification and alignment of the list of domestic PEPs.
Case study no. 24: Use of non-profit structures by a local elected representative for the purposes of passive bribery, influence peddling and breach of trust

“Mr Y” was mayor of a mid-sized municipality and held positions in the agglomeration and region to which the municipality belonged. He chaired a non-profit cultural organisation. One of his close acquaintances chaired a non-profit training organisation. Tracfin was alerted to the way in which these organisations were managed and to the mayor’s lavish lifestyle.

Tracfin’s investigations revealed that, in addition to his official income, “Mr Y” had received almost €300,000 in three years in cheques and cash. The funds were taken from the budgets of the non-profit organisations. These organisations were financed either from the public purse or by companies that had been awarded procurement contracts signed by the town and community of municipalities for which “Mr Y” was an elected representative.

• The training organisation funded itself through services invoiced to local authorities. Its expenses included direct payments to the mayor’s private bank account and inconsistent payments of invoices (website development, report writing, etc.) issued by companies managed by mayor’s close acquaintances.

• The cultural organisation was mainly financed by donations of several thousand euros each made by engineering, public works and street lighting companies, as well as local authority service providers. The total budget was disproportionate to the organisation’s purpose. These donations were then transferred to the elected representative’s private bank accounts.

Funds from both these non-profit organisations were misappropriated by “Mr Y” for personal purposes. Over the period, “Mr Y” lost over €100,000 gambling.
HELPING FIGHT TAX EVASION, SOCIAL SECURITY FRAUD AND CUSTOMS FRAUD: A CORE TRACFIN ASSIGNMENT
At a conference on 13 September 2018, the Minister for Government Action and Public Accounts stated that, although fighting fraud is no longer a taboo subject, there is no reliable consolidated assessment of the scope of tax evasion and social security fraud. Attention is centred on notified adjustments but their results are difficult to interpret.

Experts in fighting tax evasion and social security fraud agree that upstream detection is crucial. This requires clear targeting criteria based on knowledge of risks and new forms of fraud. 90% of the amounts adjusted following tax audits concern factors identified prior to the audit with the remaining 10% covering new factors revealed during the audit.

Tracfin plays a decisive role in detection, especially through international cooperation which allows for identification of foreign bank accounts and assets that the tax authorities are not always able to be aware of.

Between 2009 and 2017, the proportion of STRs which more or less directly concerned tax evasion consistently rose to its current volume assessed to represent at least 30% of reports received. In 2017, tax matters were the main suspicion in over 20,000 STRs (i.e. 29% of reports received). Out of this total, half dealt with an undeclared business activity or reduced revenue, and a third with asset-based issues (undeclared gifts, possession of foreign bank accounts and assets, and reducing wealth tax liability).

When STRs lead to the discovery of complicated fraud arrangements with intermediaries and/or committed by organised crime and reveal violations other than tax evasion, they are handed over to the investigation divisions with an eye to referring them to the courts after analysis and enhancement of the financial intelligence (in particular, by using requests for information). Since 2010, 687 tax evasion files have been referred to the courts, i.e. around 100 per year. Generally speaking, these referrals cover one or more other violations: essentially offences of undeclared labour, misuse of company assets or breach of trust. They are very frequently connected with company management.

When Tracfin’s investigations only turn up evidence of tax evasion, the inquiry is only forwarded to the tax authorities with the Public Finances Directorate General (DGFiP) being tasked with applying ordinary law rules in view of an eventual referral to the courts.

TRACFIN’S VALUE ADDED IN FIGHTING TAX EVASION

Since 2009, the number of notes sent by Tracfin to the DGFiP has been steadily rising. In 2017, Tracfin sent 625 information notes to the tax authorities, up 79% over 2016 (350 notes). This increase can be attributed, on one hand, to detailed disclosures which rose from 350 in 2016 to 377 in 2017 (up 8%) but, above all, to the 2017 rollout of so-called “flash” disclosures which accounted for 248 referrals. The latter are intended to allow for fast use of data gathered by Tracfin which does not require in-depth analysis by the Unit but which may be useful for the tax authorities.

As at 31 December 2017, the DGFiP had filed over 100 complaints for tax evasion based on Tracfin’s notes and 60 files had been sent to the National Tax Crime Unit (BNRDF).

Tracfin’s “2016 risk trends and analysis” report highlighted the detection of undeclared foreign assets and abuse of rights related to misuse of share savings plans (PEA) or to inter vivos gifts followed by disposal. In this report, Tracfin draws attention to the fact that VAT fraud is still rife and represents major financial stakes. With regard to individuals, Tracfin underscores the risks of fraud on death duties, transfer duties and the taxation of investment income (RCM).
LEGAL ENTITIES: VAT FRAUD BY FORGERY (DEDUCTIBLE VAT)

In terms of volume, VAT fraud represents the largest tax shortfall for the French government and for other EU countries. A recent study published by the European Commission estimated the so-called “VAT Gap” at €147 billion within the EU in 2016, with a loss of €21 billion for the French government alone (i.e. 12% of the VAT owed in France if the tax was fully paid).1

Although carousel fraud has been subject to media scrutiny and described on a number of occasions,2 it is not the only type of VAT fraud. Much VAT fraud is carried out by companies acting alone and autonomously. It is based on forgery and is combined with other offences such as misuse of company assets, breach of trust and bankruptcy.

Case study no. 25: Suspicion of forgery and use of forgeries, VAT fraud, misuse of company assets and bankruptcy

“Ms Y” was the sole shareholder and manager of four companies operating beauty and tanning salons in eastern France.

“Ms Y” regularly filed CA3 VAT returns for her companies. She applied for and obtained VAT repayments which were justified by purchase invoices for fixed assets. However, “Ms Y” failed to file corporation tax returns.

The invoices justifying the VAT repayments showed that the companies invested in specialist equipment such as jacuzzi bathtubs and UV cabins. These purchases of fixed assets generated a substantial amount of deductible VAT which was more than the collected VAT to be paid over to the government. As a result, over a two-year period, “Ms Y’s” four companies received almost €300,000 from the French Treasury.

The amounts corresponding to such investments had not been debited from the companies’ bank accounts. There were no payments to suppliers, even several months after the date of the invoices and the alleged delivery of the equipment. Moreover, there was no loan release or loan instalment payment that could have been used to fund these purchases.

Tracfin’s investigations revealed that the invoices used to justify the VAT repayments were false. They were not issued by suppliers, but entirely drawn up by ‘Ms Y’ herself on the basis of real invoices from the suppliers in question.

“Ms Y” also used false invoices to embezzle funds for her benefit using partners’ current accounts.

• A partner’s current account with one of the companies had a credit balance of €140,000. The fictitious purchases of equipment were booked by this company as having been paid for by “Ms Y”. In this way, “Ms Y” artificially created a receivable for her benefit with the company.

• In the other three companies, the partners’ current accounts had total debit balances of €60,000. One of the companies was subject to court-ordered reorganisation.

Case study no. 26: Breach of trust by an employee; misappropriation of VAT to be paid

“Mr Z” was the CFO of a company that recorded annual turnover of around €10 million. He resigned at the end of 2016.

As part of his duties, he kept the company’s accounts and had signing authority for the bank accounts. During the last two years when “Mr Z” worked for the company, regular cash withdrawals totalling €670,000 were made from its bank accounts.

“Mr Z” justified these withdrawals by the need to settle the running expenses relating to the company’s business activity. The number of withdrawals fell off significantly once he had left the company.

Two thirds of the withdrawals made by “Mr Z” were falsely booked in the company’s accounts.

“Mr Z” artificially created deductible VAT which he deducted from collected VAT thereby allowing the company to pay over less VAT at the month end. The deductible VAT accounts represented a fictitious debt that “Mr Z” paid back through cash withdrawals. In this manner, “Mr Z” had his embezzlement funded by the tax authorities as the company did not pay over the entire amount of VAT that was actually owed.

2 See Tracfin’s Annual Report 2016: Case study no. 7, p. 45.
INDIVIDUALS: ABUSE OF RIGHTS REGARDING THE TAXATION OF INVESTMENT INCOME AND DEATH DUTIES

Abuse of rights to avoid taxation of capital gains, investment income or death duties is a major part of tax evasion by individuals.

The tax authorities are entitled to disregard, as unenforceable against them, transactions that constitute an abuse of rights, 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.

Case study no. 27: Investment income (RCM): transformation of taxable dividends into exempt capital gains

"Mr P" held shares in “Company A”. In 2016, as he wished to retire, he sold his shares to “Company Z” for €500,000. However, the shares were paid for from the cash assets of the purchased company. “Company A” issued a cheque for €500,000 which was cashed by “Company Z” which, two weeks later, made out a cheque for the same amount to “Mr P”. This procedure violates the provisions of Article L.225-216 of the French Commercial Code which provides that a company may not advance funds or grant security for the subscription for or acquisition of its own shares by a third party.

“Mr P” then sought to make use of the allowance offered for the sale of shares upon retirement. In respect of this income for 2016, “Mr P” filed return no. 2074-DIR relating to capital gains or losses from the sale of shares by managers of European SMEs with a view to their retirement.

He declared that he had sold 5,000 shares in “Company A” for €100 each, giving a total sale amount of €500,000. As the acquisition price for the shares was €50,000, the capital gains represented €450,000.

As part of this sale of shares, the allowance provided for in Article 151 A septies of the French General Tax Code on the retirement of managers of SMEs was applied. As this allowance may be for a maximum of €500,000, it was applied to the amount of €450,000 in this case.

Tax implications:

In the case at hand, the valuation and sale price of “Company A” were established by factoring in the amount of liquid assets in this company’s balance sheet.

On the day the shares were sold, the two companies signed a cash management agreement authorising “Company Z” to take over “Company A’s” cash assets and to use these funds to finance the acquisition of the latter’s shares.

By leaving the funds available within “Company A” so that they could be transferred to the buyer in order to finance the shares being sold, “Mr P” altered the tax category of the amounts he received. The liquid assets held by the company, which were initially taxable as dividends in the event of distribution, became taxable as capital gains generated by the sale.

In the case under review, these capital gains were subject to the full allowance as part of “Mr P’s” retirement. As a result, these liquid assets held by the company were not taxed at all whereas they should have been the subject of a taxable distribution at the progressive rate prior to the sale. This transaction for the sale of the shares of a company which had a majority of liquid assets may be challenged under the abuse of rights provisions set forth in Article L.64 of the French Book of Tax Procedures.
Case study no. 27: Investment income (RCM): transformation of taxable dividends into exempt capital gains

Mr P holds shares acquired for €50,000

1. Mr P sells his shares in A

2. Company A

3. €500,000

4. Capital gains = €450,000

To be reconverted into taxable dividends owing to the cash management agreement between A and Z and the financing of the acquisition of A’s shares by Z using the former’s cash assets.

Declared as capital gains on a sale with an allowance of up to €500,000

Case study no. 28: Inheritance anomaly between a non-resident and a French tax resident

In this case, there was an 80 year old father, his 55 year old daughter and his 30 year old grandson.

The father lived abroad where he owned and managed a company that manufactured electronic components. He died in 2016.

The daughter and grandson were French tax residents. They lived in a property, valued at €550,000, which was owned by a property holding company (SCI) managed by the daughter and in which the father owned 50% of the shares.

Neither the daughter nor the grandson filed tax returns. They did however pay property tax and residence tax.

The French bank accounts of the three family members were credited with numerous transfers from abroad.

- Over a three-year period, the father received €800,000 from accounts held in his name in two offshore financial centres in Central America and the Caribbean.
- The daughter received at least €190,000 from an account held in her name in European country X which is renowned for its wealth management services industry.
- The grandson received at least €70,000 from country X and country Y, another European country.

Tax issues:

- Failure to file income tax returns by the daughter and grandson:
- They were in default as regards income tax. An examination of their French bank accounts failed to reveal the sources of their income, other than the transfers received from abroad.
- Failure to declare foreign bank accounts:

The bank accounts held in Europe by the daughter and grandson may have been credited with funds from the father’s foreign accounts. The grandson stated that he was the beneficiary of a life insurance policy in country X and that he managed a company based in country Y.

The daughter and grandson were in default as regards income tax as they failed to check box 8UU or file return no. 3916. Under the provisions of Article 1649 A of the French General Tax Code (CGI), any foreign accounts, whether opened, in use or closed, must be declared at the time of filing income tax returns. Failure to file this return results in the application of a tax fine as well as the taxation of the undeclared amounts.

The right of adjustment provided for in Article L.169(4) of the French Book of Tax Procedures is extended to 10 years under the provisions of Article 1649A of the French General Tax Code if the account’s balance on 31 December of the year for which
the return should have been filed is more than €50,000.

- Failure to declare an inheritance:
The father died at the end of 2016. A search of the tax bases failed to turn up a declaration of estate following his death.

He died abroad where he had lived for many years. Pursuant to the provisions of Article 750 ter of the French General Tax Code, if the deceased is resident outside France and if the beneficiary is a French resident on the date of death and has been for at least six years out of the last ten, all the movable and immovable assets located outside France, which are received by the beneficiary, are taxable in France unless there are special provisions in tax conventions. In the case at hand, there was no tax convention between France and the father’s country of residence. As a result, French law applied. Consequently, all the movable and immovable assets belonging to the deceased and inherited by the beneficiaries, who were French residents, were taxable in France.

The father owned 50% of the property holding company that owned the property in France, which was acquired for €550,000. A search of the Infogreffe database revealed that no instrument had been concluded since the father’s death. No information concerning ownership of these shares was available.

Moreover, the father had set up a company manufacturing electronic components abroad. Following his death, the company’s articles of association were amended on 10 December 2015. The daughter and grandson were appointed as managers. The grandson became the beneficial owner of the electronic components company.

Lastly, for a number of years, the daughter had held signing authority for her father’s bank accounts in France. These accounts were credited with funds from the American and Caribbean accounts. The daughter used them for her own expenses after her father’s death without filing any tax returns.
AVOIDANCE OF TRANSFER DUTY

A Lombard Loan may be misappropriated in order to launder the proceeds of tax evasion when the borrower takes out a loan, pledges it on undeclared assets abroad, and then defaults. He/she is then able to use the amount of the drawn-down loan whilst assigning his/her foreign assets to the lender institution. This boils down to transforming undeclared foreign assets into an amount that may be used in the country of tax residence.¹

This technique may be adapted for the acquisition of luxury property so as to avoid payment of transfer duty.

Case study no. 29: Arrangement by selling company shares to avoid notarised instruments and transfer duty during a property acquisition

An individual owned a property holding company (SCI) which held exceptional development land in the Greater Paris Region as well as the related building permit. The total estimated value was €5 million.

In March 2016, the individual sold the SCI’s shares to “Company X” which was registered in a European country reputed for its banking sector. The direct and indirect shareholders of “Company X” were members of “Family Z” which owned an industrial company in France.

1 See Tracfin’s “2016 risk trends and analysis” report: Case study no. 30.
In May 2016, “Company X” took out a loan for €3 million with a pool of two lender companies:

- Company no. 1 which belonged to members of “Family Z”
- and Company no. 2 which belonged to the family’s notary

“Company X” contributed the shares in the SCI to guarantee this loan. The loan and guarantee agreement between “Company X” and the pool of Companies nos. 1 and 2 under-estimated the value of the land by setting it at €3 million instead of €5 million. The loan had not begun to be repaid two years after the transaction. No repayment, even partial, was noted on the interested parties’ bank accounts. From the outset, the shares contributed as the guarantee were destined to belong to the lenders (indirectly “Family Z” and its notary).

No transfer duty was paid on the development land as the change of beneficial owner took place by the sale of the shares of the owner SCI. The conditions in which this sale was carried out and, in particular the release of the €3 million loan granted (for which it can be suspected that no repayment was ever considered) raise doubts as to the ultimate purpose of such arrangements.

Its purpose could have been to enable the pool of lenders (“Family Z” and its notary) to acquire the development land for €3 million without any notarised sale deed being required and without paying transfer duty.

Furthermore, the circumstances in which the beneficial owners of this property changed were such that no capital gains were noted or taxed as the land still belonged to the initial SCI.

The status of notary forbids notaries from direct or indirect involvement in commercial companies, from speculating on the purchase or sale of property, assignments of claims, inheritance duties, company shares and other intangible assets, and from taking any interest in cases in which they work. The notary, who is a personal beneficiary in this case, may also have advised other clients in respect of similar arrangements.

**PERSISTENT SOCIAL SECURITY FRAUD**

Tracfin’s workload in detecting fraud against social security organisations is increasing. This has less to do with a global increase in fraud than with improved cooperation between Tracfin, the reporting entities and the relevant organisations. This cooperation was bolstered at the end of 2015, when Tracfin recruited a liaison officer to handle relations with the Central Agency for Social Security Bodies (ACOSS). This officer is himself an URSSAF collection inspector.

In 2017, Tracfin sent 223 files to social welfare agencies, a 35% increase over the previous year. Already, in 2016, the increase had been 51%. Therefore, since 2015, the number of “social security” notes sent has doubled.

The types of illegal activities are broken down between contribution fraud (undeclared work; under declarations by self-employed workers to the RSI social security scheme or the MSA social agricultural mutual fund) and benefit fraud (receipt of unemployment benefit at the same time as carrying on undeclared work; residence fraud; “collection account” schemes for undue benefits).
Case study no. 30: Organised residence fraud

Tracfin’s attention was drawn to a group of 64 people, with no known or apparent family or business ties. They all lived at the same five addresses in a major French city. Over a two-year period, they received a total of almost €300,000 in social security benefits paid by the Family Allowances Fund (CAF).

The amounts received were systematically debited from bank accounts using a number of means:

- Transfers to payment accounts registered with a payment institution based in France. These payment accounts had been opened by thirty or so other members who were themselves also recipients of family allowances.
- Transfers to bank accounts in an Eastern European country followed by cash withdrawals in this country.

Overall, from identified flows, almost €130,000 were withdrawn in cash, €90,000 of which in the European country in question.

The majority of the perpetrators were either entirely unknown to the tax authorities or had filed totally blank tax returns.

Owing to the fast expansion of private hire vehicle (VTC) companies, the transport sector witnessed the largest increase in STRs received in 2017 concerning suspected social security fraud. This sector is highly vulnerable and this factor was flagged up in the “2016 risk trends and analysis” report (case study no. 34 pp 50-51) and in Tracfin’s Annual Report 2017 (case study no. 5 p.69).

A detailed report of the follow-up to Tracfin information notes sent to social welfare agencies is drawn up twice a year under the aegis of the National Anti-Fraud Office (DNLF). Over the last six years, the total amount of taxes notified following an audit initiated by Tracfin is €128 million for ACOSS, €533,000 for the National Family Allowance Fund (CNAF) and €292,000 for Pôle Emploi, France’s public employment service agency.

HELPING FIGHT CUSTOMS FRAUD

Tracfin cooperates closely with the Directorate General of Customs and Excise (DGDDI) and this is made easier by the fact that both bodies belong to the same ministry, have common goals and exchange staff. A DGDDI liaison officer works full-time at Tracfin.

Tracfin assists the DGDDI with the majority of its priority topics: circulation of cash and violations of reporting obligations, smuggling, counterfeiting, etc.

Case study no. 31: Suspected violation of reporting obligations

Over a two month period, “Mr Z”, a pensioner with French nationality, deposited seven cash payments totalling €410,000 into his bank account. He claimed that the funds originated from the sale of a factory abroad and represented a number of cash withdrawals for a total of €1 million in local currency made a few months earlier from a bank in said country. “Mr Z” failed to provide any convincing supporting documents. Part of the funds that had been deposited in cash in France were then transferred to two life insurance policies (€250,000) and other bank accounts (€100,000).

Two years earlier, “Mr Z” had already been the subject of a Tracfin note sent to the DGDDI for suspected violation of reporting obligations in respect of over €2.4 million. A search of customs databases failed to turn up any declaration of capital transfers by the individual.

Over a three year period, “Mr Z” is therefore suspected of having transferred at least €3 million in cash between the country where his factory was based and France, without filing a prior declaration with the customs authorities.
Case study no. 32: Illegal tobacconist activity

“Mr X” was a “frontier worker” who lived in France and worked in a neighbouring country. Over a three-year period, an examination of his bank accounts showed €130,000 in undeclared income (280 cash deposits for a total of €110,000 and 50 cheques from individuals paid in for a total of €20,000). When questioned about the origin of the funds, “Mr X” explained that he bought cigarettes in the country where he worked, as they were cheaper, and resold them in France.

Irrespective of the means of transport, EU and French legislation authorise the purchase of cigarettes in another European country and their transport to France without procedures being required or duties and taxes being paid. Nevertheless, as cigarettes are heavily taxed goods, they must be solely intended for personal, and non-commercial, use.

Customs consider personal use as representing volumes of less than four cartons per person and per trip. Above this ceiling, supporting documents are required: proof and place of purchase, means of transport used, etc. On the basis of the evidence, it was concluded that there was a commercial activity sanctioned by payment of a fine and consumption duties.

Case study no. 33: Suspected trading in counterfeit goods

“Mr Y” set up a French limited liability company (SARL) whose purpose was the online “sale of designer clothing and accessories”. The SARL’s registered office was at his personal address.

In 2016, the company received €400,000 on its bank accounts from a number of e-commerce platforms. Up to November 2016, the company made payments to suppliers totalling €200,000 and cash transfers amounting to €50,000, mainly to recipients in Turkey. As from December 2016, there was a change in the way the accounts were used. The various flows were replaced by transfers to a fund transfer company which prevented identification of the end beneficiaries.

Since 2015, “Mr Y” and his company had appeared in customs databases on several occasions for buying and selling counterfeits of major clothing brands.
SUMMARY OF THE MAIN RECOMMENDATIONS
SUMMARY OF THE MAIN RECOMMENDATIONS

Recommendation no. 1
Bolster the transparency of the law governing non-profit organisations by setting up a centralised digital register, an annual financial reporting requirement and the introduction of a special statutory audit for all public financing.

Recommendation no. 2
Increase public-private sector coordination in detecting and fighting fraud facilitated by shell companies.

Recommendation no. 3
Heighten the regulation of payment and electronic money service providers and provide national supervisors with the means to effectively oversee these stakeholders.

Recommendation no. 4
Standardise the European status of money collection websites with an eye to their full compliance with AML/CFT requirements.

Recommendation no. 5
Update the National Centralised Bank Accounts Register (FICOBA) to ensure exhaustiveness and foster the introduction of centralised bank account registers in all EU Member States pursuant to Directive (EU) 2018/843.

Recommendation no. 6
Implement regulation of the crypto-assets sector, in particular in respect of AML/CFT, at international (work of the FATF), European and national levels.

Recommendation no. 7
Strengthen operational cooperation with the AMF, especially on crypto-assets and the conditions for conducting investigations on the financial markets.

Recommendation no. 8
Consolidate the adherence of non-life insurance activities to the AML/CFT system, in particular by disseminating specific typologies.

Recommendation no. 9
Adjust the definition of Politically Exposed Persons (PEPs) in French law to better factor in the concept of known risk.

Recommendation no. 10
Extend the legal and digital framework for the inventory register which certain professionals operating on the art market are required to keep.
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACOSS</td>
<td>Central Agency for Social Security Bodies</td>
</tr>
<tr>
<td>ACPR</td>
<td>Prudential Supervision and Resolution Authority</td>
</tr>
<tr>
<td>AFA</td>
<td>French Anti-Corruption Agency</td>
</tr>
<tr>
<td>AMF</td>
<td>Autorité des Marchés Financiers (Financial Market Authority)</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering and Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CEE</td>
<td>White certificates</td>
</tr>
<tr>
<td>CI</td>
<td>Credit institution</td>
</tr>
<tr>
<td>CIF</td>
<td>Financial investment adviser</td>
</tr>
<tr>
<td>CIP</td>
<td>Crowdfunding advisers</td>
</tr>
<tr>
<td>CMF</td>
<td>French Monetary and Financial Code</td>
</tr>
<tr>
<td>COSI</td>
<td>Systematic information disclosure</td>
</tr>
<tr>
<td>DGCCRF</td>
<td>Directorate General for Competition Policy, Consumer Affairs and Fraud Control</td>
</tr>
<tr>
<td>DGDDI</td>
<td>Directorate General of Customs and Excise</td>
</tr>
<tr>
<td>DGFIP</td>
<td>Public Finances Directorate General</td>
</tr>
<tr>
<td>DNRED</td>
<td>National Directorate of Customs Intelligence and Investigations</td>
</tr>
<tr>
<td>DPAE</td>
<td>Advance hiring notices</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EME</td>
<td>Electronic money institutions</td>
</tr>
<tr>
<td>EP</td>
<td>Payment institution</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force KYC Know your customer</td>
</tr>
<tr>
<td>ML/FT</td>
<td>Money Laundering and Financing of Terrorism</td>
</tr>
<tr>
<td>OCRGDF</td>
<td>Central Office for the Prevention of Serious Financial Crime</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>PNCEE</td>
<td>National Unit for White Certificates</td>
</tr>
<tr>
<td>PNF</td>
<td>French Financial Prosecutor’s Office</td>
</tr>
<tr>
<td>PSD 2</td>
<td>Second European Directive on payment services</td>
</tr>
</tbody>
</table>
**PS/EMSPs** Payment and electronic money service providers

**RCM** Investment income

**SGP** Investment management company

**STR** Suspicious Transaction Report

**TGI** Court of First Instance

**URSSAF** Union for the Collection of Social Security Contributions and Family Allowances