New payment instruments, avatars of fiduciary money: New risk factors for AML/CFT

Bruno Dalles
Director of Tracfin (Ministry for Government Action and Public Accounts)

[special issue of *Réalités Industrielles*, November 2017]

Abstract:
The accelerating digital revolution and the development of new payment instruments represent a major challenge for anti-money laundering and combating the financing of terrorism (AML/CFT). Some of these instruments are definitely risky.
In 2016, due to the terrorist threat, French lawmakers restricted the use of electronic money, especially prepaid cards. These tighter product regulations should coincide with greater accountability for new players in the payment sector, called upon to reinforce their compliance efforts.
However, the capacity of supervisory authorities to oversee these players is hampered by the European passport and the Freedom to Provide Services regime. The lack of international harmonisation in terms of AML requirements curbs the effectiveness of this scheme, while the reliability of some players operating in Europe may be in doubt.

The new non-cash means of payment encompass online payment services[1] and e-money issuance.[2] These means of payment first appeared in the US in the 1990s, then developed in Europe in the late 2000s with the rise in e-commerce and subsequent changes to European standards.[3]

These new services rely on two components: 1) The electronic servers used by payment service providers such as PayPal that offer online payment platforms and "wallets" (users have no physical contact with these servers); 2) E-money physical devices such as prepaid payment cards, flash drives, or even vouchers including a code to be given to the payment recipient.

(1) See Articles L.314-1 *et seq.* of the French Monetary and Financial Code (CMF).
(2) See Articles L.315-1 *et seq.* of the CMF.
(3) The E-Money Directive (EMD2), Directive 2009/110/EC, enacted into French law in January 2013; the Payment Services Directive (PSD2), Directive (EU) 2015/2366, currently being enacted; and the 4th Anti-Money Laundering Directive, Directive (EU) 2015/849, enacted into French law in December 2016.

Depending on their degree of anonymity and traceability, these products present risks in terms of AML/CFT.

In 2016, due to the terrorist threat, French lawmakers restricted the use of electronic money, especially prepaid cards. These tighter product regulations should coincide with greater accountability for new players in the payment sector. However, the capacity of authorities to supervise these players is hampered by the European passport, whereas the reliability of some players operating in Europe may be in doubt.

Following the 2015 terrorist attacks, French lawmakers decided to regulate the use of e-money

Anonymous prepaid cards present a definite AML/CFT risk.

The 2015 terrorist attacks in France and Belgium increased awareness about the anonymous nature of electronic money as a means of payment or a way to store funds. Prepaid cards that can be reloaded with cash, when left unregulated, are just as anonymous and untraceable as cash. The dangers they pose are made more serious by their higher portability and global mobility of financial flows.

- The investigation carried out after the Paris terrorist attacks of 13 November 2015 revealed that anonymous prepaid cards had been used by the terrorist commandos to make purchases without being identified or to pay for accommodation while remaining entirely anonymous. After these cards were identified, investigators were able to trace back payments made by their users, as well as some of their movements. These cards were also used to prepare departures for the Iraqi-Syrian war zone.

In some cases, relatives back in France used cash to purchase reload vouchers, then sent the codes by text message to the jihadi fighters they were supporting. These vouchers were then used to reload digital wallets to pay certain expenses, notably telephone calls.

- Organised crime uses prepaid cards to gather and transfer funds. Tracfin has tackled the case of a prostitution network operating in Paris and regional France; this network was trafficking several hundred young women from Central Europe. These women sent their earnings to three pimps back in their home countries, using either money service businesses (MSB) or sets of prepaid cards connected to a single e-money account. They made cash deposits to the account and used their cards for expenses, whereas the pimps used cards connected to the same accounts to make cash withdrawals in their home country. Over several years, the total amounts involved in this scheme came to €2.4m.

In 2016, French lawmakers endeavoured to curb these risks

Several pieces of legislation were passed in France in 2016 to regulate the use of e-money.

- Since 1 January 2017, all e-money payments carried out in France, either via a card or from a server, are capped at €3,000.[4]

- The use of prepaid cards was restricted under the Act of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing.[5] A decree capped the amounts usable on prepaid cards:[6] the maximum amount that can be loaded on a card is €10,000; cash reloads are capped at €1,000 per month; cash withdrawals or refunds are also capped at €1,000 per month.

In addition, e-money providers are legally required to keep records of customer information related to activating, loading and using e-money cards or other physical devices.[7]
The 4th Anti-Money Laundering Directive was enacted into French law by Order no. 2016-1635 of 1 December 2016, reducing the anonymity of e-money.
Now, anyone using a traceable means of payment (i.e. a nominative bank account in an EEA country) to load a physical payment device must show ID for reloads of more than €250 per month. Cash refunds without ID checks are capped at €100.

Anyone using a non-traceable means of payment (i.e. cash or anonymous e-money) to load a physical payment device must show ID regardless of the amount and for each reload. The sole exception is for "branded" cards usable only in France for the purchase of a limited range of goods and services; these cards can be reloaded with cash without ID checks up to €250 per month.[8]

Lastly, for online payment services, operators are not required to check ID for online payments made using an EEA bank account to another EEA bank account, for transactions of less than €250, and up to an annual cumulative cap of €2,500.[9]

---

(4) Decree no. 2016-1985 of 30 December 2016, amending Article D.112-3 of the French Monetary and Financial Code (CMF).
(5) Act no. 2016-731 of 3 June 2016, known as the "Urvoas Act", and notably its provisions amending Article L.315-9 of the CMF.
(6) Decree no. 2016-1742 of 15 December 2016, enacted in Article D.315-2 of the CMF.
(7) Article L.561-12 of the CMF. As of the end of June 2017, this provision was not yet clarified by a decree.
(8) Article R.561-16 of the CMF.
(9) Article R.561-16-1 of the CMF. Articles R.561-16 and R.561-16-1 of the CMF may be amended soon to lower the €250 cap.

For payment services, product regulations must coincide with greater accountability for providers

Since the beginning of the 2000s, France has been working for around a decade to foster a strong compliance culture in its banking institutions. Now, the new payment service providers must be targeted with similar efforts. These payment service providers (PSPs), officially recognised in PSD2, do not have the same money laundering risk culture as banking institutions do, and in some cases, they even use the lifting of regulatory constraints as leverage for their development.

However, like all professionals subject to the AML/CFT scheme, payment institutions (PIs) and electronic money institutions (EMIs) must comply with customer due diligence requirements.[10] The French Prudential Supervisory and Resolution Authority (ACPR) has already sanctioned certain institutions for failing to comply with their customer identification obligations.[11]

These obligations are important for four reasons:

- The payment service providers (PSPs) act as an intermediary between a customer and his/her bank. The customer registers his/her bank account details or bank card information with a PSP, which in turn manages payments to third parties. The PSP thus divests the bank of a portion of the data required to carry out an in-depth analysis of the customer's transactions. From the bank's standpoint, the PSP is the sole counterparty for financial flows involving the customer's account. This is why it is important that the PSP can perform its own customer checks.

- When a customer uses several PSPs successively, the PSPs become interdependent: each one forms a link in a chain. One electronic payment platform may comply with its AML/CFT obligations, but allow its customers to load their wallets from other less vigilant institutions. One faulty institution is enough to weaken the entire scheme.

- PSPs that use networks of agents (for payment services) or distributors (for e-money) must check the compliance of these operators that are not finance professionals and therefore have no money laundering risk culture. Competition among PSPs could encourage them, in their dealings with agents and distributors, to prioritise their commercial development over compliance with AML/CFT obligations. As a result, multibrand agents and distributors are high risk.

- Lastly, professionals must be made aware of all kinds of risks. Documentary and identity fraud can seriously weaken KYC (know your customer) procedures even when PSPs are vigilant.

---

(10) Identify and check the identity of their client (Article L.561-5 of the CMF); classify the business relationship (Article L.561-5-1 of the CMF); throughout the client relationship, make sure that the client's transactions are consistent with his/her profile (Article L.561-6 of the CMF).

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

Supervision of payment service providers is hampered by the European passport, whereas the reliability of some of these providers may be in doubt

The primary source of leverage to encourage new payment service providers to fulfil their AML/CFT responsibilities is an effective supervisory and sanctioning scheme. However, the functioning of this scheme is altered by the European passport.

By establishing the Freedom to Provide Services (FPS) regime, the European passport divests national supervisors of a portion of their ability to act.

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

  a) either through freedom of establishment, using a permanent establishment (e.g. a branch or an agency) in the host country as a base, and/or by resorting to agents or distributors;

  b) or through freedom to provide services, without being established in the host country, by offering online services.

- Under freedom of establishment, financial institutions are subject to national regulations for AML/CFT and customer protection. In France, financial institutions that use e-money agents or distributors must name a permanent correspondent, whose role is to be in contact with Tracfin and the ACPR.[12]

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

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

Therefore, the free provision of services constitutes a major risk. At the end of 2016, there were 594 payment or e-money institutions operating in France. Of these, 54 were authorised by the ACPR, 48 were operating under freedom of establishment, and 492 were operating under the FPS regime.[13] It is becoming indispensable for the various EEA supervisory authorities to harmonise their level of requirements.

(12) Article L.561-3(VI) of the CMF.
(13) ACPR data as of 1 January 2017.

- Brexit is a major challenge for the future of the EU AML/CFT system. Most of the institutions authorised in the UK and operating in Europe under the FPS regime will most likely be forced to seek a new authorisation from another EU Member State.

The reliability of some payment service providers operating in Europe may be in doubt

- Tracfin has observed that some institutions operating in the EU, totalling millions of users, may be controlled by criminal organisations. Often, these institutions are authorised in the UK after failing to receive authorisations in other EU Member States. For instance, one institution is connected with a company known for having participated in transactions that defrauded banks in its home country. The effective beneficiaries of other institutions may be individuals subject to EU financial sanctions and/or known for criminal activities.

Tracfin has investigated a fraudulent network that operates using forex or binary option trading websites. Individual investors sent their payments to a bank account opened in France by a payment institution (PI) authorised in another EU Member State. In turn, this PI transferred the funds to a foreign account opened by an e-money institution (EMI) authorised in a third EU Member State. The PI was actually the sole customer of the EMI, which was controlled by the fraudsters. The funds were ultimately transferred to offshore accounts held by the website managers. The combination of a PI and an EMI led to overlapping financial flows aimed at opaqueness.

- Other EMIs located outside the EU cite guaranteed anonymity as a key sales argument. The past two years have seen the development of debit cards that allow users to convert bitcoin portfolios into real currency. These “bitcoin debit cards” function on the VISA network. The amounts of reloads for such cards can be sizeable – or even unlimited, when the cardholder's identity is verified. However, ID verification procedures are not always stringent enough.

At the end of the chain, criminals use these cards to convert the profits of illegal activities (trafficking of drugs, weapons or bank data sold on the dark web) from bitcoins into actual cash. Traffickers amass the bitcoins earned on illegal activities in a special portfolio, which is connected to a real currency debit card.

Currently, around 20 companies market bitcoin debit cards. These companies are registered in countries across the globe. Several of these companies rely on a single EMI, registered in an EU Overseas Country or Territory.

The accelerating digital revolution and the development of electronic money represent a major challenge for anti-money laundering and combating the financing of terrorism.
Banks lose access to certain data that is useful for their analysis of customer transactions, whereas the compliance culture of new payment service providers has yet to be developed. A lack of international standardisation hampers the effectiveness of the AML/CFT scheme. Only continued international talks involving supervisory authorities, combined with strengthened cooperation among national financial intelligence units, will bolster the progress made possible by the measures implemented in France in 2016.