CHAPTER 3

The security of means of payment

Updated on 17 December 2018

This chapter addresses the security challenges posed by means of payment and the mechanisms put in place to defeat fraud in all its increasingly sophisticated forms. The development of electronic means of payment is closely linked to advances in IT and communication technology. Since technological innovations also enable fraudsters to use more sophisticated techniques, the systems security mechanisms associated with means of payment must be upgraded regularly.

Security: a strategic challenge for the payment sector

Fraud hampers the general development of commercial ventures by damaging a company's image and trustworthiness in the eyes of users, and through entities' fear of their business being undermined by an organised attack and large-scale breach of payment data. In view of this, security is an absolute precondition for users' confidence in means of payment.

From the user's point of view, the added value of a means of payment boils down to three factors: ease of use, low or no cost, and security. When it comes to security, users tend to identify two key risks: the misappropriation of funds during the payment process, likely to result in immediate fraud, and theft of their bank details, which could lead to subsequent fraud.

This being the case, there can be disparities between the actual security of a means of payment and a user's perception of it. In practice, a user is more likely to consider a means of payment secure if they haven't lost money through it than because it is fraud-proof.

So, in order for consumers to adopt a means of payment, a delicate balance must be struck between, on the one hand, its cost and user friendliness, and on the other, the investments that payment service providers[1] must make to ensure that it is secure. Users will shun a means of payment deemed to have too many security holes, but will also steer clear if its security mechanisms make it too complex or costly to use. This leaves limited room for manoeuvre in the development of advanced security technologies.

A payment service provider seeking to market a new means of payment must therefore find the middle ground to accommodate these two requirements. The resulting business model must also factor in the cost of fraud, since, in the event of an attack, the payment service provider is likely to sustain a direct financial loss. In some cases, it can turn out to be more profitable for a payment service provider, and more acceptable to users, to assume a certain risk of fraud and provide for its management than to go to extreme lengths to virtually eradicate the risk, if this complicates the "customer journey" so much that the payment is likely to fail.

This chapter begins by clarifying the concept of payment fraud and presenting the types of fraud identified and the associated techniques used by fraudsters. It goes on to set out the measures put in place across the European Union to enforce the rights of those who use means of payment and ensure the security of payment transactions. Lastly, it concludes with a description of the French framework for the prevention of payment fraud.

1. Payment fraud

1.1. Definition of payment fraud

In France, many criminal offences (scams, misuse of company assets, money laundering, concealment, etc.) can be linked to the use of a means of payment, without the security mechanisms put in place by the payment service providers necessarily being at fault. These types of fraud are not qualified as "payment fraud" in this chapter. Here, we have adopted a narrower definition of payment fraud, restricted to the unlawful use of a means of payment or

1 Payment service providers (PSPs) are institutions authorised to open and maintain payment accounts for their clients and to issue means of payment. Within the meaning of French and European regulations, they include entities with the following statuses:

- credit institutions and their equivalents (as referred to in Article L. 518-1 of the French Monetary and Financial Code), electronic money institutions, payment institutions and account information service providers subject to French law;
- credit institutions, electronic money institutions, payment institutions and account information service providers subject to foreign law and authorised to practice on French soil.

related data, and any act that contributes to the preparation or performance of such unlawful use:

- **resulting in a financial loss**: for the account-holding institution and/or issuer of the means of payment, the holder of the means of payment, the legitimate beneficiary of the funds (the acceptor and/or creditor), an insurer, a trusted third party or any party involved in the design, production, transport or distribution chain of physical or logical data that could incur civil, commercial or criminal liability;

- **by whatever means, i.e. regardless of**:

  – the means used to obtain, without reasonable cause, the data or physical means of payment (theft, taking possession of the means of payment or data, hacking of acceptance devices, etc.);

  – how the means of payment or associated data was used (for remote or proximity payments or withdrawals, physical use of the payment instrument or related data, etc.);

  – the geographical region of issuance or use of the means of payment or related data.

- **and irrespective of the fraudster's identity**: third party, the account-holding institution and/or issuer of the means of payment, the lawful holder of the means of payment, the legitimate beneficiary of the funds, a trusted third party, etc.

1.2. Types of fraud

Identifying fraud techniques is by nature an ongoing quest: as security systems develop, fraudsters are constantly on the lookout for new flaws to exploit. And when anti-fraud measures are ramped up in one sector of the payment market, fraudsters can simply turn their attention to other less secure sectors or regions. For example, the introduction of EMV[2] specifications for chip cards in Europe significantly improved the security of proximity payments, but also led fraudsters to target regions that had not adopted the EMV standard and focus their attacks in the euro area on card payments made remotely.

There are four broad types of fraud involving the various payment instruments:

- **counterfeiting**: fraud by issuing a false payment order using a lost, stolen or counterfeit payment instrument or misappropriated bank data or identifiers;

- **forgery**: fraud by using a forged payment instrument (an authentic payment instrument whose physical properties or associated data have been altered by the fraudster) or making changes to a regular payment order by modifying one or more details (amount, currency, beneficiary name, beneficiary account details, etc.);

- **misappropriation**: fraud in which the intention is to use the payment instrument or payment order as it stands, without changing any details (for example, cashing a non-forged cheque on an account that is not held in the name of the cheque's lawful beneficiary);

- **wrongful use/dispute**: fraud in which the legitimate holder of a means of payment disputes a payment order that he or she has regularly issued, acting in bad faith.

This typology, used together with nationwide statistics collected by the Banque de France, provides a common basis for fraud analysis by payment service providers. Depending on the purpose of the analysis, the typology can be used in conjunction with an analysis of:

- the **means of payment** targeted: payment card, transfer, direct debit, cheque or other instrument;

2 EMV (for Europay, Mastercard, VISA) is an international security standard for chip cards, for which the specifications were developed by the EMVCo consortium, comprising American Express, JCB Cards, Mastercard and Visa. The EMV standard for proximity payments and withdrawals provides for the use of a chip attached to the card, coupled with the entering of a confidential code, a system commonly known as "chip & PIN".

- the **payment channel** used: proximity payment at the point of sale using a payment terminal or ATM, remote payment by Internet, mail, telephone or other means;
- the **loss sustained and its distribution** between the beneficiary's bank, payer's bank, merchant, holder of the means of payment, insurers where appropriate, and any other party involved;

Box 1: Types of fraud affecting common payment instruments

The four types of fraud take different forms depending on the payment instrument affected. The table below presents the most commonly observed fraud techniques.

T1: The main four types of fraud affecting common payment instruments

Type of fraud	Payment card	Cheque	Credit transfer	Direct debit
Counterfeiting	• The fraudster uses a lost or stolen card or an illegally obtained card number (for remote purchases) • A counterfeit card is created by the fraudster using data they have appropriated	• The fraudster uses a lost or stolen cheque • The fraudster creates from scratch a counterfeit cheque, "issued" by an actual or fake bank	• The fraudster places a fake transfer order • The fraudster takes possession of a person's online bank login details to initiate fraudulent transfers	• The fraudster issues a direct debit order without a mandate or using a false mandate
Forgery	• The fraudster alters the magnetic strip data, embossed data[a] or programming of a genuine card	• The fraudster intercepts a legitimate cheque and alters it by scratching, rubbing out or erasing the data	• A legitimate transfer is intercepted and altered by fraudster	• The fraudster replaces a legitimate creditor's account details with their own in a direct debit order or file
Misappropriation	• Payment or withdrawal under duress	• The lawful holder of a legitimate cheque signs it under duress or manipulation	• A legitimate account holder is forced or tricked into initiating a transfer to an account not held in the name of the legitimate beneficiary or lacking any underlying economic reality	• The fraudster steals a third party's identity and IBAN number to sign a direct debit mandate on an account that does not belong to him/her
Wrongful use/ dispute	• The fraudster, acting in bad faith, disputes a valid card payment they have made	• The legitimate holder of a chequebook deliberately writes a cheque that he or she previously reported lost or stolen	• An account holder, acting in bad faith, wrongfully disputes a valid transfer that he or she initiated	• A debtor, acting in bad faith, wrongfully disputes a valid direct debit order issued by the creditor (commercial dispute)

a) Modification of the raised card numbers embossed on the card.

- the **business sector** of the merchant that fell victim to fraud affecting remote payments: food & drink, online gaming, personal services, technical & cultural products, telephony & communications, etc.;
- the **geographical areas** of issuance or use of the means of payment or related data, depending on whether the banks of the payer and beneficiary are located in the same country or currency area.

Box 2: Payment fraud in France

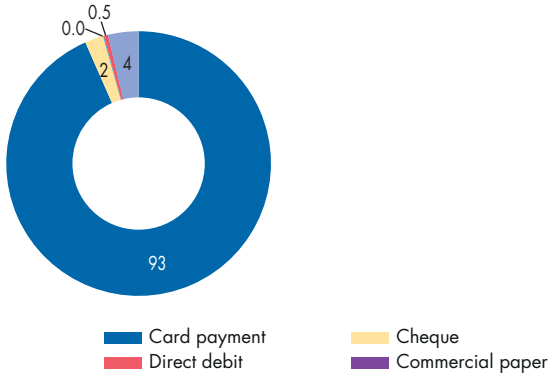
The data compiled by the OSMP *Observatoire de la sécurité des moyens de paiement* – Observatory for the Security of Payment Means) for 2016 shows the overall amount of fraud affecting cashless means of payment issued in France to be roughly EUR 800 million, for slightly over EUR 27,000 billion in total payments processed. The breakdown by means of payment shows the following profile:

- Card payments, given their prevalence (used in almost half of all cashless transactions), account for roughly 50% of fraud involving cashless means of payment (around EUR 360 million in 2017), with a fraud rate of 0.054%, i.e. one euro of fraud for every EUR 1,850 in transactions. This type of fraud has two main characteristics: firstly, it targets primarily remote payments, especially online payments, which account for two thirds of fraud in terms of amount but only 12% based on the number of transactions, and secondly, it affects cross-border transactions more than domestic transactions, with the former making up more than 60% of the fraud amount even though they account for just 13% of transactions conducted.
- Cheques are the second means of payment most affected by fraud, accounting for one third of the overall fraud amount (i.e. a fraud rate of 0.029%, representing one euro of fraud for every EUR 3,500 in payments made).
- Credit transfers show a lower fraud amount of around EUR 78 million and, proportionally speaking, are far less affected than cards and cheques, with a fraud rate that is more than sixty times lower.
- Lastly, direct debit and commercial paper fraud show the lowest fraud amounts, at around EUR 9 million and EUR 0.15 million respectively in 2017.

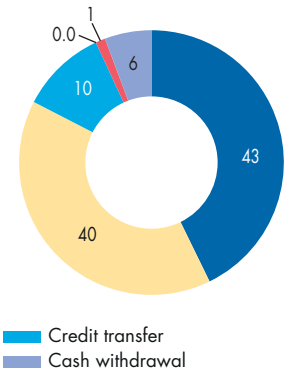
C1: Breakdown of fraud by cashless means of payment in 2017

(%)

a) Based on volume



b) Based on amount

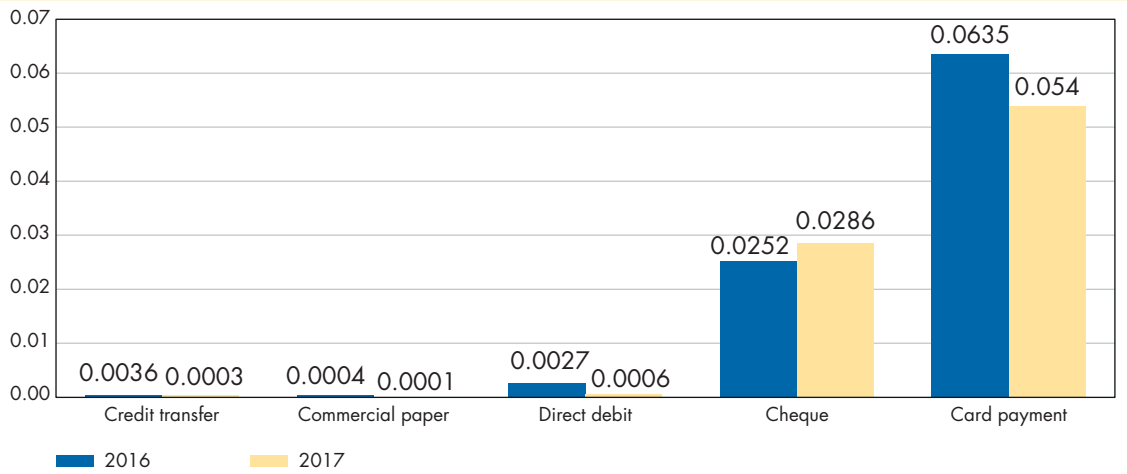


Source: *Observatoire de la sécurité des moyens de paiement.*

.../...

C2: Fraud rate broken down by cashless means of payment, 2016–2017

(%)



Source: *Observatoire de la sécurité des moyens de paiement.*

1.3. Fraud techniques

When analysing fraud, it is crucial to identify the technique used by the fraudsters. Alongside the development of electronic means of payment, fraudsters have increasingly targeted the data related to a means of payment or specific payment service. One difficulty this presents is that the data is transmitted along the entire length of the payment chain, so effective protection mechanisms must be provided throughout the chain, particularly at any sensitive points identified.

IT systems: the IT equipment (computers, smartphones, etc.) of consumers or merchants, and the databases of payment service providers and payment integrators for card-related payments, can be subject to attacks aiming to capture insufficiently secure data. The databases compiled at various stages in the payment process, containing data relating to a large number of transactions, have become magnets for fraudsters due to the sheer volume of data they contain that could be put to fraudulent use.

In order for fraudsters to launch this type of attack, they must first install malware without the user's knowledge, typically through seemingly trusted sources. This fraud technique targets the servers of large companies, as well as individual users' PCs and, increasingly, mobile phones, which are becoming more widely used in payment transactions. One of the most popular types of malware, "keylogger", records the victim's keystrokes.

Internet: a fraudster can incite users to disclose personal data such as payment card details (card number, expiry date, security code on the back of the card) or authentication data (e.g. the mobile number to which codes are sent to confirm payment transactions). This technique, known as "phishing", is typically implemented by sending the victims emails bearing usurped logos and visual branding that is familiar to them (e.g. a credit institution's logo) asking them to log onto a (fraudulent) website, with the aim of obtaining sensitive data. Another variant of this technique, "vishing", targets mobiles, with fraudsters sending messages – SMS, MMS, notifications from the mobile network – with fraudulent intent.

Another technique known as "pharming" entails tampering with servers so that users of a website are unknowingly redirected to a fake website resembling the legitimate

site, which is then used to embezzle funds or obtain sensitive data.

Email, fax and telephone conversations: targeting transactions initiated by mail, fax or phone involving an element of manual processing, fraudsters record bank details during the payment or booking process in order to reuse them at a later date.

Acceptance systems and networks: with card payments, the acceptance devices (ATMs and payment terminals) and the networks that channel data between them and their acquisition servers can be targeted by attacks to misappropriate data.

The most frequently used technique, "skimming", involves obtaining the data encoded on a card's magnetic strip without the holder's knowledge.[3] An ATM's entire front panel or card insertion slot can be faked to disguise an unlawful device. The device can also be linked to a video camera or fake keypad to obtain the user's PIN and can contain systems to store or send compromised data.

Another technique involves retaining payment cards in an ATM for their subsequent use. Fraudsters insert a device in the ATM, observe the PIN being entered on the keypad, then take possession of the card once the user has departed. This technique is similar to the physical theft of payment cards.

Fraudsters can also exploit security holes in ATM or payment terminal software. They attempt to introduce malicious code in the systems so as to modify their behaviour or even take control of their components (keypad, screen and printer).

Lastly, attacks can target the networks themselves, when data is transferred between acceptance devices, payment integrators, when used, and acquisition servers.

Physical payment instruments: The physical theft of a means of payment, when the fraudster intends to use it in place of its legitimate holder, is the predominant kind of attack. With payment cards, fraudsters try to obtain the PIN so that they can maximise their fraudulent use of the card in ATMs, payment terminals, online and through all other payment channels.

2. Combating payment fraud

2.1. Performance of oversight missions by the Banque de France

Given the wealth of payment services – and fraud techniques – in use, coordination is required between institutions and private sector players to ensure that payment services function properly.

In France, the oversight of cashless means of payment was entrusted to the Banque de France by the French law of 2001 on everyday security. It is codified in Article L. 141-4 et seq. of the French Monetary and Financial Code. The Banque de France is responsible for overseeing all cashless means of payment, together with specific electronic payment vouchers. The scope of its oversight mission is therefore extensive, given that Article L. 311-3 of the Monetary and Financial Code stipulates "any instrument which enables any person to transfer funds shall be deemed to be a means of payment, regardless of the medium or the technical process used".

To exercise its oversight, the Banque de France relies in particular on the Observatory for the Security of Payment Means (OSMP), whose mandate is threefold:

- it monitors the implementation of measures adopted by issuers, merchants and companies to reinforce the security of means of payment;
- it compiles statistics on fraud;
- it maintains a technology watch, with the aim of proposing ways to prevent security breaches involving cashless means of payment.

3 For further details on this topic, see the OSCP's 2010 report, *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2010.pdf*

Box 3: Observatory for the Security of Payment Means, a body specific to France

The Observatory for the Security of Payment Means (OSMP) is a national body whose purpose is to promote dialogue and consultation between all parties (consumers, merchants and companies, public authorities and administrations, banks and managers of payment means) involved in the smooth functioning of cashless means of payment and the fight against fraud.

Created by the French Law 2016-1691 of 9 December 2016, known as "Loi Sapin 2", the OSMP succeeded the Observatory for Payment Card Security (OSCP) and took over all its missions within a wider scope covering all cashless means of payment (credit transfers, direct debits, payment cards, electronic money, cheques and commercial paper). The pivotal role in reinforcing card payment security that had been assumed by the OSCP since its establishment in 2002, coupled with the fact that innovative payment-related developments had reached a variety and breadth extending well beyond cards, prompted the French authorities to extend the Observatory's remit to all cashless means of payment.

Chaired by the Governor of the Banque de France, the Observatory brings together representatives from a number of spheres: the State and Parliament, the banking oversight and supervisory bodies, the *Commission nationale de l'informatique et des libertés* (CNIL – the French data protection authority), issuers of means of payment, operators of payment systems, consumer associations, business associations and merchant associations.

The Observatory, whose secretariat is provided by the Banque de France, monitors security measures implemented by issuers, merchants and companies, compiles fraud statistics and maintains a technology watch in the payment sector with the aim of proposing ways to combat technological security breaches affecting means of payment. It produces an annual activity report that is sent to the Minister for the Economy, Finance and Industry and submitted to Parliament.

1 These reports are published on the Observatory's website: *www.observatoire-paiements.fr*

The Banque de France's main objective in implementing its oversight mission is to ensure that the public remains confident when using means of payment. It does this by helping to spread good security practices among all parties concerned in a consistent manner throughout France. To this end, it performs risk analyses for each means of payment and establishes an oversight framework. By conducting document-based or on-site controls, it ensures that all the parties concerned, together with their technical service providers, comply with these standards. If the Banque de France finds that a means of payment lacks sufficient security guarantees, it can recommend that its issuer take all due measures to rectify the situation. Should the issuer fail to effectively implement these recommendations, after assembling the issuer's observations, the Banque de France may decide to draft a negative opinion for publication in the Official Journal.

As part of its supervisory role, the Banque de France can monitor all payment service providers (issuers, acquirers and managers of cashless means of payment) operating on French soil: banks, payment institutions and electronic money institutions. These institutions are authorised and supervised by the Autorité de contrôle prudentiel et de résolution (ACPR, French Prudential Supervision and Resolution Authority). Banque de France oversight can also extend to institutions that are exempt from ACPR authorisation but manage cashless means of payment that are accepted within a limited network or are used to pay for a restricted range of goods or services.

Box 4: Examples of security requirements included in the oversight framework

IT systems security

Measures to combat fraud must include, as a priority, the protection of personal data. IT systems must therefore meet security standards so as to limit the risks identified in the capture of data relating to means of payment. As a general rule, IT systems must be protected against internal and external threats. To that end, they must be subject to security reviews with a view to implementing protection mechanisms appropriate for the environment in which they operate. Systems managers must therefore develop a security policy and regularly assess the risks to which their systems are exposed. A number of methods are provided for this purpose, including Ebios (developed and maintained in France by *Agence Nationale de la Sécurité des Systèmes d'Information*, the national IT systems security agency) and the suite of ISO 27000 standards.

To ward off attacks on databases, the European directive on network and information security in the EU,[1] adopted on 6 July 2016, makes it a requirement for banks and online retailers to put in place data protection systems tailored to the risks identified and to report to the authorities any breaches of databases containing customer information, particularly if it is payment-related.

These security policies must also cover the security of data upon its input into a system. They must ensure the traceability of all access to the system for the purpose of entering or modifying data needed to conduct a transaction, so as to constitute a reliable audit trail. Data tends to be compromised at this point through misconduct by dishonest employees. Acceptance devices that limit interaction between merchants and means of payment must therefore be given preference. It is also important to restrict data access to individuals who are properly authorised and to ensure that sensitive data is not retained after it has served its purpose.

User awareness

Making users aware of security-related issues helps to combat social engineering attacks. Effective communication using all available channels (regular mail, email, websites, etc.) is therefore recommended for all parties involved in the payment chain, to ensure that users know the risk factors to look out for and the best practices to implement. Users must also be urged to use only trusted websites that meet the security standards set out in these documents.

Identification of risky transactions

The implementation of systems to analyse and exploit payers' personal data is a key area of development in terms of detecting fraudulent transactions. In recent years, this type of system has tended to collect an increasing amount and variety of data during online transactions in order to check the information for consistency and authenticate a payer's identity with more certainty. For instance, alongside the data usually gathered on a person's identity and contact details (surname, first name, postal address, delivery address, email address, phone number, etc.), fraud prevention tools have gradually added:

- the payer's consumption patterns (number and breakdown of orders, frequency and amount of purchases, age of the business relationship);
- the payer's location (e.g. the IP address of the computer used);

1 Network and Information Security (NIS) Directive.

.../...

- the devices used to access the internet;
- behaviour-related data (time taken to fill in forms, input interface such as keyboard, etc.).

While using more criteria in transaction scoring has made these assessments more reliable, it also runs the risk of invading users' privacy. Players in the payment chain have taken data collection to a new level, shifting from a "declarative" approach, whereby users provide their own details, to the automatic gathering of data without users being systematically informed. This is why, in France, prior authorisation must be obtained for this type of processing from the data protection authority (CNIL), pursuant to the European Union's General Data Protection Regulation (GDPR).

In recent years, the Banque de France has conducted a number of on-site inspections covering, in turn, (i) the main French banking groups' preparedness for migration to SEPA payment methods, (ii) the security and proper management of cheque-related operations and (iii) the compliance of online payment administrative and management processes with European Banking Authority (EBA) guidelines. Following each of these inspections, the Banque de France issued a set of recommendations to the institution concerned. Its key recommendations were to reinforce mechanisms for monitoring clients' migration to SEPA, improve the quality of statistics on fraud reported to the Banque de France and enhance the quality of internal control frameworks.

In connection with its supervision of cashless means of payment, the Banque de France also issues advisory opinions for the ACPR on the technical, IT and organisational mechanisms put in place by companies seeking authorisation to operate as payment or electronic money institutions, in order to ensure that their means of payment are secure. These opinions are included in the file submitted to the ACPR banking sub-college responsible for granting the authorisation concerned.

The Banque de France reports on its supervisory activities relating to cashless means of payment in oversight reports published every three to four years.[4]

2.2. Parties involved in the fight against fraud

Alongside the work done by central banks in relation to their oversight of means of payment, law enforcement agencies play a crucial role in dismantling payment fraud networks. In France, law enforcement agencies operate within a tiered structure, whereby the national police force and gendarmerie have set up a number of specialised units:

- at the judiciary police headquarters, the department responsible for combating organised crime and financial crime (SDLCODF) is tasked with compiling information, conducting strategic analyses and maintaining relations with the authorities for issues involving specialised crime, among other areas. For this purpose, it has a number of central offices, some of which are actively involved in combating payment fraud, such as the serious financial crime office (ORCGDF) and the ICT crime office (OCLCTIC), which oversees the central unit for the prevention of payment card counterfeiting (BCRCCP);
- within the national gendarmerie, the technical department for legal research and documentation has a financial division and a division for the prevention of cyber-crime, in charge of coordinating and making use of legal information on criminal and other offences.

4 *https://www.banque-france.fr/liste-chronologique/rapports-sur-la-surveillance-des-moyens-de-paiement-et-des-infrastructures-des-marches-financiers*

These two divisions are deeply involved in combating payment card fraud;

- in addition to these specialist departments, technical departments carry out high-level technical investigations, namely the police force's department for IT and computer forensics and the digital and forensic engineering division of the national gendarmerie's institute for crime investigation.

At the level of both the police and the gendarmerie, this structure is backed up on the ground by investigators specialising in digital technology and cyber crime.

In addition, banks and, more generally, payment service providers, law enforcement agencies, accreditation bodies, specialised technical laboratories and the banking authorities have all deemed it necessary to put in place permanent cooperation

Box 5: GIE Cartes Bancaires and the fight against payment card fraud in France

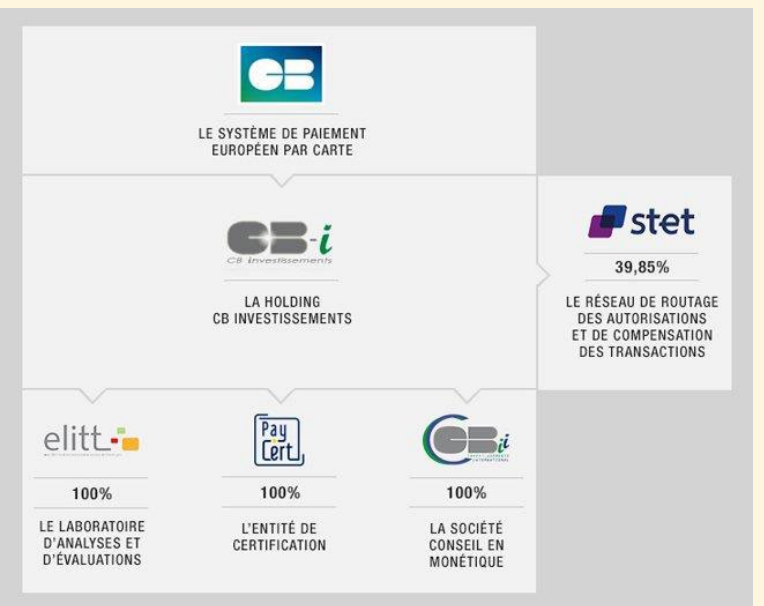
In 1984, the French banking sector put a structure in place for card payments based on the bank card economic interest group, GIE Cartes Bancaires.[1] This group assumes the governance of the "CB" (bank card) payment system, as well as providing operational input and technical expertise. Its creation helped to support the development of interbanking for payment cards in France and the group has been given a pivotal role in the operational fight against fraud.

The group's anti-fraud measures involve the following activities:

- implementing tools to identify potentially fraudulent transactions and points at which data may become compromised, using real-time analysis of transaction data on the CB system;
- regularly working closely with law enforcement agencies, providing evidence for investigations;
- analysing and assessing all CB network components (cards, terminals, networks, etc.) via a dedicated subsidiary, the Elitt laboratory;
- certifying equipment authorised in the CB network (e.g. payment terminals, mobile payment solutions, etc.) via a dedicated subsidiary, PayCert.

The Visa, MasterCard and American Express international networks also developed similar tools for the benefit of their members.

Organisational structure of GIE CB and its subsidiaries



1 GIE CB is an economic interest group consisting of around 130 institutions that provide payment services. Its missions include the governance, security and promotion of the CB system, as well as the development of products and services, and innovation in the field of payment systems in compliance with laws and regulations. As well as the CB system, the Group's objectives include development work and standardising security mechanisms specific to digital luncheon vouchers (hardware support).

structures. Lastly, depending on the matter concerned, bodies outside the banking sector, such as Europol, can be called upon to provide input.

2.3. Contribution of the global monitoring of innovations in means of payment

The Bank for International Settlement's Committee on Payments and Market Infrastructure (CPMI), which in 2014 succeeded the Committee on Payment and Settlement Systems (CPSS), has a mandate that covers retail payment systems and, by extension, means of payment. It monitors innovation in means of payment and is particularly interested in the position adopted by central banks in this field. In May 2012, it published a report on this topic.[5]

The report underscores the importance attached by central banks to promoting the use of secure and effective means of payment, while spurring innovation. It also lists the barriers to payment innovation and other general issues, such as the role of standardisation, the effect of having payment instruments that can be used differently in different countries and the role of the regulator. In terms of security, the report highlights the importance of sustaining users' confidence in payment services. Technology must be used to ensure that a payment instrument is effective. It must also make the payment process more fluid without introducing vulnerabilities in the payment chain that could be exploited by fraudsters, particularly as regards consent to execute a payment transaction.

Along these lines, the report underlines, for example, the progress afforded by EMV technology, such as the authentication of cards and payment terminals. As regards remote transactions, the following areas were singled out for attention:

- security conditions in situations where card data is retained by a merchant and/or its payment service provider;
- the use of powerful authentication mechanisms to effectively combat fraud. In this respect, the CPSS noted the effectiveness of mechanisms based on at least two authentication factors.

These considerations add weight to the regulatory decisions adopted in the European Union, as well as to the work done in France by the Observatory for the Security of Payment Means.

3. The European framework for payment security

3.1. Europe's legal framework for means of payment

The convergence of regulations applicable to the payment sector is a crucial component of Europe-wide integration in the payment sector, building on key policy initiatives such as the introduction of euro currency and the roll-out of SEPA payment schemes.

The first Payment Services Directive (PSD1)

The Payment Services Directive (PSD),[6] which was adopted on 13 November 2007 and came into force in November 2009, set out common rules for the provision of payment services in Europe. It created a harmonised regulatory framework for payment services, while increasing both consumer protection and competition in the payment sector.

Rules applicable to payment services: by laying down rules for all "payment services" – which can be likened to transactions involving the "provision or management of means of payment" (see "payment services" box) – the Payment Services Directive differs from other legislation in that it is not based on the device used to initiate or accept payment or on the underlying technology. Moreover, it does not draw distinctions based on a payment service provider's legal status. This approach ensures that payment rules are applied consistently across the technologies used as they evolve

5 *http://www.bis.org/publ/cpss102.htm*

6 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, *http://eur-lex.europa.eu/legal-content*

Box 6: Payment services as defined in PSD1

The concept of "payment service" is not explicitly defined in PSD1. The Directive does, however, provide a restrictive list of business categories considered to be payment services. These categories, of which there are seven, are as follows:

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:
- execution of direct debits, including one-off direct debits,
- execution of payment transactions through a payment card or a similar device,
- execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a payment service user:
- execution of direct debits, including one-off direct debits,
- execution of payment transactions through a payment card or a similar device,
- execution of credit transfers, including standing orders.

5. Issuing and/or acquiring of payment instruments.

6. Money remittance.

7. Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

A number of paper-based payment instruments fall outside the Directive's scope, primarily cheques, postal orders and bills of exchange, the latter being governed specifically by international agreements.

The list of services was amended when the Directive was revised. The second directive (PSD2) includes, in particular, services provided by third-party payment service providers (see below).

and across the various types of provider, while taking into account the specific characteristics of the services concerned.

Some of the Directive's provisions, such as those covering the revocation of payment orders, payment disputes and transaction execution, draw distinctions between payment services based on how they are initiated. Card payments are defined as "transactions initiated by the beneficiary". The other types of transaction are also referred to using generic terms, for example "transactions initiated by the payer" for transfers and "transactions initiated by the payee" for direct debits.

To clarify certain provisions, the Directive refers to the payment instrument used, or, to be more specific, to the presence

of "personalised security features", i.e. components used to authenticate the payer. The articles concerned mainly refer to transactions made by card, by mobile if the payment application uses personalised security features, and using online banking. Lastly, the Directive provides for "light touch" regulations for "low-value" payment instruments, particularly in terms of disclosure requirements and disputes. These regulations apply only to payment instruments subject to a contractual restriction capping transaction amounts at EUR 30.

Disputing unauthorised transactions: the Directive provides for two arrangements, depending on whether or not the payment was authorised by the payer.

The first arrangement concerns unauthorised transactions: in practice, these include cases involving the loss, theft, or misappropriation (including fraudulent remote use and counterfeiting) of payment instruments. In such cases, the payer has a period of 13 months following the date on which their account was debited to dispute the unauthorised payment. The payment service provider must then, without delay, restore the account to the state in which it would have been had the unauthorised transaction not taken place. As soon as the payer becomes aware of the theft, loss, misappropriation or any unauthorised use of his/her payment instrument, he/she must inform the payment service provider accordingly.

Under the Directive, however, this arrangement does not apply to instruments equipped with personalised security features, which is notably the case of payment cards. In these cases, the payer can be expected to bear losses of up to EUR 150 resulting from any unauthorised payment made after a payment instrument is lost or stolen or "if the payer has not kept their personalised security credentials safe, following the misappropriation of a payment instrument". Lastly, if a holder is proved to have acted fraudulently or with gross negligence before asking for their card to be blocked, the holder will not be eligible for this reimbursement arrangement.

The second arrangement for disputing a transaction under the Directive concerns transactions subject to a general authorisation by the payer, where the transaction amount is not specified at the time of authorisation. This arrangement applies to direct debits and card payments made, for example, when booking a hotel or renting a car. In these cases, the payer who authorises a payment transaction has eight weeks from the date on which their account is debited during which to request reimbursement, if the final amount debited exceeds the amount the payer could reasonably expect to pay given their past expenditure, the terms and conditions of their framework contract and other circumstances relevant to the matter. Within ten business days of receiving a reimbursement request, the payment service provider must refund the full transaction amount or provide justification for refusing to refund the payment, indicating the bodies to which the payer may refer if he or she does not accept the justification provided.

Standardisation of reporting requirements associated with the provision of payment services: the Directive specifies the information that payment service providers must provide to their clients for one-off payment transactions and transactions conducted under a "framework contract". This mainly comprises information on the payment service provider (name and contact details), use of the payment service concerned (consent format and procedure, execution time, ability to set spending limits for the instrument concerned), charges (including interest and exchange rates), reporting (frequency), safeguards and corrective measures (measures to be taken to keep an instrument safe, ability to block the instrument, liability of the payment service provider and payer, conditions for reimbursement, etc.), the amendment and termination of a contract (term of the contract, right of termination) and possible avenues of recourse.

The Directive also set out the terms and conditions for amending and terminating contracts between payment service providers and their users. This was the first time that such provisions had been included in French payment card contracts. The provisions for amending the terms of a contract were broadly in line with those generally used in French account agreements. The Directive states that a proposed amendment must be disclosed by the payment service provider no later than two months before it is scheduled to come into force. Unless the user explicitly rejects the amendment before it comes into effect, the amendment is deemed to have been accepted. If the user rejects the amendment, he or she is entitled to cancel the contract with immediate effect, free of charge, before the date on which the proposed amendment comes into effect.

As regards contract termination, the Directive imposes more substantial regulations, creating a framework that is slightly more beneficial to the users of payment services that that previously in force in France. For instance, a framework contract can be terminated at any time by the client, unless the parties have agreed on a period of notice, which can be no longer than one month. Such terminations do not incur fees if the framework contract has been signed for a fixed term of more than 12 months or if it has been concluded for an indefinite period. In all other cases, termination fees must be appropriate and in line with costs.

The second Payment Services Directive (PSD2)

The second European Payment Services Directive (PSD2), adopted on 25 November 2015,[7] follows on from PSD1 and broadens the scope of payment services covered to include new services and players, while strengthening the security requirements applicable to participants in the payment sector. It came in to force in France, as in most Member States, on 13 January 2018.

PSD2 creates a payment service provider (PSP) status for third-party providers who access accounts held by "account servicing" PSPs (mainly banks) to initiate payments or consolidate account information:

- payment initiation service providers are intermediaries able to initiate payments, usually credit transfers, from a client's online bank account. They provide this service to online retailers and their customers as an alternative to card payments or digital wallets;

- account information service providers consolidate information on the various accounts a customer may have with one or more payment service providers.

These activities were previously unregulated and carried a high risk of fraud, because users needed to disclose their online banking identifiers and access codes to a third party.

The Directive also sets out procedures to make payments safer in two key ways:

- strong account holder authentication is required to access accounts or carry out other online processes that carry high risks (such as creating a new beneficiary for transfers via a bank website);

- strong payer authentication is required to initiate electronic payments.

However, the regulations provide for exemptions to the strong authentication requirement in certain legally defined cases where transactions are deemed to be low-risk (e.g. low-value payments or transfers between accounts held by the same person).

Under this new framework, the regulation provides that bank identifiers can be shared with third-party PSPs in a secure manner, in particular by encrypting data. It also provides that third-party PSPs and account servicing PSPs, as well as users, should communicate securely using an interface, the characteristics of which are

7 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, *https://eur-lex.europa.eu/legal- content/FR/TXT/?uri=CELEX%3A32015L2366*

specified in a level 2 regulation associated with the Directive, the Regulatory Technical Standards (RTS).

The European Banking Authority (EBA) was tasked with preparing, in close collaboration with the European Central Bank (ECB), regulatory technical standards setting out: (i) the requirements for, and exemptions from, strong customer authentication for securing transactions and access to accounts; (ii) the requirements for protecting login identifiers; and (iii) the technical and operational procedures enabling banks, third-party PSPs and their clients to communicate securely. To allow time for players to adapt their IT systems and for the competent authorities to prepare to implement the associated monitoring frameworks, the Directive states that the requirements imposed by the regulatory technical standards will be applicable 18 months after they are adopted and published, i.e. from 14 September 2019.

Box 7: Strong customer authentication

The issue of making online payments safe was raised in 2008, within the Observatory for Payment Card Security at the instigation of the Banque de France. The recommendations issued by the Observatory in its 2009 annual report defined the concept of strong payer authentication and invited players in France's payment card sector to develop and implement authentication solutions in accordance with this definition.

The French example inspired the work subsequently carried out at the European level, firstly by the European SecuRe Pay forum (see below) then by the European Commission in preparation for PSD2. The new Directive defines strong authentication as a set of procedures based on the use of at least two of the following three components:

1. Something only the payer knows:
For example, a password, personal identification code (PIN), etc.;

2. Something only the payer possesses:
For example, a token, mobile phone, chip card, etc.;

3. Something the person is:
For example, a biometric element such as the payer's fingerprint or voice.

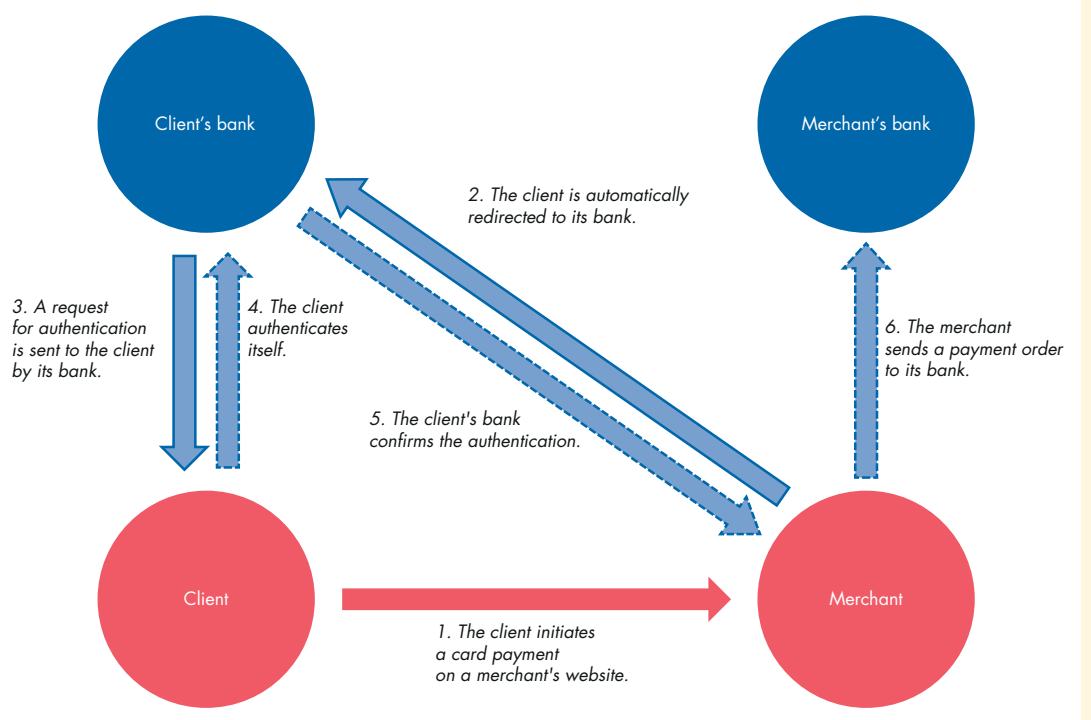
The components selected must be mutually independent, i.e. the breach of one component must not jeopardise the security of the others. In addition, at least one of the components must be non-reusable and non-replicable, i.e. it must not be able to be used in an identical way for two separate payment transactions (except for biometrics). Lastly, the strong authentication procedure must be designed to protect the confidentiality of authentication data.

Currently, the strong authentication component most frequently used for online payments is based on the use of a one-time password (OTP) given to payers using a variety of channels (SMS to a mobile phone, generated on the payer's online banking website, via a card reader or a token embedded in a key fob, etc.).[1] When a payment is made, the website puts the payer in touch with the card-issuing bank so that it can authenticate the payer using the "3D-Secure" protocol, which operates as shown in the chart hereafter.

1 The Observatory for the Security of Payment Cards 2015 annual report contains a review of the strong authentication techniques most commonly used in France: *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2015.pdf*

.../...

Functioning of the "3D Secure" protocol



Box 8: Provisions of the RTS

Following the work carried out by the European payment security forum (SecuRe Pay, see below), which actively sought interaction with the market (publication of a discussion paper, followed by a public consultation), the regulatory technical standards (RTS) for PSD2 were adopted by the European Commission on 27 November 2017, after which date the European Parliament and the Council had three months to review them. Following the review period, delegated regulation (EU) 2018/389 on the RTS was published in the European Union Official Journal on 13 March 2018,[1] marking the beginning of the 18-month period after which the RTS will come into effect, on 14 September 2019.

With respect to strong authentication, the RTS provide for a number of exemptions:
- consultation of accounts (after an initial strong authentication);
- low-value payments (up to EUR 50 for proximity payments and EUR 30 for remote payments);
- payments via transport or parking payment terminals;
- payments to trusted payees;
- recurring transactions (except for the first time such transactions are initiated);
- payments to companies using secure transfer protocols;
- transactions deemed low risk by the institution holding the payer's account.

1 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2018:069:TOC

.../...

With respect to this last case, PSPs must ensure that the fraud rates on transactions eligible for exemption remain below the thresholds set in the RTS, as a function of the means of payment and amount concerned:

Transactions involving amounts above EUR 500 are not eligible for this exemption. Moreover, if the fraud rate thresholds are breached during two consecutive quarters, the PSP concerned will no longer be authorised to grant this exemption until its fraud rates return below the threshold.

T2: Maximum fraud rate

(%)

	On remote payments by card	On transfers initiated remotely
EUR 250 to 500	0.01	0.005
EUR 100 to 250	0.06	0.010
Up to EUR 100	0.13	0.015

As regards the **security of interfaces between account servicing PSPs and third-party PSPs**, the RTS make it mandatory to set up and use a dedicated interface that facilitates: (i) identification of the third party PSP by the account servicing PSP by means of certificates, as defined in the EU eIDAS Regulation, (ii) use of the authentication procedures provided by the account servicing PSP to the payment service user, and (iii) initiation of payment orders and receipt of the associated payment execution information.

The RTS provide for a six-month trial period for the interface before the regulatory standards come into force. Account servicing PSPs can opt to develop a dedicated interface or to allow third party PSPs to access accounts via the user's interface, once they have identified themselves.

For cases where the account servicing PSP opts to provide a dedicated interface, the RTS set out a number of provisions:

- The dedicated interface must have a similar performance level to that provided by the account servicing PSP to its users. The account servicing PSP must develop performance indicators to ensure that this is the case. The competent national authorities must then ensure that third party PSPs meet their obligation to use these interfaces for access at all times;

- Should the dedicated interface become unavailable (inadequate performance), the account servicing PSP must allow third party PSPs to make use of its client-facing interface (using web scraping or screen scraping methods) with a mechanism to identify third party PSPs. Such access must be provided when an access request has been refused five consecutive times within a 30 second period. When the fallback interface is used, third party PSPs must be able to provide justification for this use to the competent authority in their country and must retain a list of accesses to be provided to their competent authority if it so requests;

- The competent national authorities can, after consulting the EBA, exempt account servicing PSPs from providing fallback interfaces if their dedicated interface meets the RTS standards, especially if it has been tested during the six-month period provided for that purpose and has been in use for three months. This exemption must be withdrawn by the national competent authority if the interface ceases to meet the RTS requirements and if the account servicing PSP is no longer able to resolve malfunctions in a two-week period. In such cases, the account servicing PSP must provide a fallback interface within two months.

3.2. The framework for European oversight and its development

The creation of the Single Euro Payments Area (SEPA, see Chapter 2) makes central banks jointly responsible for the security of means of payment of common interest. The Eurosystem therefore developed oversight frameworks applicable to pan-European means of payment, based on the provisions of the Treaty[8] and the Statutes of the European System of Central Banks and the ECB[9] relating to promoting the proper functioning of payment systems:

- In January 2008, an initial oversight framework[10] was developed by the Eurosystem to assess the security and effectiveness of card payments systems. It enabled the Eurosystem's central banks to implement harmonised oversight and obtain a coherent, standardised overview of card payment systems;

- Oversight frameworks for SEPA direct debits[11] and credit transfers[12] were established in August 2009 and October 2010, respectively. They rely on a structure similar to that designed for the oversight framework applicable to card payment systems.

Assessment guides were published for each of the three oversight frameworks to clarify the Eurosystem's expectations. They were updated in 2014 and 2015 to include, in particular, the security recommendations for online payments published by the European Forum on the Security of Retail Payments (SecuRe Pay forum, see below), reiterated in the EBA guidelines issued in December 2014.

On the basis of these oversight frameworks, the Eurosystem conducts oversight exercises among market players. Payment cards were the first cashless means of payment to benefit from joint central bank oversight: 2008 saw the launch of a Europe-wide assessment of all national and international card payment systems in use across the EU. This exercise was repeated in 2016, following the publication of EBA security guidelines for online payments, which have now been incorporated into the oversight framework. More recently, in 2016 the Eurosystem completed an oversight exercise covering SEPA direct debits and launched a similar exercise covering SEPA credit transfers.

As part of their oversight mission, the ECB and national central banks ensure that statistics on payment card fraud, covering all card payment systems in use, are compiled annually at the European level. In the coming years, similar exercises should be rolled out for statistics on fraud involving credit transfers and direct debits.

3.3. Work conducted by the SecuRe Pay forum

Set up in February 2011, the SecuRe Pay forum brings together central bankers and banking sector supervisors. Co-chaired by the ECB and EBA, its purpose is to promote dialogue between national authorities, with a view to establishing a common approach to the security of means of payment.

The first set of recommendations published by the SecuRe Pay forum in January 2013 concerned the security of online payments. The key measure recommended in this first document involved the broad implementation of strong payer identification when initiating online payments, but the forum also addressed a wealth of other measures to make online payments more secure, including the general monitoring and security environment put in place by payment service providers, the building of customer awareness of fraud-related risks and the communication channels used between payment service providers and their customers.

Lastly, the forum also looked at risks associated with the activities of unregulated new players positioning themselves as "third party payment service providers" so

8 Article 127.2 of the TFEU: "The basic tasks to be carried out by the ESCB are: defining and implementing the Union's monetary policy; conducting foreign exchange transactions in compliance with article 219; holding and managing the official reserves of Member States; promoting the proper functioning of payment systems".

9 Articles 3.1 and 22 of the statutes of the ESCB and the ECB.

10 "Oversight framework for card payment scheme standards", January 2008, *http://www.ecb.europa.eu/pub*

11 "Oversight framework for direct debit schemes", August 2009, *http://www.ecb.europa.eu/pub*

12 "Oversight framework for credit transfer schemes", October 2010, *http://www.ecb.europa.eu/pub*

as to offer "payment initiation services" and "account information services". The forum's recommendations, aiming to ensure that satisfactory security conditions were in place for the roll-out of these services, were published in March 2014[13] following a public consultation.

A number of the SecuRe Pay forum's recommendations were included in the revised version of the payment services Directive (PSD2). It was also through the SecuRe Pay forum that the RTS and the guidelines given to the EBA for its formulation of the PSD2 requirements were developed.

To ensure consistent implementation of PSD2 across the European Union, the EBA was tasked with developing, in close cooperation with the ECB, not only the regulatory technical standards (RTS) referred to above, but also guidelines covering, among other aspects, the requirements for managing operational and security risks associated with the provision of payment services, and specifications for the framework for reporting major incidents to the competent authorities.

13 The recommendations can be consulted on the ECB website: *http://www.ecb.europa.eu/pub*