Annual report
of the Observatory for the Security of Payment Means

2016

BANQUE DE FRANCE
EUROSYSTÈME

bservatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

2016 Annual report of the Observatory for the Security of Payment Means

addressed to

The Minister of the Economy and Finance
The President of the Senate
The President of the National Assembly

by

François Villeroy de Galhau,
Governor of the Banque de France,
President of the Observatory for the Security of Payment Means

The Observatoire de la Sécurité des Moyens de Paiement *(Observatory for the Security of Payment Means – hereinafter the Observatory), referred to in section I of Article L141-4 of the French* Code monétaire et financier (Monetary and Financial Code), *was created by the Law of 9 December 2016 No. 2016-1691. The Observatory is intended to promote information-sharing and consultation between all parties concerned by the smooth operation and security of cashless payment instruments (consumers, merchants, businesses, issuers and public authorities).*

Pursuant to the seventh indent of the abovementioned article, the present document reports on the activities of the Observatory. It is addressed to the Minister of the Economy and Finance and transmitted to Parliament.

A word from the president

The national payments strategy launched by the Minister of the Economy in October 2015 seeks to promote the use of innovative, secure and efficient means of payment in France. Innovative solutions are particularly welcome as they enhance the efficiency of payment processes; but the payment ecosystem, and the economy as a whole, can only derive a benefit from technological innovation when this innovation happens in a secure environment, regardless of the technologies used and the players involved. This is a sine qua non *to ensure users' confidence when they use their means of payment.*

France's lawmakers have extended the mandate entrusted to the Observatoire de la sécurité des cartes de paiement *(OSCP – Observatory for Payment Card Security) to all cashless payment instruments. In doing so, they are acknowledging the OSCP's effective contribution to reinforcing the security of card payments, and the versatility that is required when it comes to payment-related innovation, which now goes far beyond card-based solutions: there are new payment initiation channels, new forms of payment and new payment services providers.*

The OSMP is therefore taking on the missions that had been entrusted to the OSCP – monitoring the security measures put in place by issuers, merchants and businesses, compiling aggregate fraud statistics and maintaining a technology watch in the area of payment means – which now cover all forms of cashless payment. This extension will enable the Observatory to perform the security analyses that are essential to the work carried out by the Comité national des paiements scripturaux *(CNPS – National Cashless Payments Committee), tasked with ensuring that the national payments strategy is implemented. These analyses will notably focus on the introduction of instant credit transfer solutions or the promotion of the use of electronic means of payment as an alternative to cheques.*

In a rapidly-changing regulatory environment, with the entry into force in January 2018 of the second European Payment Services Directive, the Observatory will also be an essential forum in the implementation of security provisions of a legal nature. This will be second nature to the Observatory, since some of these provisions long served as a cornerstone for the OSCP's recommendations, namely the generalisation of strong customer authentication for electronic means of payment. The priority will also be to secure access to payment accounts by third parties such as the initiators of payments and aggregators of account information. The OSMP will carry out these missions by promoting a constant dialogue between the

various stakeholders: suppliers and users of payment services (businesses and consumers) and public authorities.

This first annual report provides statistical insight into cashless payment fraud in 2016. Given their prevalence, card payments make up half of the total fraud amount. However, it is important to note that the volume of card fraud has been shrinking for a number of years in domestic transactions and, for the first time, has also decreased across all transactions combined, even for international payments.

Moreover, the figures for fraud in 2016 underpin the directions taken in the national payments strategy as regards the promotion of credit transfers and card payments at points of sale as secure alternatives to cheque-based payments in France. The rate of face-to-face card payment fraud stands at 0.008% (i.e. one euro of fraud for every EUR 12,500 in transactions), notably with the rise in contactless card use in which fraud is being kept low (0.020%) and the rate of credit transfer fraud is even lower (one euro for every EUR 275,000), whereas cheque-related fraud stands at 0.025% (one euro for every EUR 4,000).

In such circumstances, the Observatory is bound to play a crucial role in continuing to ensure that users are confident when using existing and future means of payment. I would like to thank all members of the Observatory and of the Banque de France departments, every one of whom is committed to keeping payment fraud to a minimum.

François Villeroy de Galhau
Observatory President

Summary

This first annual report of the Observatory for the Security of Payment Means provides the general public with information and statistics for the first time on fraud involving all the various means of cashless payment. Until now, such information has only been available for payment cards. In it, the Observatory makes the following observations:

• Fraud involving cashless means of payment issued in France represents roughly EUR 800 million overall. This may seem like a relatively small amount comparatively speaking, considering that some EUR 27,000 billion in payments are processed annually in France. However, it is a substantial cost borne by the users and the providers of payment services.

• Payment cards, which are still the preferred method of payment for French consumers (used in almost half of cashless transactions), account for more than 50% of the fraud involving cashless means of payment issued in France, i.e. around EUR 400 million in 2016 for French-issued cards (with a fraud rate of 0.064%). This type of fraud has two main characteristics: it targets card-not-present (CNP) payments in particular, notably online, which account for two thirds of the fraud amount but only 12% of transactions; and it also affects cross-border transactions more strongly than domestic transactions, with the former making up more than 60% of the fraud amount even though they account for just 15% of transactions.

Within France, and for the first time since the early 2000s, the transaction fraud amount has fallen by around 4%, even though payment card use has risen by 6%, fuelled mainly by the development of contactless payment technology. The rate of card fraud has fallen for the second year in a row across all usage categories: face to-face payments (down to 0.008%, of which 0.020% attributable to contactless payments), card-not-present payments (down to 0.199%) and ATM withdrawals (0.029%). All participants have helped lower the rate of card fraud by developing strong customer authentication solutions for online payments, and with card issuers and card payment schemes also putting transaction scoring solutions in place.

For international payments, fraud affecting transactions within the Single Euro Payments Area (SEPA) is now better controlled on the whole, helped by the introduction of ever more stringent European regulations on payment security. Increasing use of strong authentication solutions for card-not-present transactions, and gradual smartcard deployment across Europe

and beyond, have helped stabilise the fraud at a time when the number of cross-border transactions is rising.

• Cheques are the second means of payment most affected by fraud, which amounted to close to EUR 272 million in 2016 (i.e. a fraud rate of 0.025%). There are two main categories of cheque-related fraud, with very little to separate the two in terms of prevalence: fraudulent use of lost or stolen cheques, which makes up 44% of overall cheque fraud; and the falsification of cheques, i.e. the fraudulent modification of the amount or the beneficiary of a valid cheque, which accounts for 42%.

Given the particular characteristics of cheques, fraud prevention hinges first and foremost on the vigilance of users, be they the payer or the payee, to prevent risks of theft, loss and falsification.

• Credit transfers involve a lower fraud amount, around EUR 86 million in 2016 and, proportionally speaking, are far less affected than cards and cheques, with a fraud rate that is more than sixty times lower than for those two methods of payment.

Credit transfer fraud shares some similarities with card fraud, insofar as online transactions (via the account holder's online bank account) and cross-border transactions are more affected by fraud. The manner in which fraud affects account holders can differ depending on their nature: private individuals are usually targeted by malware or phishing campaigns in which the fraudsters attempt to gather their online banking credentials in order to impersonate the account holder and initiate fraudulent credit transfers; while businesses are also targeted in this way, they can also fall victim to social engineering attacks, in which the fraudster poses as a person with whom the business usual deals (a supplier, a director of the company, etc.) in order to trick them into issuing an illegitimate payment order.

The account-holding banks can prevent credit transfer fraud by putting transaction analysis mechanisms in place to identify any unusual transactions and contacting the holder of the account before approving them. This prevention also relies on strong authentication mechanisms to approve payment orders. However, businesses and individuals must remain on their guard in order to identify any fraudulent requests made of them and protect their IT tools and environments (installing virus protection software and setting up firewalls, deleting suspicious email attachments without opening them, etc.).

• Lastly, direct debit and commercial paper fraud account for the lowest fraud amounts, at around EUR 40 million and EUR 1 million respectively in 2016. This type of fraud targets almost exclusively domestic transactions, despite the European nature of SEPA direct debits. Fraud prevention with these means of payment first requires that banks be familiar with their clients' payment usage profiles, be they the creditor or the payer, and put alert mechanisms in place that would be triggered should an unusual or unexpected transaction arise, such as a request to add a new name for a direct debit mandate.

All this data relies on a statistical methodology that is harmonised across all means of payment, presented in detail in Chapter 1 of this report. This approach fits in with the methodological framework previously applied by the Observatory for Payment Card Security (OSCP). The continuity that this approach affords enables to draw on the entire set of statistical data that has been compiled for payment card fraud since the early 2000s.

Lastly, in keeping with the technology watch conducted by the OSCP, this annual report also contains a study into the security of m-POS (mobile point-of-sale) payment terminals in which a smartphone or a tablet is used for the acceptance of card payments. The Observatory draws particular attention to the need to subject these new types of payment terminals to the requirements in place for electronic payment terminals as regards the protection of PIN entry, and to encrypt the data to avoid any vulnerability that might arise due to the use of non-certified payment terminals (smartphone or tablet).

1 Methodological approach used to measure fraud on cashless payment means

1.1 General framework

Definition of means of payment fraud

In this report, fraud is understood as the **illegitimate use of a means of payment or its related data and any act that contributes to the preparation for illegitimate use and/or effective illegitimate use of them:**

- **resulting in a financial loss:** for the account-holding bank and/or issuer of the means of payment, the holder of the means of payment, the lawful beneficiary of the funds (the acceptor and/or creditor), an insurer, a trusted third party or any party involved in the chain of design, manufacture, transport or distribution of physical or logical data that could incur civil, commercial or criminal liability;
- **by whatever means:**
  - the methods used to obtain, without lawful reason, the means of payment or related data (theft, taking possession of the payment means or data, hacking of acceptance devices, etc.);
  - the procedures for using the means of payment or related data (payments/withdrawals, face-to-face or card-not-present (CNP), via physical use of the means of payment or the related data, etc.);
  - the geographical area of issuance or use of the means of payment and related data;
- **regardless of the identity of the fraudster:** a third party, the account-holding bank and/or issuer of the means of payment, the lawful holder of the means of payment, the lawful beneficiary of the funds, a trusted third party, etc.

In accordance with this definition, the Observatory measures fraud by recording all payment transactions that have given rise to an entry on the account of at least one of the counterparties of the transaction and which have subsequently been rejected on fraud-related grounds. The following are therefore not recorded as fraud:

- attempted fraud (when the fraud is foiled before the transaction is processed);
- improper use of a means of payment by reason only of insufficient

funds and resulting notably in a non-payment;

• the use of a false or stolen identity to open an account and/or obtain a means of payment for the purposes of making payments.

The Observatory applies a "gross approach" when measuring fraud, which consists in identifying the initial payment transaction amounts without taking into account any measures that may subsequently be taken by the counterparties to mitigate the related losses (for instance, the interruption of product delivery or service provision, out-of-court agreement to reschedule payment in the event of wrongful repudiation of the payment, damages and interest subsequent to legal proceedings, etc.). In its 2015 annual report,[1] the Observatory for Payment Card Security estimated that such measures reduced the gross estimate of card payment fraud by 5%.

The Observatory's secretariat gathers the fraud data from all relevant institutions, using different approaches depending on the means of payment (see below). Due to the confidential nature of the personal data gathered, only national consolidated statistics are made available to the members of the Observatory and presented in its annual report.

Typologies of means of payment fraud

In order to analyse means of payment fraud, the Observatory defined five fraud typologies, bearing in mind that they do not all apply in the same manner to the various payment instruments:

• loss/theft: fraud involving the use of a physical payment instrument (card, chequebook, etc.) that has been lost or stolen;

• counterfeiting: fraud involving the use of a counterfeit payment instrument or of misappropriated payment data;

• forgery: fraud involving the use of a forged payment instrument (an authentic payment instrument in which the physical characteristics or related data have been modified by the fraudster or an accomplice) or of a validly-issued payment order to which one or more alterations have been made (amount, currency, name of the beneficiary, account details of the beneficiary, etc.);

• misappropriation: fraud in which the intention is to use the payment instrument or payment order without forgery or alteration (for example, the cashing of a non-forged cheque on an account that is not held in the name of the lawful beneficiary of the cheque);

• "replay": fraud involving the wrongful use of a payment instrument by its lawful holder after it has been reported lost or stolen or through the dispute of a valid payment order by the lawful holder of the payment instrument, acting in bad faith, or the re-use of a payment order that has already been processed.

1 *https://www.banque-france.fr/en/financial-stability/observatory-security-payment-means*

1.2 Measurement of payment card fraud

Transactions covered

Payment card fraud, as measured in this report, covers payments (face-to-face and CNP) and withdrawals made using a payment card in France and abroad when one of the counterparties to the transaction is considered to be French: when the issuer is a French financial institution or the acquiring institution is domiciled in France. No distinction is made as to the nature of the acceptance network (four-party/open[2] or three-party/closed[3] payment schemes) or card category (debit card, credit card, commercial card or prepaid card).

Source of fraud data

The Observatory gathers payment card fraud data:

- through the consortium from members of the "CB" Bank Card Consortium (*Groupement des cartes bancaires CB*), and from MasterCard and Visa Europe France;
- from three-party card issuers operating in France.

Analysis of fraud

Analysis of payment card fraud takes a number of parameters into consideration: type of fraud, payment initiation channel, geographical area of issuance and use of the card or of the data held on it and, in the case of CNP payments, the merchant's sector of activity.

2 Payment card systems that involve a large number of payment services providers, card issuers and payment acquirers.

3 Payment card systems that involve a small number of payment services providers, card issuers and payment acquirers (for example, within a single banking group).

Typology of payment card fraud	Forms of fraud
Lost or stolen cards	The fraudster uses a lost or stolen credit card, without the lawful cardholder's knowledge.
Intercepted cards	The card is intercepted when the issuer sends it to the lawful cardholder. This type of fraud is similar to card loss or theft. However, the difference is that it is difficult for the lawful cardholder to ascertain that a fraudster is in possession of a card that belongs to them. In such cases, the fraudster seeks to exploit vulnerabilities in the procedures used to send cards.
Forged or counterfeit cards	Forgery of a payment card consists in modifying an authentic card's magnetic stripe data, embossing[a] or programming. Counterfeiting a card means creating an object that appears to be an authentic payment card and/or is capable of deceiving an unattended payment terminal (UPT) or a merchant's payment terminal. In both cases, the fraudster endeavours to create a card that incorporates the data required to deceive the acceptance system.
Misappropriated card numbers	A cardholder's card number is taken without his/her knowledge or created through card number generation[b] and used in card-not-present transactions.
Unallocated card numbers	Use of a true card number (or PAN: Personal Account Number) that has not been attributed to a cardholder, generally in card-not-present transactions.

a) Modification of the raised numbers printed to form the card number.
b) A technique that consists in using issuers' own rules for creating payment card numbers to generate such numbers.

Card usage channels	Procedures for using the card
Face-to-face payment	Payments made at a point of sale or through a UPT, including contactless payments.
Card-not-present payment	Payments carried out online, by mail, by fax/telephone, or any other means.
Withdrawal	Cash withdrawals at ATMs.
Geographical area	**Description**
Domestic transaction	Both the issuer and the acquirer are established in France. However, for card-not-present payments, the fraudster may operate from abroad.
International FR ➔ SEPA transaction	The issuer is established in France and the acquirer abroad within SEPA.
International FR ➔ non-SEPA transaction	The issuer is established in France and the acquirer abroad outside SEPA.
International SEPA ➔ FR transaction	The issuer is established abroad within SEPA and the acquirer in France.
International non-SEPA ➔ FR transaction	The issuer is established abroad outside SEPA and the acquirer in France.
Merchant's sector of activity for CNP payments	**Description of the sector of activity**
Foodstuffs	Groceries, supermarkets, hypermarkets, etc.
Account loading, person-to-person sales	Sites enabling online sales between private individuals, etc.
Insurance	Insurance policy subscription.
General and semi-general trade	Textiles/apparel, department stores, mail-order sales, private sales, etc.
Household items	Sale of furnishings and DIY products.
Online gaming	Online gaming and betting sites.
Technical and cultural products	IT hardware and software, photographic equipment, books, CDs/DVDs, etc.
Health, beauty and personal care	Sale of pharmaceutical products, personal care products and cosmetics.
Personal and professional services	Hotels, rental services, box office, charities, office equipment, courier service, etc.
Telephony and communication	Telecommunication/mobile telephony equipment and services.
Travel/transportation	Rail, air, sea.
Other	

1.3 Measurement of credit transfer fraud

Payment instruments covered

Credit transfer fraud, as measured in this report, covers payment orders issued by the debtor – the payer – to transfer funds from his/her payment account or electronic purse to the account of a third-party beneficiary. This includes SEPA credit transfers and customer credit transfers issued via large-value payment systems (notably the TARGET2 system operated by the national central banks of the Eurosystem and the pan-European EURO1 private sector system).

Source of fraud data

The data relating to credit transfer fraud is provided by the Banque de France and taken from the annual mandatory fraud reports filed by authorised payment services providers.[4] To avoid any risk of double reporting, only the institution that has executed the credit transfer files such a report.

Analysis of fraud

Credit transfer fraud is analysed by looking at the fraud typologies, geographical areas of issuance and destination of the transfer and the initiation channels used.

4 Financial institutions that are authorised to hold payment accounts on behalf of their customers and to issue means of payment, which have the following statuses within the meaning of French and European regulations:

- credit institutions or equivalent (institutions referred to in Article L518-1 of the *Monetary and Financial Code*), electronic money institutions and payment institutions incorporated in France;
- credit institutions, electronic money institutions and payment institutions incorporated abroad that are authorised to operate and are established in France.

Typologies of credit transfer fraud	Forms of fraud
Forgery	The fraudster counterfeits a credit transfer order, forces the lawful account holder to issue a transfer order, or fraudulently acquires the lawful payer's online banking credentials in order to initiate a payment order (in this case, the credentials may be obtained through hacking methods (phishing, malware, etc.) or under duress.
Falsification	The fraudster intercepts and modifies a transfer order or a legitimate remittance document.
Misappropriation	Through deception (notably social engineering, which involves impersonating a person with whom the payer has business dealings: line manager, supplier, bank clerk, etc.), the fraudster induces the lawful account holder to issue a transfer order in due form to an account number that is not the account of the lawful beneficiary of the payment or does not correspond to any economic reality.

Geographical area of issuance and destination of the credit transfer	Description
Domestic transfer	Transfer issued from an account held in France towards an account held in France.
European transfer	Transfer issued from an account held in France towards an account held in another SEPA country.
Non-SEPA transfer	Transfer issued from an account held in France towards an account held in a non-SEPA country.

Initiation channels used	Procedures for use
Paper	Transfer orders sent by mail, through a form, email, fax or phone.
Online	Transfer orders sent via an online bank or a mobile payment application.
Telematics	Transfer orders sent via electronic channels other than online banking and mobile payment application channels, such as the EBICS (Electronic Banking Internet Communication Standard) system (interbank communication channel through which businesses can exchange automated data files with banks).

1.4 Measurement of direct debit fraud

Payment instruments covered

Direct debit fraud, as measured in this report, covers payment instructions given by a creditor to their payment services provider for them to debit the account of a debtor, in accordance with the authorisation (or direct debit mandate) that the debtor has signed. This includes SEPA direct debits and, up to 1 February 2016, French interbank payment orders (*Titres interbancaires de paiement* – TIP) and electronic payment orders (*télé-règlement*), non-SEPA domestic means of payment equivalent to direct debit payments that were legal tender up to that date.

Source of fraud data

The data relating to direct debit fraud is provided by the Banque de France and taken from the annual mandatory fraud reports filed by authorised payment services providers. Depending on the typology of the fraud, the fraud is either reported by the payment service provider of the creditor (forgery, misappropriation) or by that of the debtor ("replay"), thus

Typologies of direct debit fraud	Forms of fraud
Forgery	Fraud at the creditor's end: the fraudster originates direct debit instructions using illegally obtained account numbers, without any authorisation or underlying economic reality.
	Fraud at the payer's end: the fraudster steals the identity and IBAN of a third party to sign a direct debit mandate on an account that does not belong to him/her.
Misappropriation	The fraudster changes the account number to be credited as per direct debit documents that have been issued in due form, or steals a SEPA Creditor Identifier in order to originate direct debit instructions for payment to themselves from accounts for which the creditor holds legitimate mandates.
Replay	The creditor knowingly originates direct debits that have already been issued (that have either already been settled or rejected, for instance, following a request by the payer to block the transaction).

Geographical area of issuance and destination of the direct debit	Description
Domestic direct debit	Direct debit instruction originated by a creditor whose account is held in France for payment from an account held in France.
European direct debit	Direct debit instruction originated by a creditor whose account is held in France for payment from an account held in another SEPA country.
Non-SEPA direct debit	Direct debit instruction originated by a creditor whose account is held in France for payment from an account held in a non-SEPA country.

Initiation channels used	Procedures for use
Paper	Transfer orders sent by mail, through a form, email, fax or phone.
Online	Transfer orders sent via an online bank or a mobile payment application.
Telematics	Transfer orders sent via electronic channels other than online banking and mobile payment application channels.

avoiding any risk of double counting or undervaluation of the fraud data.

Analysis of fraud

Direct debit fraud is analysed by looking at the fraud typologies, geographical areas of issuance and destination of the direct debit and the authorisation channels used.

1.5 Measurement of cheque fraud

Unlike other cashless means of payment, cheques only exist in paper form and the payer's signature is the only means of authentication by his/her bank. This makes it impossible for banks to put automatic authentication systems in place before payment.

Scope of fraud

Cheque-related fraud, as measured in this report, covers cheques payable in France, in euros or a foreign currency (in this case, the cheque is to be drawn on a payment account held in foreign currency), falling within the legal framework set forth in Articles L131-1 to 88 of the *French Monetary and Financial Code*. This specifically

Cheque fraud typologies	Forms of fraud	Reporting bank
Fake (theft/loss/apocryphal[a])	Use by the fraudster of a cheque that has been lost by or stolen from the lawful owner, which carries a forged signature that corresponds to neither the signature of the account holder or of their authorised representative.	Collecting bank
	Unlawful issuance of a cheque by a fraudster using a blank cheque specimen[b] (including transactions carried out under duress by the legitimate account holder).	
Counterfeiting	False cheque entirely fabricated by the fraudster to be drawn on an existing or fake bank.	
Falsification	Valid cheque intercepted by a fraudster who deliberately alters it by scratching, rubbing out or erasing the information contained on it.	
Misappropriation/replay	Re-cashing of a cheque that was lost or stolen after being cleared in the payment systems.	Paying bank
	Lost or stolen valid cheque, intercepted en route to the beneficiary and cashed on an account other than that of the lawful beneficiary. The cheque specimen is correct, the name of the beneficiary unchanged and the MICR (Magnetic Ink Character Recognition) line of numbers and characters at the bottom is valid, as is the customer's signature.	
	Deliberate issuance of a cheque by the account holder after a request to block the cheque.	

a) Apocryphal: a term that some banks use to qualify a document that is of doubtful authenticity.
b) Blank cheque specimen: made available to the customer by the account-holding bank.

concerns cheques drawn by the customers of a bank on accounts that are held by that bank and cheques received from the customers of a bank for deposit on such accounts.

This definition encompasses the following payment orders: bank cheques, banker's drafts, cheque-letters for businesses and *titres de travail simplifiés* (TTS – simplified employment cheques for small businesses); it does not include travellers cheques or special payment vouchers referred to in Article L525-4 of the *Monetary and Financial Code*, such as holiday vouchers, luncheon vouchers, culture cheques and *chèques emploi-service universels* (CESU – universal employment service vouchers), which span a variety of categories and can only be used for specific products and services or in a small number of acceptance networks.

Source of fraud data

The data relating to cheque fraud is provided by the Banque de France and taken from the annual mandatory fraud reports filed by authorised payment services providers. These payment services providers either report as the financial institution that receives cheques to be cashed from their customers (the collecting bank) or as the institution that holds the payer's account (the paying bank).

- Data pertaining to fraud that falls into the "theft, loss (forgery, apocryphal)", "counterfeiting" and "falsification" categories is reported by the collecting banks.

- Data pertaining to fraud that falls into the "misappropriation, replay" category, in which a cleared cheque is presented a second time to be cashed, is reported by the paying banks, since such instances are usually detected by their fraud departments.

The division of these reporting roles helps avoid any risk of double counting or undervaluation of the fraud data gathered.

Analysis of the data

The Observatory analyses cheque fraud data based on the main typologies of fraud that it has defined.

The preceding table summarises the most common forms of fraud observed, their typology and the reporting bank.

1.6 Measurement of commercial paper fraud

Payment instruments covered

Commercial paper fraud, as measured in this report, covers two payment instruments:

- truncated bills of exchange: payment instruments in paper or electronic form by means of which the payer (generally the supplier) issues an order for the debtor (its customer) to pay it a particular sum of money;

- truncated promissory notes: an electronic payment instrument by means of which the payer acknowledges its liability towards the beneficiary and undertakes to pay a certain sum of money by a certain date, both of which are specified on the note.

Typology and source of fraud data

The typologies of commercial paper fraud are the same as those defined for cheques.

The data relating to draft fraud is provided by the Banque de France

and taken from the annual mandatory fraud reports filed by authorised payment services providers. These payment services providers either report as the financial institution that receives commercial papers to be honoured from their customers (the collecting bank) or as the institution that holds the payer's account (the paying bank).

- Data pertaining to fraud that falls into the "theft, loss (forgery, apocryphal)", "counterfeiting" and "falsification" categories is reported by the collecting banks.

- Data pertaining to fraud that falls into the "misappropriation, replay" category, in which a draft that has already been honoured is presented a second time, is reported by the paying banks, since such instances are usually detected by their fraud departments.

The division of these reporting roles helps avoid any risk of double counting or undervaluation of the fraud data gathered.

1.7 Specific provisions relating to fraud on e-money transactions

Electronic money is a monetary value that is stored in electronic form, representing a claim on the issuer, which must be pre-charged using another payment instrument, and can be accepted as payment by a natural person or legal entity other than the electronic money issuer.

Electronic money can be stored in two ways:

- physically, on prepaid cards for instance;

- online, in accounts held by the issuing bank.

The Observatory incorporates the measurement of e-money fraud into its measurement of fraud involving:

- payment cards, when the e-money is stored in physical form (prepaid cards);

- credit transfers, when the e-money is stored in online accounts.

2 Fraud in 2016

2.1 Overview

Means of payment

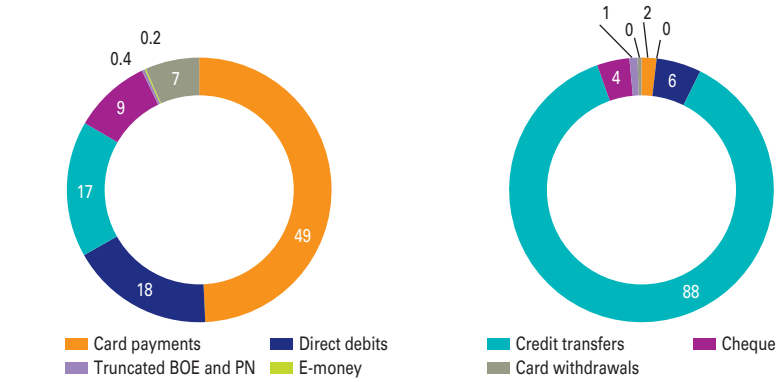
The customers (individuals and businesses) of French banks and payment services providers carried out 22.6 billion cashless transactions in 2016 totalling EUR 27,161 billion. By comparison with the previous year, the number of transactions rose by 5% and the amounts exchanged increased by 3%.

Payments by card remained the preferred payment method in France, being used in almost half of cashless transactions based on volume (49%) for a total amount of EUR 499 billion in 2016. Cash withdrawals by card accounted for 1,491 million transactions, totalling EUR 129 billion.

Credit transfers were still the favourite method of payment for large amounts (salary and pension payments, intercompany payments, etc.), making up 88% of the total

C1 Use of cashless means of payment in France in 2016

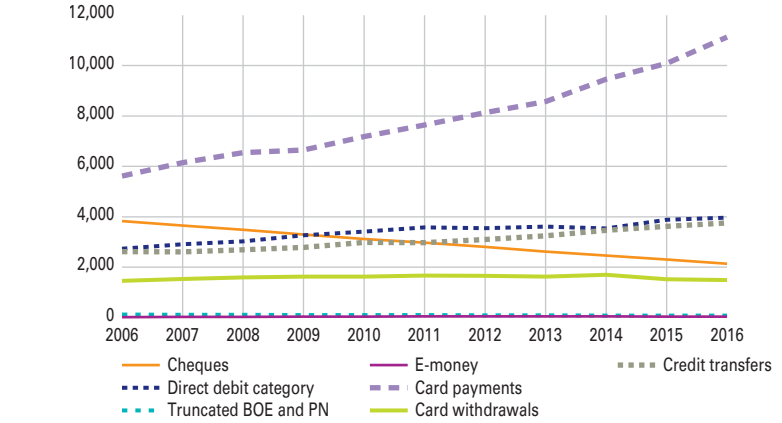
(as a %)



Source: Observatory for the Security of Payment Means.

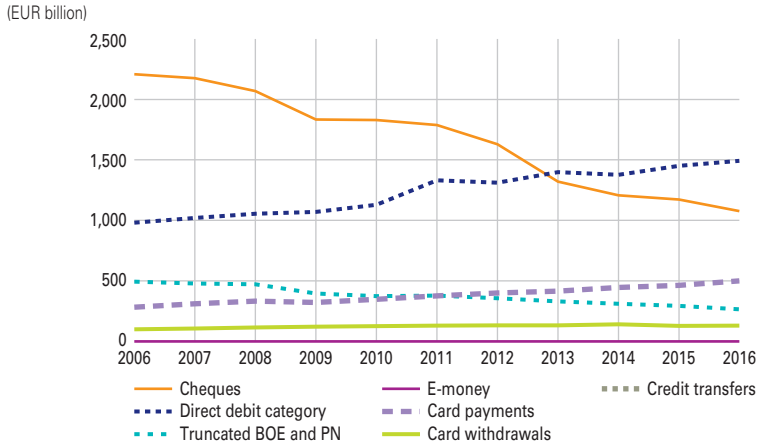
C2 Use of means of payment in France since 2006

(in millions of transactions)



Source: Observatory for the Security of Payment Means.

C3 Transaction amounts in France excluding credit transfers

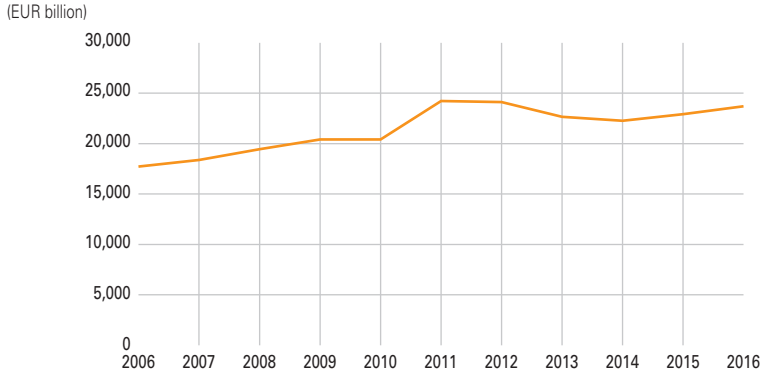


Source: Observatory for the Security of Payment Means.

cashless transaction amount. They ranked in third position (17%) in terms of the number of transactions, just after direct debits and well behind card payments. Credit transfers were primarily issued domestically (77% of total credit transfers), with SEPA transactions accounting for 18% and non-SEPA payments 4%.

Direct debit was the second most common form of cashless payment, both in number (18%) and value (6%). Direct debit transactions were almost exclusively domestic, with cross-border SEPA direct debit transactions accounting for less than 1% of all flows originated.

C4 Credit transfer amounts in France



Source: Observatory for the Security of Payment Means.

Cheque transactions have been falling steadily for a number of years and this situation continued in 2016, both in number (down 8%) and value (8% fall). Some 2.1 billion cheques were issued in 2016, representing a total amount of EUR 1,077 billion, i.e. 9.5% of cashless payments in volume and 4% in value.

Truncated bills of exchange and promissory notes made up less than 1% of cashless transactions in volume and value, with 2016 confirming a steady decline, both in terms of amount (down 9%) and transaction numbers (down 3%).

Lastly, the use of **electronic money** remained marginal in France with 38 million transactions, corresponding to a total value of EUR 591 million.

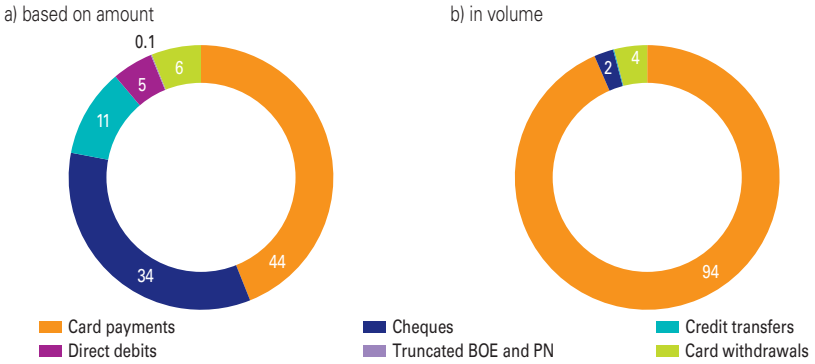
Fraud affecting means of payment

In 2016, cashless transaction fraud totalled approximately EUR 800 million, with 4.8 million fraudulent transactions being perpetrated.

Payment cards[1] accounted for half of the total fraud amount, i.e. close to EUR 400 million for both payments and withdrawals combined, and very close to all fraudulent transactions (97%). Nevertheless, after several years of growth, the overall fraud amount relating to cards issued in France fell for the first time in 2016; this meant that, after levelling out over a number of years, the fraud rate decreased to 0.064%, i.e. one euro of fraud for every EUR 1,600 worth of transactions. However, contrasting situations combined to create this average rate, notably with a very low rate in point-of-sale payments (0.008%, or one euro of fraud for every EUR 12,500 worth of transactions) but a much higher rate in card-not-present payments (0.199%, or one euro for every EUR 500).

C5 Distribution of fraud affecting cashless payment means in 2016

(as a %)



Source: Observatory for the Security of Payment Means.

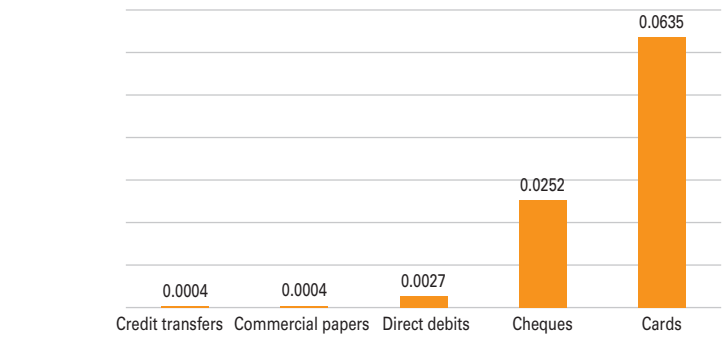
Cheques were the second means of payment most targeted by fraud in 2016, with fraudulent transactions amounting to close to EUR 272 million, even though it was only the fourth most common form of payment used. The fraud rate on cheques stood at 0.025%, slightly lower than the rate recorded for card transactions and equating to one euro of fraud for every EUR 4,000 in payments.

At EUR 86 million in 2016, the annual **credit transfer** fraud amount was well below the levels recorded for cards and cheques. Given that credit transfers involve large transaction amounts, they registered the lowest rate of fraud across all cashless means of payment, at 0.0004% or one euro for every EUR 275,000 paid.

Direct debits recorded a lower fraud amount in 2016 at around EUR 40 million, with an intermediate fraud rate of 0.003%, i.e. one euro

C6 Fraud rate for each means of payment

(as a %)



Source: Observatory for the Security of Payment Means.

1 Cards issued in France and used in France and abroad.

for every EUR 37,000 in direct debit instructions originated.

Commercial papers are relatively unaffected by fraud, which amounted to around EUR 1 million in 2016, with a similar fraud rate to credit transfers of 0.0004%.

2.2 Card payment and withdrawal fraud

The Observatory for Payment Card Security (OSCP) has compiled fraud statistics for three-party and four-party cards since 2003, using data collected from issuers and accepters. The statistics use harmonised definitions and typologies that were established in the OSCP's first year of operation and are provided in Appendix 6 to this report. The working group on fraud statistics recently conducted a qualitative study that confirmed the

Box 1

Fraud statistics for card payments: respondents

To ensure the quality and representativeness of its fraud statistics, the Observatory gathers data from all issuers of "four-party" and "three-party" cards.[1]

The 2016 statistics calculated by the Observatory thus cover:

- EUR 612.1 billion in transactions in France and in other countries performed with 73.4 million four-party cards issued in France (including 44.5 million contactless cards);
- EUR 16.3 billion in transactions (primarily in France) with 10.9 million three-party cards issued in France;
- EUR 44.8 billion in transactions in France with foreign three-party and four-party cards.

Data was gathered from:

- the 120 members of the "CB" Bank Card Consortium (i.e. *Groupement des Cartes Bancaires CB*). The data was collected through the consortium and from MasterCard and Visa Europe France;
- nine three-party card issuers: American Express, Oney Bank, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance, Cofidis, Diners Club, Franfinance, JCB and UnionPay International.

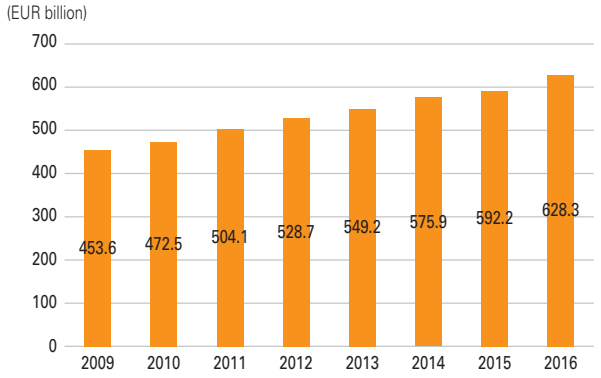
1 "Four-party" card payment schemes involve a large number of issuing and acquiring payment services providers; whereas "three-party" schemes involve a smaller number.

appropriateness of this approach (see previous chapter). The work of the Observatory for the Security of Payment Means will continue in this vein (see Chapter 1).

Overview

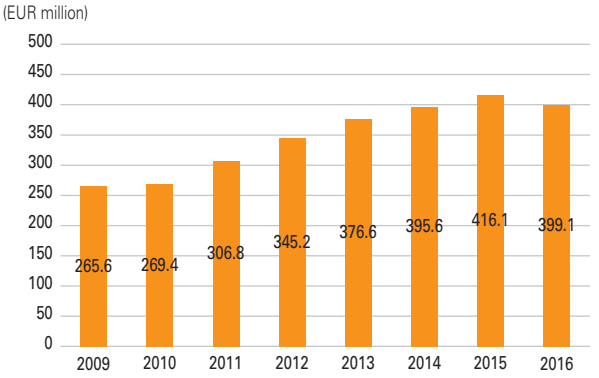
In 2016, the total fraud amount involving payments and withdrawals made using French payment cards in France and abroad came to EUR 399.1 million, down 4.1% compared to 2015. Meanwhile, the total value of transactions increased by 6.1% relative to 2015 to EUR 628.3 billion.

C7 Transaction amount, French cards



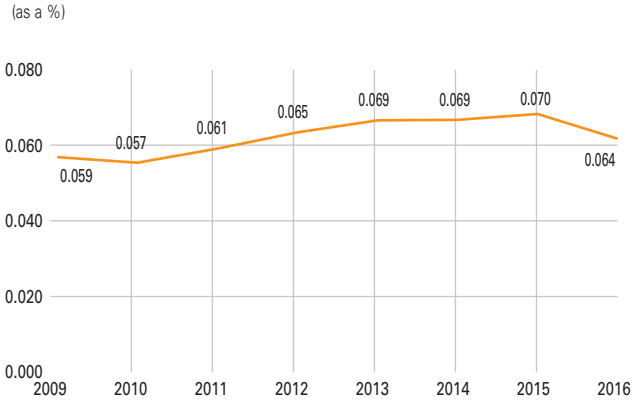
Source: Observatory for the Security of Payment Means.

C8 Fraud amount, French cards



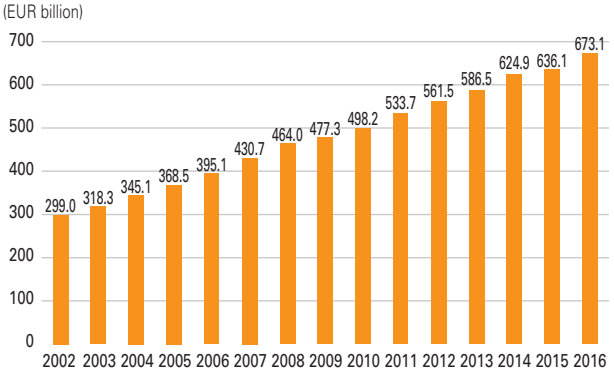
Source: Observatory for the Security of Payment Means.

C9 Fraud rate, French cards



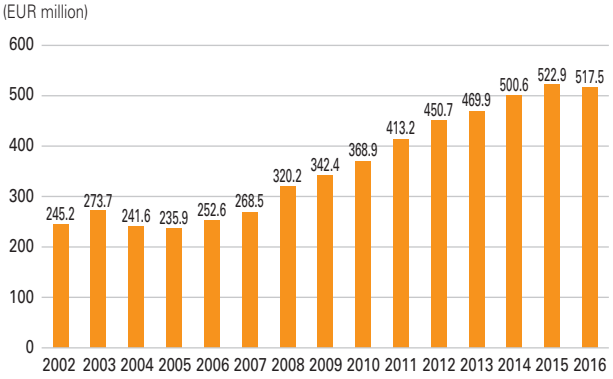
Source: Observatory for the Security of Payment Means.

C10 Transaction amounts processed in French payment systems, French and foreign cards



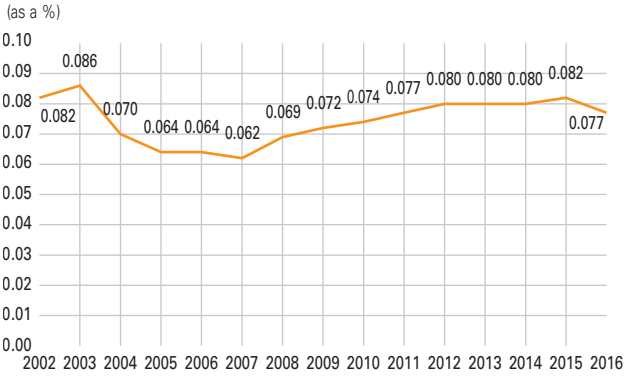
Source: Observatory for the Security of Payment Means.

C11 Fraud amount on transactions processed in French payment systems, French and foreign cards



Source: Observatory for the Security of Payment Means.

C12 Fraud rate on transactions processed in French payment systems, French and foreign cards



Source: Observatory for the Security of Payment Means.

This implies that **the rate of fraud affecting French payment cards registered a marked decrease in 2016, down from 0.070% the previous year to 0.064%** (see Chart 9).

The number of French cards for which at least one fraudulent transaction was recorded in 2016 rose by 31% compared with 2015 to 1,138,200.

When transactions conducted in France using cards issued in other countries are also included, the total fraud amount fell by 1.0% compared with 2015 to EUR 517.5 million in 2016, while the total value of transactions climbed 5.8% to EUR 673.1 billion.

As a result, **the overall fraud rate for transactions processed by French systems**, which includes payments and withdrawals made in France and abroad using French cards, along with payments and withdrawals made in France using foreign cards, **decreased significantly from 0.082% in 2015 to 0.077%**.

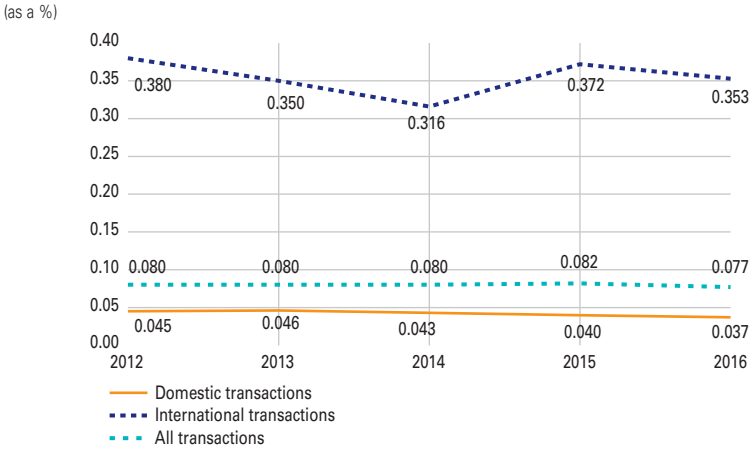
The average fraudulent transaction amount fell to EUR 95, down from EUR 113 in 2015.

Geographical breakdown of fraud

The downtrend that began in domestic transaction fraud in 2014 continued into 2016, **with a decrease of close to EUR 8 million** to EUR 217.2 million. The fraud rate also moved down to 0.037% from 0.040% in 2015.

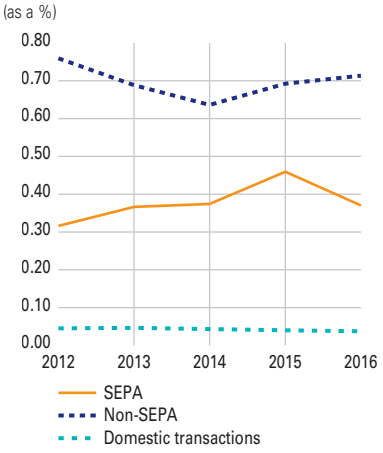
The fraud rate in international transactions decreased also, shrinking to 0.353%. However, the fraud rate for international transactions is still around ten times higher than the rate for domestic transactions. Given the growth in international transactions, the fraud amount continued to trend slightly upwards, coming to EUR 300.3 million compared with EUR 297.9 million in 2015.

C13 Fraud rate by geographical area



Source: Observatory for the Security of Payment Means.

C14 Fraud rate by geographical area – French holders



Source: Observatory for the Security of Payment Means.

International transactions thus accounted for 58.0% of the total fraud amount even though they made up just **12.6% of the total value of the transactions.**

Within international transactions, fraud continues to be kept lower for transactions inside SEPA[2] as compared with transactions involving non-SEPA countries:

- in the case of French cards, the fraud rate for transactions carried out outside SEPA (0.713%) was almost twice as high as the rate for transactions carried out within SEPA (0.370%);

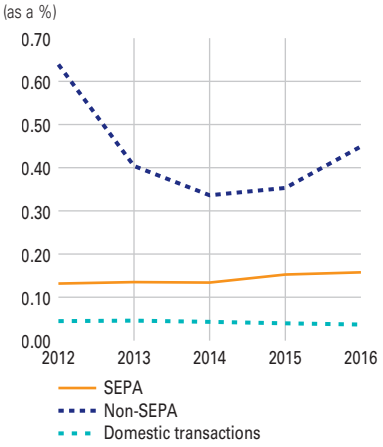
- in the case of foreign cards, the fraud rate for transactions carried out in France using cards issued outside SEPA (0.449%) was almost three times as high as the rate for cards issued within SEPA (0.158%).

These figures underpin the efforts that have been made in Europe for many years now to migrate all cards and payment terminals to the EMV (Europay, MasterCard and Visa) standard and enhance the security of Internet payments.[3]

2 SEPA covers the 28 European Union Member States, as well as Monaco, Switzerland, Liechtenstein, Norway, Iceland and San Marino.

3 The European Banking Authority's guidelines to enhance the security of Internet payments came into force in August 2015.

C15 Fraud rate by geographical area – French merchants



Source: Observatory for the Security of Payment Means.

Box 2

Fraud targeting contactless card payments

The Observatory gathered data to measure the fraud rate for contactless payments for the third year in a row. A total of 628.5 million contactless payments were recorded for 2016 as a whole, worth a total of EUR 6,450.7 million, representing respectively 6.5% in volume and 1.6% in value of face-to-face payments, with an average transaction value of EUR 12.5. Some 119,000 fraudulent payments were recorded over the same period for a total transaction amount of EUR 1.298 million. *This put the rate of fraud in contactless transactions at 0.020%* for the period. As in 2015, when it stood at 0.019%, the fraud rate was midway between the overall rate for face-to-face payments across all methods of payment (0.008%) and the rate for withdrawals (0.029%), thus well below the level for card-not-Present (CNP) payments (0.199%).

As in 2015, fraud in contactless payments could almost always be traced back to theft or loss of the card. However, amid the very strong growth in contactless payments, which increased by a factor of 2.5 between 2015 and 2016, the share of fraud originating from the loss or theft of cards has continued to decrease steadily. Moreover, card issuers have placed ceilings on individual transactions (usually EUR 20 or EUR 25) and on the total consecutive transaction amount possible without entering the PIN (typically EUR 100), thus limiting the loss amount if a card is lost or stolen.

The Observatory reiterates that cardholders are protected by law in the event of fraud. In France, they have 13 months[1] to challenge unauthorised transactions by contacting their payment services provider, which must refund the amount promptly. Cardholders are also encouraged to contact their issuing institution promptly to report their card lost or stolen. In the event of fraud resulting from a contactless payment made following the theft or loss of a card, the cardholder will not bear any losses linked to this unauthorised payment transaction.[2]

As the use of contactless payment functions continues to grow rapidly, with almost 45 million cards featuring contactless payment capabilities in circulation at the end of December 2016, the Observatory calls on issuers to

1 See details in Appendix 2.

2 See Appendix 1: a card payment in contactless mode is performed without using the card's personalised security features (no PIN entered), which means that even before reporting the card lost or stolen, the holder is not liable for losses linked to unauthorised payments.

.../...

remain on their guard and reminds them of the commitments they have made regarding the ability to deactivate the contactless function: i) users must be provided with protective covers for their cards,[3] or ii) it should be possible to switch off the contactless function remotely,[4] or iii) cardholders must be able to ask to replace their contactless card with a non-contactless card.

As the overseer of cashless means of payment, the Banque de France is monitoring implementation of these measures.

3 Protective covers block NFC radio waves, preventing the card from being activated unintentionally.

4 The contactless function is disabled by executing an EMV (Europay, MasterCard and Visa) script on the card, which is done when the card is entered in an ATM or electronic payment terminal.

Breakdown of fraud by transaction type

Fraud affecting domestic transactions

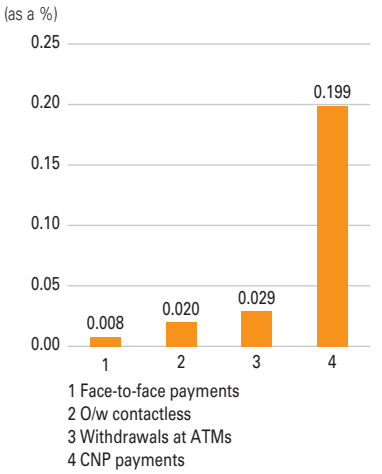
The **rate of fraud affecting face-to-face payments and unattended payment terminals (UPT)[4] moved down to 0.008% from 0.009% in 2015**. These types of payments accounted for 66.2%, i.e. almost two thirds, of the value of domestic transactions, but just 13.5% of the total fraud amount.

The **fraud rate for withdrawals edged down to 0.029% from 0.034% in 2015**. This mainly reflected the decline in the number of Automated Teller Machine (ATM) attacks (down from 640 in 2015 to 301) and POS attacks (down from 575 in 2015 to 434). These machines remain a prime target for organised fraud rings, however, and the Observatory again reminds cardholders to be on their guard and reiterates the best practices to follow when making payments to a merchant or when making withdrawals (see Appendix 1).

The fraud rate for card-not-present (CNP) payments dropped from 0.229% in 2015 to 0.199%, falling steeply for the fifth year running.

However, this was still more than twenty times higher than the rate for face-to-face payments.

C16 Comparison of fraud rates by type of transaction, domestic



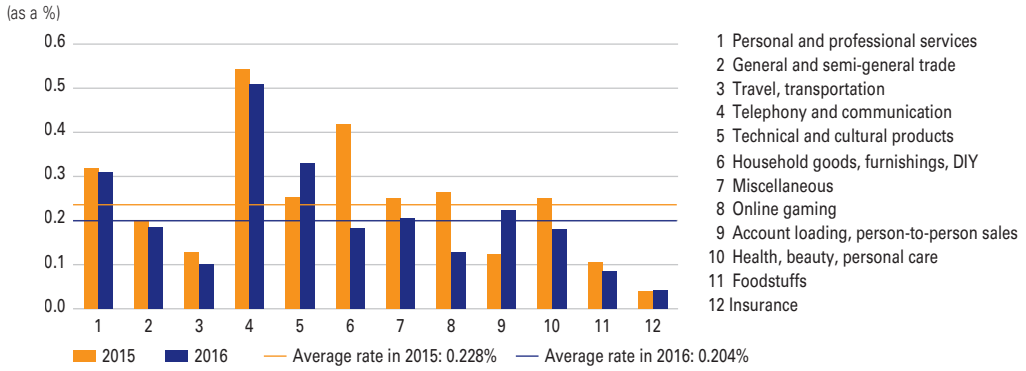
Source: Observatory for the Security of Payment Means.

4 Notably including automated fuel pumps, automatic car park pay points and toll stations.

Box 3

Domestic fraud with CNP payments, by sector of activity

Fraud rate with CNP transactions, by sector of activity – domestic



Source: Observatory for the Security of Payment Means.

The Observatory has gathered data that provides information about the distribution[1] of fraud in card-not-present (CNP) payments by sector. This data covers domestic transactions only.

The "personal and professional services", "general and semi-general trade", "travel, transportation" and "telephony and communication sectors" were the most exposed to CNP fraud, accounting for 78.7% of the total amount.

Sector	Fraud amount (in EUR millions)	Sector share of fraud
Personal and professional services	40.6	26.6%
General and semi-general trade	32.8	21.5%
Travel/transportation	23.7	15.5%
Telephony and communication	23.1	15.1%
Technical and cultural products	11.9	7.8%
Household goods, furnishings, DIY	8.2	5.4%
Miscellaneous	4.8	3.1%
Online gaming	2.6	1.7%
Account loading, person-to-person sales	2.2	1.4%
Health and beauty and personal care	1.2	0.8%
Foodstuffs	0.8	0.5%
Insurance	0.4	0.3%
Total	**152.3**	**100.0%**

Despite a slight decline in 2016, the telephony and communication sector continues to report a much higher-than-average fraud rate (see above chart). The Observatory calls on market participants in this sector in particular to step up fraud prevention measures.

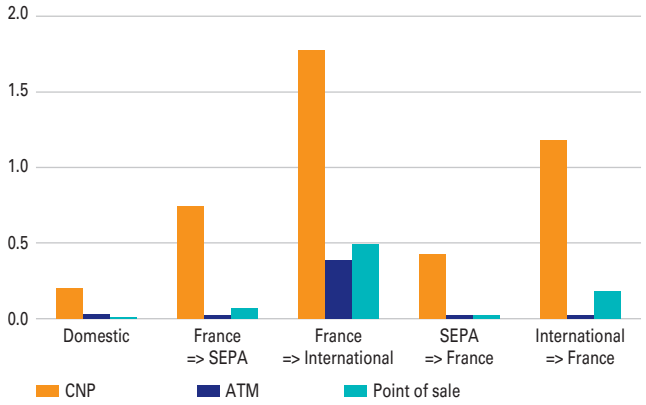
By comparing the average fraud rates for each sector of activity, we can see that, while certain sectors, such as technical and cultural products, account for a smaller share of overall fraud, they are still recording fraud rates that are well above the average.

1 See Appendix 6 for sector descriptions.

As a result, **CNP payments, which accounted for just 13% of the value of domestic transactions, made up more than 70% of the total fraud amount.** This situation justifies continued efforts to extend the use of robust customer authentication solutions by merchants and cardholders alike (see section 2–7).

C17 Fraud rate by type of transaction and geographical origin

(as a %)



Source: Observatory for the Security of Payment Means.

Fraud affecting international transactions

The total fraud amount affecting transactions carried out abroad using French cards decreased in SEPA in 2016 (from EUR 116.8 million in 2015 to EUR 113.8 million) after rising significantly over a number of years; the rate of fraud also fell in each type of transaction (face-to-face payments, CNP payments and withdrawals). One explanation for this may be the prospect of the entry into force in January 2018 of the second European Union Payment Services Directive (PSD2), which requires electronic payment transactions to be protected by strong customer authentication including, for online electronic payments in particular, elements that dynamically link the transaction to a specific amount and a specific payee.

There has also been a decrease in fraud targeting non-SEPA transactions, mainly because of improved tools to detect attempted fraud through the counterfeiting of magnetic stripes.

Breakdown by fraud type

Fraud involving the use of misappropriated card numbers for CNP payments was still the most common type of fraud in 2016 (70.1% of the total amount), accounting for a larger proportion than in 2015 (66.8%).

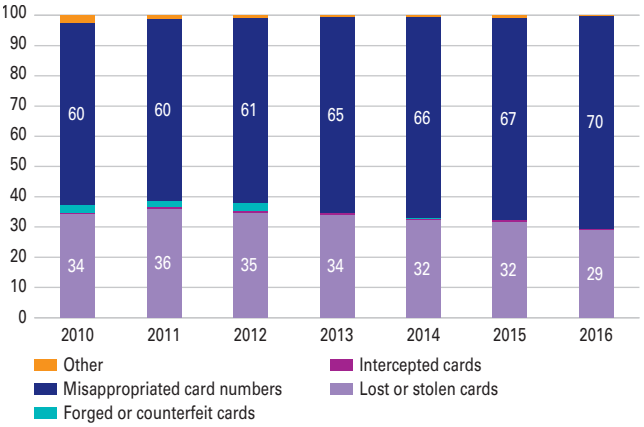
Fraud involving lost or stolen cards continued to account for close to a third of fraud in domestic transactions (29.0%). This share has been shrinking for five years (36.1% in 2011).

Counterfeit cards accounted for just 0.2% of fraudulent domestic payments. This very low level is mainly attributable to the adoption of smartcard technologies by most three-party card schemes and to enhanced security for existing EMV smartcards.[5]

5 Migration from Static Data Authentication (SDA) to Dynamic Data Authentication (DDA) technology.

C18 Distribution of card payment fraud by origin

(domestic transactions, in value, excluding withdrawals)



Source: Observatory for the Security of Payment Means.

Monitoring of strong authentication deployment

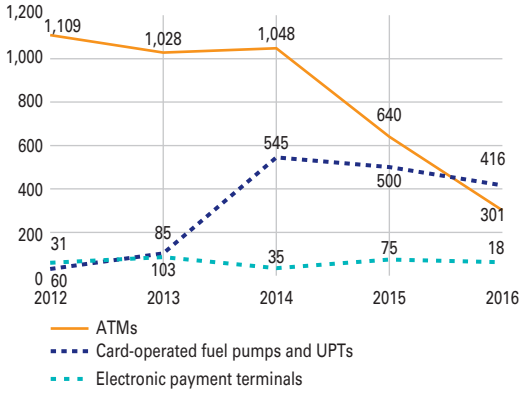
The development of online commerce has led to the increasing use of cards for CNP payments. For configuration reasons, security features embedded in the cards themselves (chip reading and PIN entry) cannot be relied upon, such that other mechanisms are needed to protect transactions. The recommendations that the Observatory for Payment Card

Box 4

Indicators provided by law enforcement agencies

Automated Teller Machine (ATM) attacks fell sharply again in 2016, with 301 cases (compared with 640 in 2015), after remaining at a higher level in previous years (approximately 1,000 a year between 2012 and 2014 and around 500 a year between 2006 and 2011, 200 in 2005 and just 80 in 2004). There were also 434 attacks on POS terminals (compared with 575 in 2015), including 354 on card-operated fuel pumps, 18 on merchant payment terminals and 62 on UPTs (Universal Payment Transfers, such as parking pay points). Despite the encouraging decline, particularly as regards ATM attacks, these figures remain high and are evidence that crime rings are constantly seeking to gather card data. This data can be used either to create counterfeit magnetic stripe cards to make foreign payments and withdrawals, chiefly in countries where EMV (Europay, MasterCard and Visa) chip technology is not widespread, or to misappropriate card numbers for use in remote payments, particularly on websites that have not yet implemented strong cardholder authentication solutions.

Attacks on ATMs and terminals



Source: Observatory for the Security of Payment Means.

Security issued in 2008, aimed at strengthening the security of CNP payments, focused on wider adoption of strong authentication solutions. Statistics monitoring implementation of these recommendations have been kept since 2011.

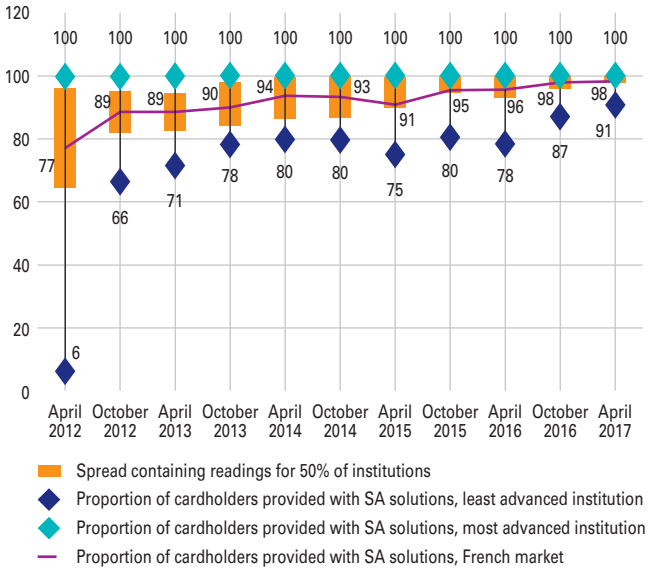
For the period November 2016 to April 2017, the monitoring by the Observatory of statistics on the deployment of authentication solutions at the main banking institutions covered a volume of 61.6 million payment cards and EUR 45.1 billion worth of transactions (of which EUR 15.7 billion protected using the 3D-Secure mechanism), making it possible to measure progress in the implementation of strong authentication both quantitatively and qualitatively.

2017 has confirmed last year's observation that cardholders have completed the switch to strong authentication, with a rate averaging 98% in 2016, covering all holders who might carry out transactions online.

Take-up of strong authentication solutions by e-merchants continues to increase and now stands at 71%, in keeping with the steady rise observed in the past three years.

C19 Distribution of cardholders provided with strong authentication (SA) solutions

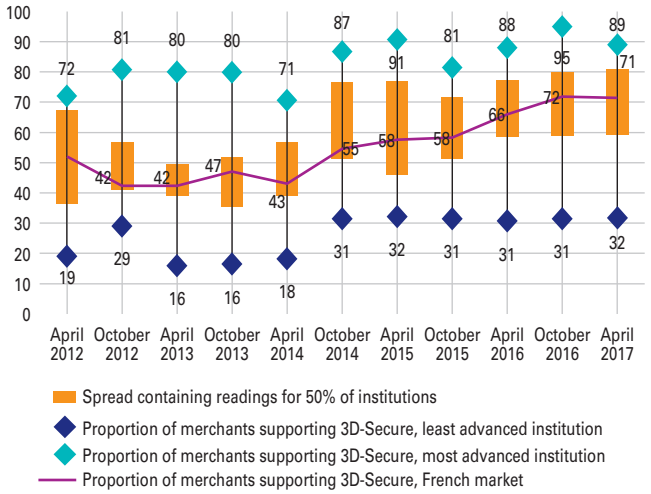
(as a %)



Source: Observatory for the Security of Payment Means.

C20 Take-up of 3D-Secure by e-merchants

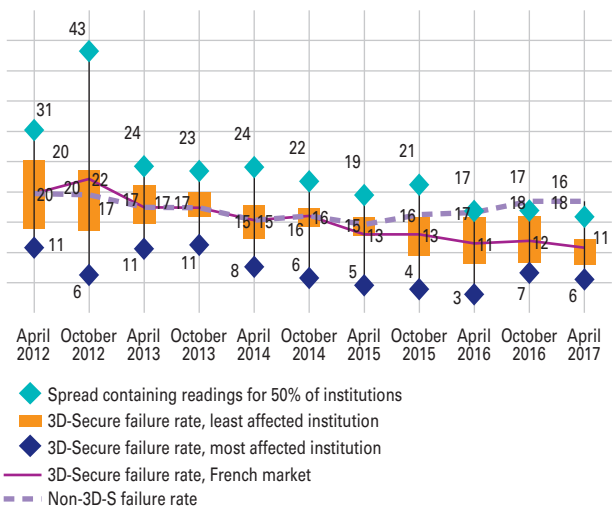
(as a %)



Source: Observatory for the Security of Payment Means.

C21 Distribution of 3D-Secure failure rates

(as a %)

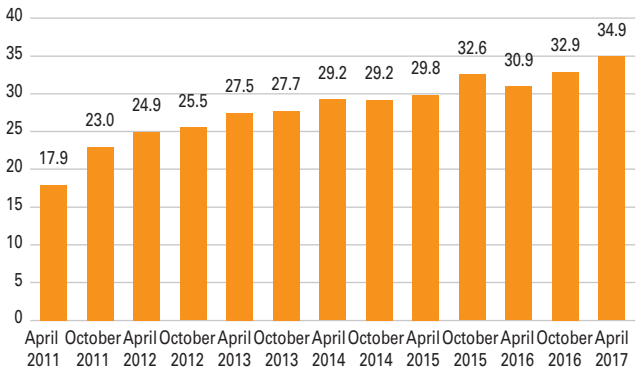


Source: Observatory for the Security of Payment Means.

The Observatory and the Banque de France encourage e-merchants to make the switch to strong payment authentication, regardless of the type of customers they cater for, before PSD2 comes into force in 2018.

C22 Proportion of online payments protected by 3D-Secure

(as a %)



Source: Observatory for the Security of Payment Means.
Note: Due to a change in scope in the collection of this statistical data, the values for financial years 2015 and 2016 have been re-estimated in relation to the data published in the Observatory for Payment Card Security's annual report for 2015.

The Observatory has observed a steady decline in the failure rate for authenticated transactions, which has fallen below 11% and remains substantially lower than the rate recorded for non-authenticated transactions, suggesting that consumers have become accustomed to such mechanisms. This is also a reflection of more effective checks on websites with strong authentication, which is forcing fraudsters to concentrate on websites that are not protected by such solutions.

In view of these trends, which are supportive of continued growth in the use of strong authentication, the share of online payments covered by 3D-Secure authentication has been rising steadily since 2011 and now represents close to 35% of the value of CNP payments.

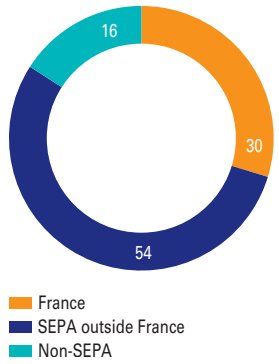
2.3 Credit transfer fraud

Overview

In 2016, fraud relating to credit transfers issued from accounts held in France amounted to EUR 86 million out of a total transaction value of close to EUR 23,700 billion. This put

C23 Amount-based breakdown of credit transfer fraud, by geographical area

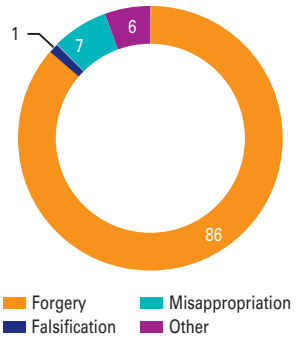
(as a %)



Source: Observatory for the Security of Payment Means.

C24 Amount-based breakdown of credit transfer fraud, by fraud typology

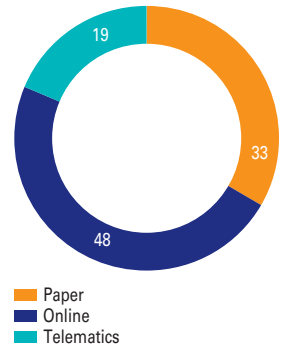
(as a %)



Source: Observatory for the Security of Payment Means.

C25 Amount-based breakdown of credit transfer fraud, by transmission channel

(as a %)



Source: Observatory for the Security of Payment Means.

the rate of fraud, based on amount, at 0.00036%, equating to one euro of fraud for every EUR 275,000 or so in credit transfers issued. Proportionally speaking, credit transfers were therefore the cashless payment method least affected by fraud, even though they were the most common form of payment in terms of transaction amount (89%). Fraudulent credit transfers averaged around EUR 15,500.

Cross-border transfers accounted for a larger proportion of fraud than domestic transfers, representing 70% of the credit transfer fraud amount, even though cross-border transactions represented just 23% of the overall issued transfer amount.

Forgeries accounted for the lion's share of fraudulent credit transfers, accounting for 86% of the total fraud amount. Misappropriation was the second most common type of fraudulent transfer (7% in value).[6]

Transfer initiation from online banking accounts (on the Internet or via a mobile phone application) was the most vulnerable channel, accounting for almost half of fraud cases (48% in value). Paper-based fraud (post, fax) made up a third, and fraud via secure telematic channels 19%.

Main instances of fraud encountered in 2016 and prevention measures

Social engineering[7] and malware and phishing attacks were the main techniques used in credit transfer fraud in 2016.

6 The typologies of credit transfer fraud are detailed in Chapter 1, paragraph 3.

7 Social engineering is defined as the art of manipulating someone to make them do something or to make them disclose confidential information.

Credit transfer fraud encountered in 2016	Prevention measures
Social engineering fraud mainly took the following forms in 2016: • **CEO fraud:** the fraudster impersonated a senior company executive to trick an employee into making an urgent, confidential credit transfer to a foreign account. To do this, the fraudster used information that he or she had gathered on the company and its executives via the Internet or directly from the company itself. • **bank account details fraud:** the fraudster impersonated a supplier, lessor or any type of creditor and falsely informed the client, tenant or debtor that there had been a change in the bank account details that they used to pay their bills, invoices or rent, misappropriating the funds for themselves. The fraudster sent the new bank details by email or by post in a properly-worded letter from the creditor. • **technical support scams:** the fraudster impersonated an IT technician (from the bank for instance) to run fake tests in order to recover log-in IDs and passwords, trigger fraudulent transfers or install malware.	**Tools that can monitor and detect unusual transactions** and can suspend the execution of a transfer that has been flagged as suspicious considering the usual activity on the account, due to the amount involved or the country to which the funds are destined. The order can then be cross-checked with the customer before execution. **Initiatives** led by banks and payment services providers to **inform and heighten awareness** among businesses.
In 2016, **cyber attacks** essentially targeted online banking websites and telematic channels, such as the EBICS (interbank communication channel through which businesses can exchange automated data files with banks) system, and were mainly perpetrated by: • **malware**: such as Trojan horses, spammers, viruses, etc., which infected a person's or a business' computer without their knowledge when they opened a fraudulent e-mail, browsed corrupted websites or connected up to infected peripherals (e.g. USB sticks). Fraudsters can use this malware to analyse and collect data traffic on a customer's computer or information system. For instance, when the customer logs into his or her online banking account, the malware can retrieve the ID and password that he or she has entered and use them to log in themselves, request that a new beneficiary be added for credit transfers or initiate a fraudulent transfer order. • **phishing**: fraudsters use this technique to gather personal and banking details by sending out unsolicited e-mails inviting recipients to click on a link that takes them to a fake website (online banking or e-commerce site), where the person is usually asked to enter their banking credentials. The tone of these emails is usually alarmist, urging the recipient to act quickly (to settle a bill in order to avoid the interruption of a service, to lift a banking suspension or to update security features). There are variants of phishing through other channels, such as "vishing" over the phone or "smishing" via SMS.	**Deployment of a strong authentication system to approve credit transfer orders** entered online. **Triggering of time delays or strong customer authentication when new transfer beneficiaries are added** on an online banking site. **Setting of maximum transfer ceilings** on online banking sites. **Provision of secure solutions to customers** to scan for malware-type infections on their terminals. **Tools that can monitor and detect** unusual transactions and can suspend the execution of a transfer that has been flagged as suspicious considering the usual activity on the account, due to the amount involved or the country to which the funds are destined. A warning message can be sent to the customer giving him or her the possibility to block the transaction, if required, during the time delay. **Initiatives** led by banks and payment services providers to **inform and heighten awareness** among consumers.

2.4 Direct debit fraud

Overview

In 2016, fraud relating to direct debit payments to be debited from accounts held in France amounted to EUR 40 million out of a total transaction amount of EUR 1,492 billion. This put the rate of fraud in value at 0.003%, i.e. one euro of fraud for every EUR 37,000 or so in direct debit instructions originated. Fraudulent direct debit instructions averaged EUR 34,000.

Domestic direct debit fraud was the most prevalent, whereas cross-border transactions within SEPA accounted for a very marginal proportion of fraud.

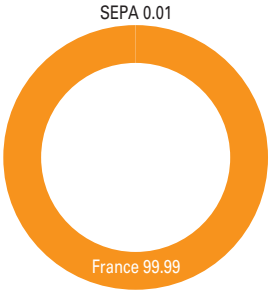
Misappropriation[8] was the most common form of direct debit fraud, making up 87% of the total fraud amount. Fraud was also attributable, but to a lesser extent (13% in value), to the origination of forged direct debit instructions.

Direct debit fraud only affected SEPA transactions in 2016. No cases of fraud were reported with French interbank payment orders (TIP – *Titres Interbancaires de Paiement*) and electronic payment orders (*télérèglement*), which were legal tender up to 1 February 2016 and fell into the direct debit payment category.

8 The typologies of direct debit fraud are detailed in Chapter 1, paragraph 4.

C26 Amount-based breakdown of direct debit fraud, by geographical area

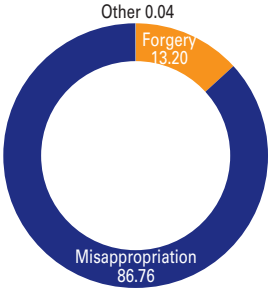
(as a %)



Source: Observatory for the Security of Payment Means.

C27 Amount-based breakdown of direct debit fraud, by fraud typology

(as a %)



Source: Observatory for the Security of Payment Means.

Direct debit fraud encountered in 2016	Prevention measures
Issuance of illegitimate direct debit instructions: a false creditor registers as the originator of a direct debit instruction with a payment services provider and originates a very large number of direct debit instructions using IBANs that he or she has acquired illegally without any authorisation.	**Tools to monitor the behaviour of creditors who originate direct debit instructions** that can detect any unusual movements based on knowledge of the customer. It is important to note that a creditor must have a SEPA Creditor Identifier (SCI) to originate direct debit instructions. Payment services providers assign SCIs after first verifying that the applicant can originate direct debit instructions. **Transmission of an alert to the customer** when a direct debit instruction is first received from a creditor to debit his or her account. **Optional services** through which a customer can set a maximum amount to be debited by creditor and by country or compile a list of creditors who are authorised to make direct debits on his or her account ("white-listed" creditors) or, alternatively, a list of creditors who are not authorised to do so ("black-listed' creditors).
Misappropriation of IBANs for subscription to services: a debtor with fraudulent intent provides the account details of a third party on the direct debit mandate, enabling him or her to obtain the services without honouring the related payments.	**Transmission of an alert to the customer** when a direct debit instruction is first received from a creditor to debit his or her account. **Optional services** through which a customer can set a maximum amount to be debited by creditor and by country or compile a list of creditors who are authorised to make direct debits on his or her account ("white-listed" creditors) or, alternatively, a list of creditors who are not authorised to do so ("black-listed' creditors).
Collusion between the creditor and the payer: a creditor with fraudulent intent originates direct debit instructions on an account that is held by an accomplice in a regular manner, gradually increasing the amounts. The payer disputes the debited amounts not long before the end of the statutory cancellation period (13 months after the direct debit is cleared), on the grounds that he or she did not sign a mandate for the direct debit. When the direct debit is rejected, the balance on the creditor's account is not sufficient to refund the disputed amounts as the funds have been transferred to an account held abroad.	**Tools to monitor the behaviour of creditors who originate direct debit instructions** that can detect any unusual movements based on knowledge of the customer. It is important to note that a creditor must have a SEPA Creditor Identifier (SCI) to originate direct debit instructions. Payment services providers assign SCIs after first verifying that the applicant can originate direct debit instructions.

2.5 Cheque fraud

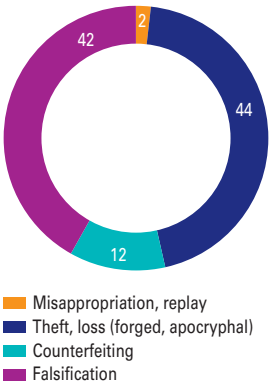
Overview

In 2016, fraud relating to cheques paid in France amounted to EUR 272 million out of a total volume of EUR 1,077 billion, i.e. a fraud rate of 0.0252%. This makes cheques the second means of payment most targeted after payment cards, even though it is only the fourth most common form of payment used. Fraudulent cheques averaged EUR 2,300.

Two categories of fraud made up, almost equally, most of the cases of fraud observed in 2016: the fraudulent use of lost or stolen cheques, which accounted for 45% of total cheque-related fraud, for an average individual cheque amount of EUR 1,300; and the falsification of validly-issued cheques, which represented 42%, with a higher average individual cheque amount of EUR 7,400. Lastly, fraud through counterfeiting and the misappropriation/replay of cheques was less common (respectively 12% and 2% of cheque-related fraud).

C28 Amount-based breakdown of cheque fraud, by fraud typology

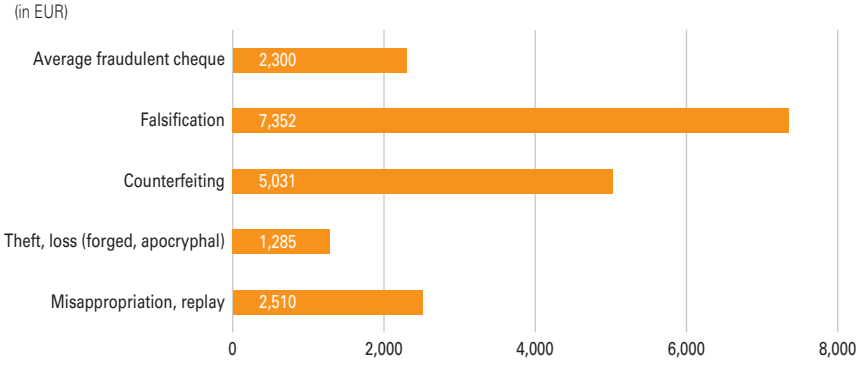
(as a %)



Source: Observatory for the Security of Payment Means.

C29 Individual fraudulent cheque amounts by fraud typology

(in EUR)



Source: Observatory for the Security of Payment Means.

Main cases of cheque fraud encountered in 2016	Prevention measures
Theft of chequebooks in the distribution circuit: a number of service providers outside the bank are involved in the distribution circuit, notably during transport and delivery to the customer. Chequebooks and blank cheque specimens can be stolen at three levels: • before delivery to the customer: at the place at which they are manufactured and/or from where they are dispatched, at transporters or deliverers to bank branches, in customers' postboxes. • on collection at bank branches, where fraudsters can use stolen or forged identity documents to collect a chequebook. **Chequebook theft when in possession of the customer** due to break-in, theft or loss.	**Rendering the shipment process traceable** for chequebooks and cheque-letters during the different transport phases. **Notifying the customer that a chequebook is available**, either for collection at the branch or for delivery by post, depending on the option selected by the customer when he or she applied for a chequebook, and indicating an expected delivery timeframe so that the customer can inform the bank if they have not received the chequebook within that timeframe. **Issuance of regular reminders from the bank that the holders of chequebooks and cheque-letters must be on their guard** and are required to report a loss or theft even if they have taken out insurance to cover such risks.
Falsification of a valid cheque intercepted by a fraudster, consisting in altering a stolen cheque by scratching, erasing or rubbing out information contained on it. The fraudster exploits the vulnerabilities of a stolen cheque by, for instance: • Scratching or rubbing out the name of the lawful beneficiary if it has been written in weak ink and replacing it with another name; • Writing the name of a new beneficiary over the legitimate beneficiary's name; • Adding something (for example a name or an acronym, a company stamp, etc.) after the name of the lawful beneficiary if blank spaces are left on the line; • Adding an amount in letters and/or figures if any blank spaces are left before or after the handwritten amount.	**Systematic examination of the cheque and of the information on it, as well as payer identity** The cheque should be physically examined to ensure that it has not been altered before acceptance, and to verify the identity of the payer, for instance, by requesting proof of identity or proof of home address. **Merchants can protect themselves against irregular cheques by consulting the national register of irregular cheques (FNCI – *Fichier national des chèques irréguliers*)** via the Banque de France's official prevention service for unpaid cheques.[1]
Counterfeiting of cheques, through the creation of a false cheque from scratch to be drawn on an existing or a fake bank.	**In-depth physical examination of the cheque and of the payer's proof of identity** (see above).
Fraud techniques derived from "**kiting**" consisting in depositing a number of fraudulent cheques to be cashed and immediately transferring the credited funds. This mainly targets accounts held by businesses and entrepreneurs, which are credited with immediate effect when cheques are deposited.	**Identification of deposit movements** that are unusual given the customer's profile, in order to suspend, if necessary, any withdrawals or transfers towards another bank that may occur immediately after a cheque is deposited.

1 *https ://www.verifiance-fnci.fr*

3 Acceptance of card payments on a remote basis

3.1 Introduction

Technological innovation is playing a key role in the development of electronic payments, particularly by bank card, as it is expanding the range of payment solutions that are available. Cards were originally designed as a payment instrument for use at points-of-sale (POS), where devices were used to read the data stored on the physical cards. Since then, technological developments mean that cards can now be used to initiate payments through other channels, for online or contactless transactions.

Alongside these developments, which have been covered many times in the work of the Observatory,[1] market participants have sought to draw on the latest technological capabilities to enrich POS payment options and provide solutions to facilitate their take-up by businesses that sell products or provide services on a remote basis (skilled tradespeople and providers of home services, professionals in private practice, taxis, etc.). This was one of the development angles to be explored as part of the national payments strategy, in response to objectives aimed at facilitating payment card acceptance and offering alternatives to payment by cheque.

As a reminder, in 2011, the Observatory started to lead a technology watch on the security of mobile phones used as payment terminals, which led it to conclude the following:

"As the situation currently stands, therefore, if mobile payment terminals are to be used in the acceptance chain, then measures must be adopted to guarantee a level of security on a par with that provided with conventional payment terminals.

In view of the rapid rise of these solutions and their immaturity on the French market, all participants should closely review the possible and future uses of these payment terminals, the majority of which do not meet current requirements [in 2011]. These reviews should factor in the increasingly international scope of the acquisition chain and the development of similar offers in Europe. In this setting, adequate security criteria are needed, as well as a legal framework suited to these methods of acceptance, which clarifies the nature of contractual relations and identifies the responsibilities of payment chain participants. The Observatory will pay close attention to developments in this area."

The findings of the Observatory's most recent technology watch on the solutions for payment acceptance on a remote basis update and complement those made in the

1 Notably in the technology watch findings contained in the 2014 annual report on contactless payments and in the 2015 annual report on payments by mobile phone and new authentication solutions for card-not-present solutions.

2011 report, taking into account the technological innovations that have emerged since then and the fact that market participants have acquired more experience in the development of well rounded, secure commercial offers.

3.2 Acceptance solutions by mobile phone or on a remote basis

Scope

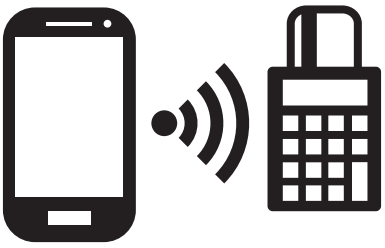
There are two main categories of card-based face-to-face payment acceptance solutions tailored to the needs of highly mobile businesses.

- Solutions on standalone terminals that can connect to the network of a telecoms operator to communicate with the payment acquirer. While these solutions are similar to the conventional payment terminals used by merchants, the difference is that they can connect to the mobile networks of telecoms operators, instead of having to go through fixed phone lines (traditional RTC-type phone lines or ADSL/fibre-optic high-speed connections).
- Solutions that involve pairing a card reader unit with a smartphone or tablet via a wired (USB or Lightning cable etc.) or wireless connection (Bluetooth, WiFi etc.), commonly grouped together under the acronym of m-POS (mobile point-of-sale). The card reader features one or more payment card interfaces that make it possible to read a magnetic stripe or exchange data with an EMV (Europay MasterCard Visa) chip in contact or contactless mode; by pairing with a connected device such as a smartphone or tablet, the card reader unit has access to a modem that enables it to communicate with the acquiring financial institution via a mobile phone network. In some cases, a receipt may be printed via a connected printer; otherwise, the receipt can be sent in digital form by SMS or email, systematically or at the customer's request.

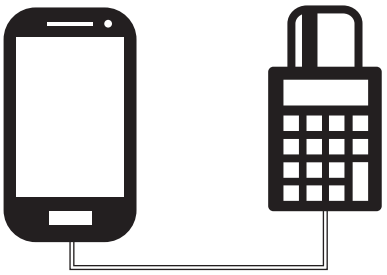
Example of a standalone terminal

Examples of m-POS solutions

With a wireless connection



With a wired connection



Solutions based on card-not-present transactions (excluded from the scope of the study)

Some businesses may opt for card-not-present (CNP) solutions as an alternative to relying on particular devices (standalone or m-POS terminals). Instead, an application or website can be used to initiate a payment, whereby the card data is entered, much the same as on an e-commerce site. Autocomplete technologies can be helpful in such cases, through photographic recognition of the card number or the reading of card data using an NFC (Near Field Communication) interface.

These software solutions are not comparable to a POS transaction, insofar as they do not rely on the physical security mechanisms embedded in the card (notably the cryptographic properties built into the chip).

This means that the security of these solutions is intrinsically lower, bearing in mind that the rate of fraud with CNP payments is almost twenty times higher than with face-to-face payments. *It is therefore advisable to avoid using them in transactions in which the cardholder and the seller are both present.*

As the Observatory has already issued recommendations regarding the security of CNP payments,[2] such mechanisms have not been covered in the latest technology watch.

3.3 Deployment of m-POS acceptance solutions

The Observatory has gathered data from the main institutions and banking groups in France on the monitoring of deployment of m-POS type mobile payment terminals. Some institutions also provided data on transactions using electronic payment terminals connected to a mobile phone network.

Solutions currently operational

The institutions surveyed currently supply units that read the chip or magnetic stripe on cards and are connected using Bluetooth wireless technology to a smartphone or tablet. Most of these solutions are scheduled to be upgraded to enable them to accept contactless payments by 2017; the development of wired connection capabilities is also being explored for some of them. The solutions marketed in France comply with all of the security standards set by the Payment Card Industry Security Standards Council (PCI SSC) and are certified by the leading interbank payment networks (CB, Visa and MasterCard).

The commercial roll-out dates for m-POS devices vary significantly, with the first solutions coming on the market in the middle of 2014, while others are still under development by certain institutions for launch in 2017.

Payments

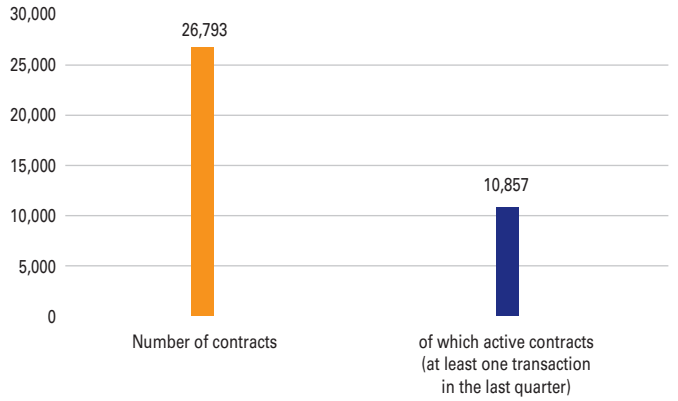
As of the middle of 2016, the main French banking institutions

2 Notably in the Observatory's 2009 annual report: the European Central Bank cited these recommendations in favour of strong customer authentication for card-not-present payments in its own recommendations published in 2013, as did the European Banking Authority in its 2014 guidelines. Systematic use of strong authentication for electronic payments is one of the key provisions of the second Payment Services Directive, which will enter into force in the European Union in January 2018.

were registering close to 450,000 transactions per quarter accepted via m-POS type devices by their business customers, representing roughly EUR 22.5 million.

Nevertheless, comparatively speaking, in mobile sales settings, this acceptance mode takes second place to transactions using more conventional electronic payment GPRS terminals. According to the data gathered by the banks that reported figures for both types of terminals, 250 GPRS payments are made for every m-POS payment.

C1 Supply of m-POS solutions in France



Source: OSMP – Data as at September 2016.

Fraud

The main French banking groups reported that they had not observed any significant payment fraud with m-POS type terminals. On a quarterly basis, the fraudulent transaction amount stands at around EUR 1,000 (for 35 fraud cases), implying a fraud rate in terms of amount of 0.004%. On the whole, this rate is lower than with face-to-face payments (which averages 0.009%).

The Observatory would like to point out that this fraud data was measured based on a low volume of m-POS transactions, and is therefore not representative of a more widespread use of such terminals. Nevertheless, the data suggests that fraudsters have yet to identify and exploit any security vulnerabilities in such solutions.

3.4 Challenges relating to the level of security of m-POS

Solutions relying on standalone terminals

The controlled environment for such solutions is very similar to the one observed for payment terminals used in stores, for which the Observatory has issued security recommendations in the past.

For the record, these terminals are essentially required to comply with the EMV standards (see the Observatory's annual report for 2009) and the Payment Card Industry – Pin Transaction Security (PCI-PTS) standards set by the PCI SSC to ensure the security of devices used to enter PINs in POS card transactions.

m-POS solutions

Any assessment of the degree of security of m-POS solutions must take into consideration all the components involved in their implementation: the smartphone or tablet used, the particular card reading unit, the centralised management server and their respective communication interfaces. While the card reading

unit and the electronic payment management server have been developed specifically for this purpose and can therefore hold the same mandatory security certifications as conventional payment terminals, smartphones and tablets cannot reasonably be subject to the same constraints, and are therefore the main source of risk with these solutions.

The security principles that apply to card payment terminals in Europe[3] are designed to protect the data stored on the card, the PIN number and PIN entry and to prevent their misappropriation. These principles require that a technical mechanism be in place to protect the PIN number from being intercepted on entry, and that this mechanism be PCI-PTS certified. *Given the technologies currently available, for this level of security to exist, there must be a physical certified keypad on the card reading unit;*[4] entry of the PIN number on the screen or keypad of a paired smartphone would pose a risk of the data being intercepted if the smartphone is infected by a malware.

At the other end of the payment mechanism, *the payment management server must be capable of protecting transaction data in a remote and secure environment*, and must therefore be required to be certified accordingly, e.g. under the Payment Card Industry – Data Security Standard (PCI-DSS).

In between these two specific components, the smartphone is the most vulnerable element of the payment mechanism; as it belongs to the merchant and is used for tasks other than the acceptance of transactions, the acquiring bank cannot be sure that its software environment is entirely secure. This potential exposure to security flaws warrants the introduction of measures to confine the role that smartphones play in the payment mechanism to that of an accounting machine and communication modem, by preventing them from accessing basic data relating to the transaction.

- The communication protocols between different physical devices must be designed to ensure point-to-point protection of the confidentiality and integrity of the transaction data. This requires an encryption system between the card reading unit and the payment management server. This will prevent the data from being intercepted and exploited by a third party as it will be encrypted on transfer via the smartphone and public telecommunications networks.

- To avoid the risk of malware manipulation, the smartphone must not have any functionality that could be used to control the inner workings of the unit other than those required for the acceptance of card payments. This is necessary to ensure that the payment mechanism can withstand attack from malware installed on a smartphone, which could try for example to:

  – generate fraudulent transactions;

  – steal data stored on the payment card;

  – alter the data of a transaction in progress;

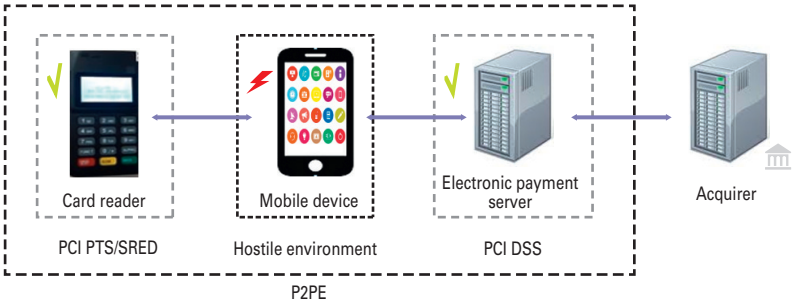
  – approve a transaction by sidestepping certain security steps such as cardholder authentication for instance.

3 Notably the European Payments Council's (EPC) SEPA Cards Framework and the Eurosystem's oversight framework for card payment schemes.

4 While other geographic areas with less stringent security requirements authorise the use of m-POS type terminals simply featuring a card reader with no keypad (where the PIN is entered on the smartphone), European card payment schemes are required to block the acquisition of payment when such basic terminals are used, as they do not comply with the oversight frameworks applicable in SEPA.

Box 1

The different components of an m-POS type solution and the related security certifications



Card reading unit: a trusted technical device that can be used to accept card payments in face-to-face transactions. Through it, data can be exchanged with the payment method, controls carried out (security, validity, risk, etc.) and transaction data communicated to the acquirer. The applicable security level requires that these units have a screen, a keypad and a mechanism to read data stored on cards. They must guarantee the confidentiality and integrity of the data (PIN, account number) and be PCI-PTS (Payment Card Industry – PIN Transaction Security) and SRED (Secure Reading Exchange of Data) certified.

Mobile device: a portable communication device (smartphone, tablet, etc.) owned by the acceptor (merchant, etc.). It hosts an application that, combined with a terminal, makes it possible to accept card payments (using a card or an NFC-compatible device such as a mobile phone). This component does not have suitable security mechanisms and assurance features (evaluation, certification, etc.) to guarantee the confidentiality and integrity of payment transaction data. It is considered as the "hostile environment" of the solution.

Electronic payment server or payment management server: hardware that manages authorisation requests and payment transaction data before transmission to the acquirer. These servers must have suitable security and assurance features to guarantee the confidentiality and integrity of payment transaction data. They must be PCI-DSS (Payment Card Industry – Data Security Standard) certified.

Security of the solution: communication protocols between the terminal and the electronic payment server must guarantee the confidentiality and integrity of the payment transaction data being transmitted on potentially open networks (Internet, GSM, etc.). Point-to-point encryption (P2PE) must be enabled.

As a protection measure, to thwart certain methods used in an attempt to recover PINs, the screen used during the transaction must be part of a secure environment; in other words, it must be embedded in the card reader unit.

Since these solutions use a payment management server, there is no need to print out a paper receipt for the acceptor, as the electronic receipts can be accessed from the stored data, lessening the risk of the data being compromised.

3.5 Conclusion and recommendations of the Observatory

The development of point-of-sale payment acceptance solutions on a remote basis should be seen as an opportunity for market participants and echoes the needs expressed in the national payments strategy.

The Observatory has observed two main emerging categories of solutions to meet these needs: standalone payment terminals similar to those used by sedentary merchants, with mobile phone network connectivity (GPRS, 3G or 4G) capabilities; and m-POS devices in which a card reading unit is paired with a mobile device (a smartphone or tablet), which essentially serves as a modem.

In an effort to ensure that the emergence of these new solutions, which are already being supplied by certain acquirers, does not jeopardise the high-level security features of conventional payment terminals, the Observatory stresses the importance of putting suitable security measures in place.

- For standalone terminals: ensuring compliance with the security principles that the Observatory has defined for face-to-face payment terminals, and notably with EMV and PCI-PTS standards, to enable payment mechanisms to withstand attempted fraud.

- For solutions along the lines of m-POS: taking steps to ensure an equivalent security environment to that in place for standalone terminals. This means that both the card reading unit and PIN entry system must be subject to the same requirements as conventional terminals (EMV, PCI-PTS and SRED [Secure Reading Exchange of Data]); moreover, the communication protocols between the components of the solution must make it possible to keep access by the mobile device to the transaction data to a minimum. On this second point, the framework must notably endeavour to safeguard the point-to-point security and integrity of the data using encryption methods, taking into consideration the risks incurred when a component that is not exclusively used for payment transactions – the mobile device that serves as a modem – is present in the transaction chain.

With this in mind, the Observatory urges market participants to apply the approval procedures that have been put in place for such solutions and ensure compliance with these requirements.

The Observatory reminds cardholders that they must be on their guard when making a payment on a mobile terminal. In light of the multiplication of payment acceptance solutions, the Observatory invites cardholders to exercise caution when they are requested to make a payment on an unusual terminal.

- In France and the rest of Europe, terminals that read only the

magnetic stripe are only tolerated if a special derogation has been issued and in specific payment environments. If the payment card has an EMV chip, the only payments authorised are those that entail reading the chip (in which case the card must be inserted in the terminal when the PIN is entered) and those in contactless mode (where the card is placed on the terminal's NFC reader).

- Cardholders are advised to request the receipt that certifies payment, and to make sure that they have received it (notably when the receipt is sent electronically by SMS or email) and to retain it as proof in order to later verify that the payment has been correctly debited from the cardholder's account.

Lastly, the Observatory emphasises that m-POS payment is an innovative industry and that it will therefore be closely monitoring the emergence of new types of solutions, which might lead it to update these recommendations.

A1 Security tips for the use of means of payment

Fraudsters are always trying to find new ways to bypass ever more stringent security mechanisms. This is why the users of cashless payment instruments (cards, cheques, credit transfers and direct debits) must be increasingly on their guard and make sure they keep abreast of the protection mechanisms in place and recommended secure payment habits.

A number of types of fraud targeting cashless payment means have been identified:

- issuance of false payment orders, either involving the theft or counterfeiting of a physical payment instrument, or through the misappropriation by a third party of data or banking credentials;
- misappropriation or falsification of a valid payment order, through the duplication of a payment order issued by the lawful holder of the payment instrument or the modification of information contained on it (amount, name of the beneficiary or payer, etc.);
- fraud involving the use or wrongful repudiation by the lawful holder of a payment method, whereby a validly issued payment order is disputed without grounds, resulting in the cancellation of the receipt of funds.

These different forms of fraud do not all apply in the same manner to the various payment instruments and vary depending on the payment initiation channel used (face-to-face payments, card-not-present payments on the Internet, online banking, etc.).

The security of your payment instruments hinges directly on your own safety habits.

Please follow these basic security recommendations to protect your transactions.

Be responsible

- Your physical payment instruments, such as your card or chequebook, are strictly personal: never lend them to anyone, even your closest friends and relatives. Check regularly that you still have them and keep them in a safe place, preferably separate from your ID documents.

- If the payment instrument comes with a personal identifier (PIN for a card, password for a mobile phone payment, etc.), keep it secret and do not disclose it to anyone. Memorise it. Avoid writing it down and, if you do, never keep it with your payment instrument or in such a way that it could be linked to it.

Do not disclose your passwords, personal identifiers and log-in IDs to administrative or judicial authorities or to your bank, especially by phone or email. These bodies are never likely to request such information.

- When entering your PIN or secret password, make sure that nobody can see it. Do not hesitate to shield the keypad on the terminal, ATM or telephone with your other hand.

- Read your statements carefully and regularly.

- Regularly consult the security advice provided on your bank's website and make sure that your bank has your contact details should it need to get in touch with you quickly to verify any suspicious transactions on your account. Should your bank contact you by phone or email regarding such transactions, remember that you should not disclose your passwords or personal identifiers to the person contacting you.

- Never agree to pay a seller or lessor of goods who you do not know by money transfer before the goods have been made available or delivered to you; they may be fraudsters who will delete all means of contact (email address, social network account, etc.) once they have received the payment.

Be aware

When making payments to businesses or individuals

- Watch how the merchant uses your card. Do not let your card out of your sight.

- Make sure to check the amount displayed on the terminal before validating the transaction.

- When a cheque is automatically filled in by a merchant, pay careful attention to the information that they have entered before you sign the cheque, particularly the amount.

- Some precautions when filling out a cheque help reduce the risk of fraud: do not cross out or write over anything, fill in the name of the beneficiary and the amount to be paid in figures and in letters without leaving any gaps and then draw a line through any unused space. The place of payment and the date must be entered at the same time as the other information. Your signature must not encroach on the line of numbers at the bottom of the check. Under no circumstances should only your signature appear on a cheque without the amount and beneficiary, which should be filled in before your signature.

When withdrawing cash from ATMs

- Check the appearance of the ATM. Try not to use machines that you think may have been tampered with.
- Only follow the instructions displayed on the ATM screen: do not let strangers distract you, even if they are offering their help.
- If the ATM swallows your card and you cannot retrieve it immediately from the branch, report it right away.

When making Internet payments

- Do not store your bank details on your computer (card number, account number, IBAN and SWIFT codes, etc.), never send them in an ordinary e-mail message and verify the security features of the merchant's website when you are required to enter them (padlock in the lower corner of the window, URL beginning with "https", etc.).
- Make sure you are dealing with a reputable company, that you are on the right site and read the legal notices and general terms of sale carefully.
- Do not reply to an email, SMS, phone call or any other invitation that you find suspicious. It is particularly important never to click on a link in a message that refers to a banking website.
- Protect your computer by running the security updates offered by software editors (usually free) and by installing antivirus software and a firewall.
- Regularly change your passwords and do not select the 'save' option to memorise them for future use (should your identifiers and bank details be intercepted, you could be exposed to fraud across all of your means of payment).

- Do not use the same password for your means of payment, your online bank account and any other websites on which you have an account.

When receiving a payment or a payment order

- When you receive a direct debit mandate, check that the information on the creditor (name/company name, address) corresponds to the information contained in your contract with it. If your bank has compiled a list of creditors authorised to make direct debits from your account (white list), make sure you keep the list up-to-date.

- Should you receive a remote payment from a payer you do not know personally (e.g. as part of an online sale transaction), verify that the information provided is correct (name, address, payer identifier, etc.) before agreeing to the transaction. If in any doubt, check with the payer's bank that the payment means is valid and that the payer can be trusted.

- Should you receive a banker's draft (e.g. if you sell your car), contact the issuing bank by finding its address and phone number yourself (do not rely on the information provided on the banker's draft) to confirm the validity of the document before finalising the transaction.

- Verify that received cheques contain all the mandatory information, notably the signature of the issuer, the name of the paying bank, and the date and place of issue of the cheques. Check also that the information is consistent (beneficiary, amount, cheque number on the MICR line) and that nothing has been crossed out or written over, which could be an indication of fraud.

When travelling to other countries

- Find out what precautions you need to take and contact the bank that has issued your card before leaving to find out about any card protection systems that may be implemented.

- Remember to take the international telephone numbers with you for reporting lost or stolen means of payment.

Know what to do

If your payment instrument or banking credentials have been lost or stolen

- Report it immediately by calling the number provided by your bank or the issuer of the payment instrument. Do this for all lost or stolen cards, chequebooks or mobile devices with payment applications. Similarly, inform your bank if you have communicated your bank details (account number, IBAN and SWIFT codes, etc.) to a dubious third party.

- In the event of theft, file a complaint with the police as soon as possible.

If you report a lost or stolen payment instrument promptly, you will be covered by provisions limiting your liability to the first EUR 150 of fraudulent payments. If you fail to act promptly, you could be liable for all fraudulent payments made before you report it missing. Once you have reported it lost or stolen, you can no longer be held liable.

If you notice any unusual transactions involving your means of payment

- Contact your bank promptly to verify the validity of any unidentified payment transactions or ones that you are uncertain about. Be sure in particular to contact your bank should you receive information by phone, email or SMS confirming or requesting your approval of payment transactions that you have not initiated.

If you see any unusual transactions on your statement, and your means of payment are still in your possession

Report this promptly so that you are protected against any new fraudulent attempts using misappropriated payment data.

If you file a claim with the bank that holds your account within 13 months of the debit date of the contested transaction (time limit set by law), the disputed amounts must be immediately refunded to you at no charge. If you do this, you will not be liable. Nevertheless, you will be held liable in the event of gross negligence on your part (e.g. you let someone see your card number and/or PIN and this person has used your card without telling you) or if you deliberately fail to comply with your contractual security obligations (e.g. you have been

careless enough to tell someone the card number and/or the PIN and this person has used your card without telling you). Note that if the payment instrument was misappropriated in a non-European country, the time limit for submitting a claim is 70 days from the debit date of the contested transaction. The issuer of the payment instrument may extend this limit, although it cannot exceed 120 days.

Naturally, in the event of fraudulent activity on your part, the protective mechanisms provided for under the law will not apply and you will be liable for all amounts debited before and after reporting the payment instrument lost or stolen, as well as any other costs resulting from these transactions (e.g. if there are insufficient funds in the account).

A2 Protection of the payer in the event of unauthorised payments

The Order that transposed the Directive on Payment Services in the Internal Market, which came into force on 1 November 2009, amended the rules concerning the liability of the payer in the event of an unauthorised payment transaction.

The burden of proof lies with the payment services provider. Accordingly, if a customer denies having authorised a transaction, the payment services provider has to prove that the transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency. The law strictly governs the arrangements concerning forms of proof, stating that the use of a payment instrument recorded by the payment services provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer failed with gross negligence to fulfil one or more of his or her obligations in this regard.

However, to determine the extent of the payer's liability, it is necessary to identify whether the disputed payment transaction was carried out within the territory of the French Republic or within the European Economic Area (EEA).

Domestic and intra-Community transactions

These protective measures cover:

- payment transactions made in euros or CFP francs within the territory of the French Republic;[1]
- intra-Community transactions in which the beneficiary and the payer respectively call on a payment services provider that is located:
  - in metropolitan France, in the French overseas departments, Saint Martin or Saint Barthelemy on the one hand;
  - and, in another State party to the EEA agreement[2] on the other,

and carried out in euros or in the domestic currency of one of those States.

1 The order to extend the provisions of the transposition order to New Caledonia, French Polynesia and the Wallis and Futuna Islands came into force on 8 July 2010.

2 The European Economic Area is made up of the European Union, Liechtenstein, Norway and Iceland.

As regards unauthorised transactions, i.e. in practice cases of loss, theft or misappropriation (including by remote fraudulent use or counterfeiting) of the payment instrument, the user of the payment service must inform the service provider that he or she did not authorise the payment transaction within 13 months of the debit date. The service provider is then required to immediately refund the payer the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. Further financial compensation may also be paid. Although the maximum time for disputing transactions has been extended to 13 months, the holder of the payment instrument should notify his or her payment services provider without undue delay on becoming aware of the loss, theft or misappropriation of the payment instrument or of its unauthorised use.

A derogation from these refund rules is allowed for payment transactions carried out using personalised security features, such as the entry of a secret code or a one-time password to initiate a transfer online.

Before submitting notification to block the payment instrument

Before reporting the payment instrument lost or stolen, the payer could be liable for losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment card, if the transaction is carried out using the instrument's personalised security features. By contrast, the payer will not be liable if the personalised security features are not used to conduct the transaction.

The payer is not liable if the unauthorised payment transaction was carried out through the misappropriation of the payment instrument or data related to it without his or her knowledge. Similarly, the payer is not liable in the event that the payment instrument is counterfeited, if the card was in his or her possession when the unauthorised transaction was carried out.

However, the payer shall bear all the losses relating to any unauthorised payment transactions arising from fraudulent actions on his or her part, or from a failure to fulfil the terms of safety, use or blockage agreed with the payment services provider, whether with intent or through gross negligence.

Lastly, if the payment services provider does not provide appropriate means to report lost, stolen or misappropriated cards, the payer shall not be liable for any of the financial consequences, except where he or she has acted fraudulently.

After submitting notification to block the payment instrument

The payer shall not bear any financial consequences resulting from the use of a payment instrument or misappropriation of the related data after reporting the loss, theft or misappropriation to his or her payment services provider.

Once again, if the payer acts fraudulently, he or she forfeits all protection and becomes liable for any losses associated with the use of the payment instrument.

Notification to block the payment instrument may be made to the payment services provider or to the entity indicated by the services provider to the customer, as applicable, in the payment service agreement or the deposit account agreement.

Once the user has notified the payment services provider that his or her payment instrument has been lost, stolen, misappropriated or counterfeited, the payment service provider shall supply the user, on request and for 18 months after notification, with the means to prove that he or she made such notification.

Transactions outside Europe

The Payment Services Directive applies only to intra-Community payment transactions. However, French legislation in place prior to adoption of the directive protected cardholders, irrespective of the location of the beneficiary of the unauthorised transaction. It was decided to provide customers with the same protection as they enjoyed before. To this end, the rules for domestic and intra-Community transactions apply with some adjustments.

The payment transactions concerned by these adjustments include transactions made with a payment card whose issuer is located in metropolitan France, in the French overseas departments,[3] Saint Martin or Saint Barthelemy, on behalf of a beneficiary whose payment services provider is located in a non-European State,[4] no matter what currency the transaction was in. Also concerned are transactions carried out with a card whose issuer is located in Saint Pierre and Miquelon, New Caledonia, French Polynesia or Wallis and Futuna, on behalf of a beneficiary whose service provider is located in a State other than the French Republic, no matter what currency was used.

3 Including Mayotte since 31 March 2011.

4 That is not party to the EEA agreement.

In such cases, the maximum amount of EUR 150 applies to unauthorised transactions performed using lost or stolen cards, even if the transaction was carried out without using the card's personalised security features.

The maximum time limit for disputing transactions has been changed to 70 days and may be extended by agreement to 120 days. All unauthorised transactions must be refunded immediately.

A3 Missions and organisational structure of the Observatory

Articles R141-1, R141-2 and R142-22 to R142-27 of the *Code monétaire et financier* (French *Monetary and Financial Code*) set out the missions, composition and operating procedures of the Observatory for the Security of Payment Means.

Scope

Pursuant to Article 65 of the Law of 9 December 2016 (No. 2016-1691) and in accordance with the national means of payment strategy, Article L141-4 of the French *Monetary and Financial Code* has been amended by extending the missions of the Observatory for Payment Card Security to all cashless means of payment. Henceforth, in addition to cards issued by payment service providers or equivalent institutions, all other cashless means of payment now fall within the scope of the missions of the Observatory for the Security of Payment Means.

In accordance with Article L311-3 of the French *Monetary and Financial Code*, a means of payment is understood as any instrument that allows any person to transfer funds, regardless of the form that such instrument takes or the technical process used. The means of payment covered by the Observatory are as follows:

Credit transfers, carried out by the payment service provider that holds the payer's payment account, consist in crediting a beneficiary's payment account with a payment transaction or a series of payment transactions from a payer's payment account, pursuant to instructions from the payer.

Direct debits are used to debit a payer's payment account, where a payment transaction is initiated by the beneficiary on the basis of the payer's consent given to the beneficiary, to the beneficiary's payment service provider or to the payer's own payment service provider.

Payment cards are payment instruments that enable the holder to withdraw or transfer funds. There are different types of cards.

- Debit cards are cards that draw on a payment account and enable their holders to make withdrawals or payments that are debited in accordance with a timeframe set out in the card issuance contract.

- Credit cards are backed by a credit line that carries an interest rate and a maximum limit negotiated with the customer. These serve to make payments and/or cash withdrawals. They enable their holders to pay the issuer at the end of a certain period. The payment acceptor is paid directly by the issuer without any particular credit-related delay.

- Commercial cards are issued to businesses, public bodies or natural persons engaged in an independent activity. Their use is restricted to expenses incurred in a professional capacity, and any payments made with them are directly billed to the account of the business, public body or natural person engaged in an independent activity.

- Prepaid cards can store electronic money.

Electronic money is a monetary value that is stored in electronic form, including magnetically, representing a claim on the issuer. It is issued (by credit institutions or electronic money institutions) against the remittance of funds for the purpose of performing payment transactions. It can be accepted by a natural person or legal entity other than the electronic money issuer.

Cheques are documents whereby a person, the drawer, instructs a credit institution, the drawee, to pay on demand (at sight) a certain sum to the drawer or to a third party, the beneficiary.

Commercial paper is a marketable security which state that the bearer holds a claim for payment of a sum of money and serve for that payment. Commercial paper includes bills of exchange and promissory notes.

Responsibilities

Pursuant to Articles L141-4 and R141-1 of the French *Monetary and Financial Code*, the Observatory for the Security of Payment Means has a threefold responsibility.

- It monitors the implementation of measures adopted by issuers, merchants and businesses to strengthen the security of payment means.

- It compiles statistics on fraud. These statistics are compiled from the information reported by the issuers of payment means to the Observatory's secretariat. The Observatory issues recommendations aimed at harmonising procedures for establishing fraud statistics for the various cashless payment means.

- It maintains a technology watch on cashless payment means, with a view to proposing ways to tackle threats to the security of payment instruments. To this end, it collects all the available information that is liable to reinforce the security of payment means and puts it at the disposal of its members. It organises the exchange of information between its members while respecting confidentiality where necessary.

In accordance with Article R141-2 of the French *Monetary and Financial Code*, the Minister of the Economy and Finance may request the Observatory's opinion on various issues, setting a time limit for its response. These opinions may be published by the Minister.

Composition

The composition of the Observatory is set out in Article R142-22 of the French *Monetary and Financial Code*. Accordingly, the Observatory is made up of:

- a Deputy and a Senator;
- eight general government representatives;
- the Governor of the Banque de France or his representative;
- the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (French prudential supervision and resolution authority – ACPR) or his representative;
- a representative of the *Commission nationale de l'informatique et des libertés* (French data protection body – CNIL);
- fourteen representatives of issuers of payment means and operators of payment systems;
- five representatives of the Consumer Board of the French National Consumers' Council;
- eight representatives of professional organisations of merchants and businesses, notably from the retail sector, the supermarket sector and CNP sales and e-commerce channels;
- two qualified prominent persons chosen for their expertise.

The names of the members of the Observatory are listed in Appendix 4 to this report.

The members of the Observatory, other than the members of Parliament, those representing the State, the Governor of the Banque de France and the Secretary General of the ACPR, are appointed for a three-year term. Their appointments shall be renewable.

The President is chosen from the Observatory members by the Minister of the Economy and Finance. He or she has a three-year term of office, which may be renewed. François Villeroy de Galhau, the Governor of the Banque de France, is the current President of the Observatory.

Operating procedures

In accordance with Article R142-23 et seq. of the French *Monetary and Financial Code*, the Observatory meets at least twice a year at the invitation of its President. The meetings are held in camera. Measures proposed within the Observatory are adopted by absolute majority. Each member has one vote; the President has the casting vote in the event of a tie. The Observatory has adopted internal rules of procedure setting out its working conditions.

The secretariat of the Observatory, which is provided by the Banque de France, is responsible for organising and following up on meetings, centralising the information required for the establishment of payment means fraud statistics, and collecting and making available to members the information required to monitor the security measures adopted and maintain the technology watch in the field of payment means. The secretariat also drafts the Observatory's annual report that is submitted every year to the Minister of the Economy and Finance and transmitted to Parliament.

The Observatory may constitute working or study groups, notably when the Minister of the Economy and Finance requests its opinion. The Observatory defines the mandate and composition of these groups by absolute majority. The groups report on their work at each meeting of the Observatory. They may hear all persons who could provide them with information that is useful to their mandates. The Observatory has set up two standing working groups: the first is responsible for harmonising and establishing fraud statistics and the second for ensuring a payment means technology watch.

Given the sensitivity of the data reported to them, the members of the Observatory and its secretariat are bound by professional secrecy under Article R142-25 of the French *Monetary and Financial Code* and must therefore maintain the confidentiality of the information that is transmitted to them in the course of their work. To this end, the Observatory's rules of procedure stipulate the members' obligation to make a commitment to the President to ensure the complete confidentiality of working documents.

A4 Members of the Observatory

Pursuant to Article R142-22 of the *Code monétaire et financier* (French *Monetary and Financial Code*), the members of the Observatory, other than the members of Parliament, those representing the State, the Governor of the Banque de France and the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (the French prudential supervision and resolution authority – ACPR), are appointed for a three-year term by order of the Minister of the Economy and Finance. The most recent appointment order was issued on 16 June 2017.

President
François Villeroy de Galhau
Governor of the Banque de France

Members of Parliament

Senate
National Assembly

Representative of the General Secretariat of the ACPR

Édouard Fernandez-Bollo
Secretary General

Representatives of general government

Nominated on proposition by the General Secretariat for Defence and National Security:

- The Director General of the National Agency for the Security of Information Systems or his/her representative:
  Guillaume Poupard

Nominated on proposition by the Minister of the Economy and Finance:

- The Senior Official for Defence and Security or his/her representative:
  Christian Dufour

- The Head of the Treasury or his/her representative:
  Odile Renaud-Basso
  Isabelle Bui

- The Director General for Enterprises or his/her representative:
  Pascal Faure
  Loïc Duflot

- The Director General for Competition, Consumer Affairs and the Punishment of Fraud Offences or his/her representative:
  Éric Maurus

Nominated on proposition by
the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  Nicolas Barret

Nominated on proposition by
the Minister of the Interior:

- The Head of the Central Office for the Fight against Crimes Linked to Information and Communication Technologies or his/her representative:
  François-Xavier Masson

- The Director General of the *Gendarmerie nationale* or his/her representative:
  Nicolas Duvinage

Nominated on proposition by the *Commission nationale de l'Informatique et des Libertés* (CNIL)

- The Head of Economic Affairs
  Clémence Scottez

Representatives of the issuers of payment means and the operators of payment systems

Andrée Bertrand
Bureau member
Association française des établissements de paiement et de monnaie électronique (Afepame)

Nathalie Chabert
Head of Communications and Institutional Relations
Association française du multimédia mobile (AFMM)

Corinne Denaeyer
In charge of Market Research
Association française des sociétés financières (ASF)

Jean-Marie Dragon
Head of electronic banking and innovative payments
BNP Paribas (BNPP)

Olivier Durand
Director in charge of interbank matters
Office de coordination bancaire et financière (OCBF)

Caroline Gaye
Country Manager
American Express France (AMEX)

Solveig Honore-Hatton
Vice-President, Business Development
MasterCard France

Philippe Laulanie
Executive Director
Groupement des cartes bancaires (GCB)

Philippe Marquetty
Global Head of Payments
& Cash Management Products
Société Générale

Gérard Nebouy
Executive Director
Visa Europe France

Jérôme Raguenes
Head of Digital Solutions and Payment
Fédération bancaire française (FBF)

Caroline Sellier
Head of Risk Management and Fraud Prevention
Natixis Payment Solutions

Jean-Marie Vallée
CEO (Chief Executive Officer)
STET

Narinda You
Head of Strategy and Market Relations
Crédit Agricole

Representatives of the Consumer Board of the National Consumers' Council

Mélissa Howard
Lawyer
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane Lenain
Lawyer
Union nationale des associations familiales (UNAF)

Robin Mathieu
Project leader Banking/Insurance
UFC – Que choisir

Hervé Mondange
Lawyer
Association Force ouvrière consommateurs (AFOC)

Ariane Pommery
Lawyer
Association de défense, d'éducation et d'information du consommateur (ADEIC)

Corporate representatives

Bernard Cohen-Hadad
President of the business financing commission
Confédération des petites et moyennes entreprises (CPME)

Delphine Kosser-Glories
Head of the Department of Economic Affairs
Mouvement des entreprises de France (MEDEF)

Christophe Lesobre
President of the electronic banking and payment means commission
Association française des trésoriers d'entreprises (AFTE)

Representatives of merchants' professional organisations

Jean-Michel Chanavas
General Delegate
Mercatel

Vincent Depriester
Member of the finance group
Fédération du commerce et de la distribution (FCD)

Philippe Joguet
Correspondent on financial issues
Conseil du commerce de France (CdCF)

Marc Lolivier
General Delegate
Fédération du e-commerce *et de la vente à distance* (FEVAD)

Philippe Solignac
Vice-President
Chambre de commerce et d'industrie de Paris – Île de France (CCIP)

Persons chosen for their expertise

Claude France
Chief Operations Officer
France Worldline

David Naccache
Professor
École normale supérieure (ENS)

A5 Statistics

Overview

T1 Payment means used in France in 2016

(changes in %)

Cashless transactions	Number of transactions (in EUR millions)		Transaction amounts (in EUR billions)		Average amounts in EUR
	2016	Change 2016/2015	2016	Change 2016/2015	
Card payments(*)	11,134	+10	499	+8	45
Direct debits	3,963	+2	1,492	+3	377
Credit transfers	3,753	+4	23,697	+3	6,314
Cheques	2,137	-8	1,077	-8	504
Truncated BOE and PN	82	-3	266	-9	3,236
E-money	38	+5	1	+47	16
Total payments	**21,107**	**+5**	**27,032**	**+3**	**1,281**
Card withdrawals(*)	1,491	-2	129	+1	87
Total transactions	**22,598**	**+5**	**27,161**	**+3**	**1,202**

(*) cards issued in France only.

T2 Breakdown of payment means fraud in value and volume in 2016

(share in %)

	Value		Volume		Average amount in EUR
	2016 (in EUR)	Share of value	2016 (in units)	Share of volume	
Card payments(*)	350,694,173	44	4,675,093	93	75
Cheques	271,706,352	34	118,299	2	2,296
Credit transfers	86,284,101	11	5,585	0	12,226
Direct debits	39,935,882	5	1,176	0	33,959
Truncated BOE and PN	1,018,149	0	4	0	254,537
Total payments	**749,638,657**	**94**	**4,800,157**	**96**	**156**
Card withdrawals(*)	48,384,911	6	201,193	4	240
Total transactions	**798,023,568**	**100**	**5,001,350**	**100**	**159**

(*) cards issued in France only.

Fraud statistics for payment cards

The Observatory gathers payment card fraud data from:

- the 120 members of the "CB" Bank Card Consortium, through the consortium, MasterCard and Visa Europe France;
- nine three-party card issuers: American Express, Oney Bank, BNP Paribas Personal Finance (Aurore, Cetelem and Cofinoga), Crédit Agricole Consumer Finance (Finaref and Sofinco), Cofidis, Diners Club, Franfinance, JCB and UnionPay.

In 2016, there were 84.3 million cards in circulation, of which:

- 73.4 million four-party cards ("CB", MasterCard, Visa);
- 10.9 million three-party cards.

Around 1,138,000 cards[1] were reported lost or stolen in 2016.

1 Cards reported lost or stolen and for which at least one fraudulent transaction was recorded.

T3 The payment card market in France – Issuance

(volume in millions; value in EUR billions)

	French issuer, French acquirer		French issuer, Foreign SEPA acquirer		French issuer, Foreign non-SEPA acquirer	
	Volume	Value	Volume	Value	Volume	Value
Four-party cards						
Face-to-face payments and UPT	9,528.76	381.65	224.79	12.02	46.11	3.84
CNP payments excluding internet	32.00	2.88	25.30	1.34	1.65	0.29
CNP payments online	918.02	67.92	198.30	11.76	19.39	1.29
Withdrawals	1,432.56	122.07	35.54	3.95	20.34	3.03
Total	**11,911.34**	**574.53**	**483.94**	**29.07**	**87.49**	**8.45**
Three-party cards						
Face-to-face payments and UPT	80.02	7.41	3.79	0.68	4.98	0.81
CNP payments excluding internet	29.94	4.52	6.09	0.38	0.55	0.13
CNP payments online	10.15	1.37	3.41	0.60	0.89	0.16
Withdrawals	2.68	0.24	0.00	0.00	0.00	0.00
Total	**122.78**	**13.53**	**13.30**	**1.66**	**6.42**	**1.09**
Grand total	**12,034.13**	**588.06**	**497.23**	**30.74**	**93.91**	**9.55**

Source: Observatory for the Security of Payment Means.

T4 The payment card market in France – Acceptance

(volume in millions; value in EUR billions)

	French issuer, French acquirer		Foreign SEPA issuer French acquirer		Foreign non-SEPA issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Four-party cards						
Face-to-face payments and UPT	9,528.76	381.65	239.96	14.20	61.86	6.39
CNP payments excluding internet	32.00	2.88	9.66	1.55	3.89	1.02
CNP payments online	918.02	67.92	64.74	6.94	17.71	2.95
Withdrawals	1,432.56	122.07	23.33	3.81	6.92	1.68
Total	**11,911.34**	**574.53**	**337.69**	**26.50**	**90.38**	**12.04**
Three-party cards						
Face-to-face payments and UPT	80.02	7.41	6.09	0.89	8.13	3.32
CNP payments excluding internet	29.94	4.52	3.23	0.70	1.16	0.59
CNP payments online	10.15	1.37	2.01	0.26	0.77	0.17
Withdrawals	2.68	0.24	0.00	0.00	0.68	0.29
Total	**122.78**	**13.53**	**11.34**	**1.85**	**10.74**	**4.38**
Grand total	**12,034.13**	**588.06**	**349.03**	**28.34**	**101.12**	**16.42**

Source: Observatory for the Security of Payment Means.

T5 Breakdown of fraud by card type

(fraud amount in EUR millions)

	Fraud rate									
	2012		2013		2014		2015		2016	
Four-party cards	0.080%	(434.4)	0.080%	(455.8)	0.080%	(486.4)	0.083%	(507.2)	0.077%	(504.0)
Three-party cards	0.076%	(16.3)	0.065%	(14.0)	0.062%	(14.2)	0.068%	(15.5)	0.060%	(13.5)
Total	**0.080%**	**(450.7)**	**0.080%**	**(469.9)**	**0.080%**	**(500.6)**	**0.082%**	**(522.7)**	**0.077%**	**(517.5)**

Source: Observatory for the Security of Payment Means.

T6 Geographical breakdown of fraud

(fraud amount in EUR millions)

	Fraud rate									
	2012		2013		2014		2015		2016	
Domestic transactions	0.045%	(226.4)	0.046%	(238.6)	0.043%	(234.6)	0.040%	(225.0)	0.037%	(217.2)
International transactions	0.380%	(224.3)	0.350%	(231.3)	0.316%	(266.0)	0.372%	(297.9)	0.353%	(300.3)
o/w French card and non-SEPA acceptor	*0.759%*	*(62.5)*	*0.688%*	*(70.2)*	*0.636%*	*(70.0)*	*0.692%*	*(74.5)*	*0.713%*	*(68.0)*
o/w French card and SEPA acceptor	*0.316%*	*(56.3)*	*0.366%*	*(67.9)*	*0.374%*	*(91.0)*	*0.459%*	*(116.8)*	*0.370%*	*(113.9)*
o/w foreign non-SEPA card and French acceptor	*0.639%*	*(78.2)*	*0.404%*	*(64.1)*	*0.336%*	*(65.6)*	*0.353%*	*(69.7)*	*0.449%*	*(73.7)*
o/w foreign SEPA card and French acceptor	*0.132%*	*(27.3)*	*0.135%*	*(29.1)*	*0.134%*	*(39.3)*	*0.153%*	*(36.9)*	*0.158%*	*(44.7)*
Total	**0.080%**	**(450.7)**	**0.080%**	**(469.9)**	**0.080%**	**(500.6)**	**0.082%**	**(522.9)**	**0.077%**	**(517.5)**

Source: Observatory for the Security of Payment Means.

T7 Breakdown of domestic fraud by transaction type

(fraud amount in EUR millions)

	Fraud rate									
	2012		2013		2014		2015		2016	
Payments	0.049%	(190.0)	0.050%	(199.9)	0.046%	(193.2)	0.043%	(185.1)	0.039%	(181.5)
o/w face-to-face and UPT	*0.015%*	*(51.2)*	*0.013%*	*(45.8)*	*0.010%*	*(37.1)*	*0.009%*	*(34.7)*	*0.008%*	*(29.2)*
o/w CNP	*0.299%*	*(138.8)*	*0.269%*	*(154.2)*	*0.248%*	*(156.0)*	*0.228%*	*(150.4)*	*0.199%*	*(152.3)*
o/w by post/phone	*0.338%*	*(29.4)*	*1.122%*	*(29.2)*	*0.147%*	*(2.8)*[2]	*0.208%*	*(5.1)*	*0.079%*	*(5.8)*
on the Internet	*0.290%*	*(109.4)*	*0.229%*	*(125.0)*	*0.251%*	*(153.2)*[3]	*0.229%*	*(145.3)*	*0.211%*	*(146.5)*
Withdrawals	0.031%	(36.4)	0.033%	(38.6)	0.034%	(41.5)	0.033%	(39.9)	0.029%	(35.7)
Total	**0.045%**	**(226.4)**	**0.046%**	**(238.6)**	**0.043%**	**(234.6)**	**0.040%**	**(225.0)**	**0.037%**	**(217.2)**

2) The substantial decline between 2013 and 2014 in the amount of fraud in CNP payments made by post or phone and the corresponding increase in the amount for internet payments are largely attributable to a change in the statistical methodology used by the "CB" Bank Card Consortium. A slight adjustment was also made in 2015. See the 2014 Annual Report for more details.
3) See previous footnote.
Source: Observatory for the Security of Payment Means.

T8 Breakdown of international fraud by transaction type – French cards

(fraud amount in EUR millions)

	Fraud rate			
	2013	2014	2015	2016
French card – Foreign non-SEPA acceptor				
Payments	0.547% (40.3)	0.532% (41.7)	0.735% (56.3)	0.862% (56.2)
o/w face-to-face and UPT	*0.377% (17.7)*	*0.350% (19.2)*	*0.509% (25.8)*	*0.494% (23.0)*
o/w CNP	*0.848% (22.6)*	*0.960% (22.5)*	*1.174% (30.5)*	*1.781% (33.3)*
o/w by post/phone	*1.234% (6.4)*	*4.955% (7.5)*	*2.345% (9.5)*	*2.239% (9.4)*
o/w on the Internet	*0.755% (16.2)*	*0.682% (14.9)*	*0.959% (21.1)*	*1.648% (23.9)*
Withdrawals	1.054% (29.9)	0.890% (28.3)	0.586% (18.1)	0.390% (11.8)
Total	**0.688% (70.2)**	**0.636% (70.0)**	**0.692% (74.5)**	**0.713% (68.0)**
French card – Foreign SEPA acceptor				
Payments	0.434% (66.8)	0.434% (89.8)	0.526% (115.7)	0.422% (112.9)
o/w face-to-face and UPT	*0.089% (8.2)*	*0.067% (7.8)*	*0.071% (8.0)*	*0.066% (8.4)*
o/w CNP	*0.937% (58.6)*	*0.910% (82.0)*	*1.004% (107.7)*	*0.742% (104.5)*
o/w by post/phone	*1.566% (11.3)*	*1.317% (13.9)*	*1.399% (18.7)*	*1.142% (19.7)*
o/w on the Internet	*0.856% (47.3)*	*0.856% (68.1)*	*0.948% (89.0)*	*0.687% (84.9)*
Withdrawals	0.036% (1.1)	0.033% (1.2)	0.033% (1.1)	0.024% (0.9)
Total	**0.366% (67.9)**	**0.374% (91.0)**	**0.459% (116.8)**	**0.370% (113.8)**

Source: Observatory for the Security of Payment Means.

T9 Breakdown of international fraud by transaction type – Foreign cards

(fraud amount in EUR millions)

	Fraud rate			
	2013	2014	2015	2016
Foreign non-SEPA card – French acceptor				
Payments	0.451% (63.2)	0.380% (65.0)	0.391% (68.1)	0.507% (73.2)
o/w face-to-face and UPT	*0.230% (25.3)*	*0.162% (21.9)*	*0.168% (22.8)*	*0.179% (17.4)*
o/w CNP	*1.268% (37.9)*	*1.213% (43.1)*	*1.185% (45.3)*	*1.179% (55.8)*
o/w by post/phone	*0.930% (9.2)*	*1.018% (7.7)*	*1.159% (10.8)*	*1.127% (18.2)*
o/w on the Internet	*1.436% (28.7)*	*1.265% (35.4)*	*1.193% (34.5)*	*1.206% (37.7)*
Withdrawals	0.051% (0.9)	0.026% (0.6)	0.069% (1.6)	0.024% (0.5)
Total	**0.404% (64.1)**	**0.336% (65.6)**	**0.353% (69.7)**	**0.449% (73.7)**
Foreign SEPA card – French acceptor				
Payments	0.158% (28.2)	0.156% (38.5)	0.175% (36.0)	0.178% (43.8)
o/w face-to-face and UPT	*0.039% (4.9)*	*0.026% (5.1)*	*0.033% (4.8)*	*0.025% (3.7)*
o/w CNP	*0.458% (23.2)*	*0.476% (33.1)*	*0.528% (31.3)*	*0.424% (40.0)*
o/w by post/phone	*0.308% (3.8)*	*0.397% (4.8)*	*0.734% (7.7)*	*0.490% (11.0)*
o/w on the Internet	*0.506% (19.4)*	*0.492% (28.6)*	*0.484% (23.6)*	*0.403% (29.0)*
Withdrawals	0.025% (0.9)	0.018% (0.9)	0.025% (0.9)	0.024% (0.9)
Total	**0.135% (29.1)**	**0.134% (39.3)**	**0.153% (36.9)**	**0.158% (44.7)**

Source: Observatory for the Security of Payment Means.

T10 Breakdown of domestic fraud by fraud type and by type of card

(amounts in EUR millions; share in %)

2016	All types of cards		Four-party cards		Three-party cards	
	Montant	Part	Montant	Part	Montant	Part
Lost or stolen cards	63.0	29.0	62.5	29.2	0.5	16.3
Intercepted cards	0.8	0.4	0.6	0.3	0.2	7.0
Forged or counterfeit cards	0.4	0.2	0.3	0.1	0.0	1.5
Misappropriated numbers	152.2	70.1	150.4	70.2	1.8	63.5
Other	0.7	0.3	0.4	0.2	0.3	11.7
Total	**217.2**	**100.0**	**214.3**	**100.0**	**2.9**	**100.0**

Source: Observatory for the Security of Payment Means.

T11 Breakdown of four-party card fraud by type of transaction, fraud type and geographical zone – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, Foreign SEPA acquirer		French issuer, Foreign non-SEPA acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	586.0	28,378.7	79.8	8,003.0	124.6	22,161.5
Lost or stolen cards	566.0	27,378.1	46.6	4,075.7	15.9	2,985.7
Intercepted cards	8.6	403.8	0.4	31.6	0.1	21.1
Forged or counterfeit cards	10.3	299.1	10.6	1,698.5	88.4	16,320.0
Misappropriated card numbers	0.1	10.8	13.4	1,696.7	14.5	2,121.3
Other	1.2	286.8	5.7	500.6	5.8	713.5
CNP payments excluding internet	43.5	4,979.8	242.1	19,349.9	62.9	9,114.3
Lost or stolen cards	0.5	18.0	21.5	2,619.1	6.9	1,344.0
Intercepted cards	0.0	0.1	0.1	4.8	0.0	2.3
Forged or counterfeit cards	0.0	1.0	5.0	398.4	2.5	400.7
Misappropriated card numbers	42.9	4,955.1	214.9	16,285.3	52.5	7,313.1
Other	0.1	5.6	0.6	42.2	1.0	54.1
CNP payments online	1,915.5	145,465.8	1,350.7	83,643.9	231.4	23,470.1
Lost or stolen cards	0.2	10.1	85.3	5,967.0	15.9	1,670.4
Intercepted cards	0.0	0.0	0.3	19.3	0.1	22.3
Forged or counterfeit cards	0.0	2.0	20.7	1,532.3	6.1	639.3
Misappropriated card numbers	1,915.3	145,442.3	1,242.5	75,983.5	208.6	21,069.5
Other	0.1	11.6	1.9	141.7	0.8	68.5
Withdrawals	119.7	35,445.3	4.4	932.3	75.9	11,802.2
Lost or stolen cards	118.0	35,098.1	3.0	696.9	4.8	291.6
Intercepted cards	0.7	232.4	0.1	46.9	0.0	3.0
Forged or counterfeit cards	0.0	12.6	0.9	132.9	48.1	11,165.9
Misappropriated card numbers	0.0	0.9	0.1	10.0	8.5	140.8
Other	0.9	101.3	0.3	45.6	0.9	200.9
Total	**2,665.0**	**214,269.6**	**1,677.1**	**111,929.1**	**494.9**	**66,548.1**

Source: Observatory for the Security of Payment Means.

T12 Breakdown of four-party card fraud by type of transaction, fraud type and geographical zone – Acceptance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		Foreign SEPA issuer, French acquirer		Foreign non-SEPA issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	586.0	28,378.7	26.8	3,499.7	77.4	14,912.1
Lost or stolen cards	566.0	27,378.1	12.3	1,827.3	18.8	4,634.5
Intercepted cards	8.6	403.8	0.8	171.5	0.3	147.3
Forged or counterfeit cards	10.3	299.1	7.3	432.6	48.9	7,754.2
Misappropriated card numbers	0.1	10.8	5.8	937.8	8.5	1,763.4
Other	1.2	286.8	0.6	130.6	0.9	612.7
CNP payments excluding internet	43.5	4,979.8	42.0	10,511.3	48.1	16,800.0
Lost or stolen cards	0.5	18.0	1.2	213.9	1.9	444.7
Intercepted cards	0.0	0.1	0.1	5.5	0.1	7.6
Forged or counterfeit cards	0.0	1.0	1.5	492.2	3.4	1,284.5
Misappropriated card numbers	42.9	4,955.1	39.1	9,764.1	42.3	14,869.5
Other	0.1	5.6	0.2	35.6	0.4	193.7
CNP payments online	1,915.5	145,465.8	158.1	28,234.4	191.6	35,909.8
Lost or stolen cards	0.2	10.1	2.9	532.7	5.5	1,029.6
Intercepted cards	0.0	0.0	0.1	18.5	0.1	19.4
Forged or counterfeit cards	0.0	2.0	2.4	403.6	13.4	2,322.4
Misappropriated card numbers	1,915.3	145,442.3	151.6	27,078.3	171.3	35,056.9
Other	0.1	11.6	1.1	201.3	1.4	481.5
Withdrawals	119.7	35,445.3	3.9	918.7	1.7	450.3
Lost or stolen cards	118.0	35,098.1	3.4	822.1	0.8	231.0
Intercepted cards	0.7	232.4	0.0	11.7	0.0	8.9
Forged or counterfeit cards	0.0	12.6	0.2	46.0	0.8	190.1
Misappropriated card numbers	0.0	0.9	0.1	25.1	0.1	16.7
Other	0.9	101.3	0.1	13.7	0.0	3.6
Total	**2,665.0**	**214,269.6**	**230.8**	**43,164.0**	**318.8**	**68,072.2**

Source: Observatory for the Security of Payment Means.

T13 Breakdown of three-party card fraud by type of transaction, fraud type and geographical zone – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, Foreign SEPA acquirer		French issuer, Foreign non-SEPA acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	2.63	855.95	0.85	418.76	3.70	801.00
Lost or stolen cards	0.75	272.75	0.11	80.64	0.33	128.21
Intercepted cards	0.47	159.22	0.05	16.47	0.02	1.74
Forged or counterfeit cards	0.14	23.85	0.15	84.02	2.20	364.38
Misappropriated card numbers	0.44	200.23	0.49	218.32	1.15	305.87
Other	0.84	199.89	0.05	19.31	0.01	0.80
CNP payments excluding internet	2.98	849.91	4.70	300.49	1.78	269.82
Lost or stolen cards	0.08	6.86	0.49	2.30	0.02	6.66
Intercepted cards	0.02	6.63	0.06	0.84	0.01	1.97
Forged or counterfeit cards	0.06	13.26	0.13	11.15	0.06	40.20
Misappropriated card numbers	2.75	766.49	4.00	281.10	1.70	220.51
Other	0.07	56.66	0.02	5.10	0.00	0.48
CNP payments online	2.80	984.49	16.04	1,232.32	2.65	414.48
Lost or stolen cards	0.14	24.81	0.14	3.20	0.04	3.22
Intercepted cards	0.02	2.09	0.01	0.04	0.00	0.20
Forged or counterfeit cards	0.02	5.15	0.07	16.44	0.05	14.87
Misappropriated card numbers	2.52	871.05	15.67	1,182.28	2.55	391.22
Other	0.11	81.39	0.16	30.36	0.01	4.97
Withdrawals	1.25	205.13				
Lost or stolen cards	1.05	168.96				
Intercepted cards	0.19	33.46				
Forged or counterfeit cards	0.00	0.00				
Misappropriated card numbers	0.00	2.26				
Other	0.01	0.44				
Total	**9.65**	**2,895.47**	**21.59**	**1,951.57**	**8.12**	**1,485.30**

Source: Observatory for the Security of Payment Means.

T14 Breakdown of three-party card fraud by type of transaction, fraud type and geographical zone – Acceptance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		Foreign SEPA issuer, French acquirer		Foreign non-SEPA issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	2.63	855.95	0.99	248.34	3.90	2,473.08
Lost or stolen cards	0.75	272.75	0.16	45.13	0.65	388.49
Intercepted cards	0.47	159.22	0.39	38.69	0.02	5.33
Forged or counterfeit cards	0.14	23.85	0.16	81.00	2.70	1,551.92
Misappropriated card numbers	0.44	200.23	0.12	49.80	0.28	119.76
Other	0.84	199.89	0.16	33.72	0.24	407.58
CNP payments excluding internet	2.98	849.91	1.27	530.04	3.15	1,358.85
Lost or stolen cards	0.08	6.86	0.01	14.21	0.11	38.41
Intercepted cards	0.02	6.63	0.00	0.86	0.11	21.82
Forged or counterfeit cards	0.06	13.26	0.04	21.51	0.41	111.55
Misappropriated card numbers	2.75	766.49	1.21	482.47	2.45	1,543.20
Other	0.07	56.66	0.01	0.99	0.07	49.77
CNP payments online	2.80	984.49	2.45	749.73	7.42	1,758.76
Lost or stolen cards	0.14	24.81	0.01	1.67	0.23	47.29
Intercepted cards	0.02	2.09	0.01	3.36	0.18	24.35
Forged or counterfeit cards	0.02	5.15	0.11	24.98	0.47	94.16
Misappropriated card numbers	2.52	871.05	2.26	671.14	6.43	1,543.20
Other	0.11	81.39	0.07	48.57	0.13	49.77
Withdrawals	1.25	205.13			0.11	33.12
Lost or stolen cards	1.05	168.96			0.09	27.40
Intercepted cards	0.19	33.46			0.00	0.00
Forged or counterfeit cards	0.00	0.00			0.00	0.00
Misappropriated card numbers	0.00	2.26			0.00	0.00
Other	0.01	0.44			0.02	5.72
Total	**9.65**	**2,895.47**	**4.71**	**1,528.11**	**14.59**	**5,623.81**

Source: Observatory for the Security of Payment Means.

Fraud statistics for credit transfers

T15 Geographical breakdown of credit transfer fraud

(value in EUR; share in %)

	Amount	
	Value	Share
France	25,671,275	29.7
SEPA outside France	46,943,345	54.4
Non-SEPA	13,744,853	15.9
Total	**86,359,473**	**100**

Source: Observatory for the Security of Payment Means.

Fraud statistics for direct debit payments

T16 Geographical breakdown of direct debit fraud

(value in EUR; share in %)

	Amount	
	Value	Share
France	39,930,322	99.99
SEPA outside France	5,560	0.01
Total	**39,935,882**	**100**

Source: Observatory for the Security of Payment Means.

Fraud statistics for cheques

T17 Breakdown by typology of fraud in 2016

(amount in EUR; share in % and volume in units)

	Amount		Volume	Amount
	Value	Share		
Misappropriation, replay	5,010,202	1.8	1,996	2,510
Fake (theft/loss/apocryphal)	123,537,940	44.7	96,112	1,285
Counterfeiting	32,418,849	11.7	6,444	5,030
Falsification	115,749,563	41.8	15,743	7,352
Total	**276,716,554**	**100**	120,295	2,300

Source: Observatory for the Security of Payment Means.

Published by
Banque de France
39, rue Croix-des-Petits-Champs
75001 Paris

Managing Editor
Denis Beau,
Director General, Operations
Banque de France

Editor-in-Chief
Emmanuelle Assouan,
Director of Payment Systems and Market Infrastructures
Banque de France

Editorial Secretariat
Véronique Bugaj, Guylène Chotard, Caroline Corcy, Bernard Darrius, Florian Dintilhac, Christelle Guiheneuc, Julien Lasalle, Antoine Lhuissier, Lucas Nozahic, Scott Oldale, Éloïse Senkur, Alexandre Stervinou, Mathieu Vileyn

Production
Banque de France
Press and Communication Directorate

Technical production
Studio Creation
Press and Communication Directorate
Banque de France

Orders
Observatory for the Security of Payment Means
011-2323
Telephone : + 33 1 42 92 96 13
Fax : + 33 1 42 92 31 74

Imprint
Banque de France

Website
www.observatoire-paiements.fr

The *Annual Report of the Observatory for the Security of Payment Means* can be downloaded for free on the Observatory's website *(www.banque-france.fr)*.