Annual Report
of the Observatory for the Security of Payment Means

2018

BANQUE DE FRANCE

EUROSYSTÈME

bservatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

2018 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 L. 141-4 of the French* Code monétaire et financier *(Monetary and Financial Code), was created by Law No. 2016-1691 of 9 December 2016. 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.

SUMMARY 7

1. MIGRATION PLAN FOR AUTHENTICATION SOLUTIONS BASED ON ONE-TIME PASSWORDS RECEIVED VIA SMS (SMS OTP) 11

1.1 Introduction 12

1.2 Monitoring migration towards strong customer authentication solutions 12

1.3 Target migration rate 13

1.4 The migration plan 15

2. FRAUD IN 2018 17

2.1 Overview 17

2.2 Card payment and withdrawal fraud 22

2.3 Cheque fraud 33

2.4 Credit transfer fraud 35

2.5 Direct debit fraud 37

3. TECHNOLOGY WATCH 41

3.1 The security of offline payment methods 41

3.2 The security of mobile payments 64

APPENDICES 87

A1 Security recommendations for the use of payment means 87

A2 Payer protection in the event of unauthorised payments 93

A3 Missions and organisational structure of the Observatory 97

A4 Members of the Observatory 103

A5 Methodological approach used to measure fraud on cashless payment means 107

A6 Statistics 117

Summary

This third Annual Report of the Observatoire de la sécurité des moyens de paiement *(OSMP - the Observatory for the Security of Payment Means) presents a mixed picture in terms of cashless payment means fraud.*

The following trends (discussed in greater detail in ***Chapter 2****) were noticeable in 2018.*

- *Cheques became the most used means of payment for fraudulent purposes in France, accounting for 43.1% of total fraud (compared with 40% in 2017) and amounting to EUR 450 million (up 52% from EUR 296 million in 2017), despite the continued decline in cheque use (down 11% in value terms).*

- *The fraud rates for other payment means remained low and relatively stable.*

  – *Thus, while the rate of fraud affecting French payment cards increased very slightly to 0.062%, compared with 0.058% in 2017, the fraud rate by type of card payment in France either (i) remained contained at low levels and relatively stable (0.010%, compared with 0.009% the previous year for face-to-face payments and UPTs – unattended payment terminals), (ii) was unchanged (0.020% in 2017 and 2018 for contactless payments despite them doubling in value in 2018), or (iii) continued to fall, as in the case of remote payment fraud, which declined for the seventh consecutive year to a rate of 0.173%, down from 0.190% in 2017, despite sharp growth in remote payments compared with 2017 (up 22% year on year).*

  – *The fraud rate for international transactions also declined once again from 0.281% in 2017 to 0.270% in 2018.*[1] *Fraud on Single Euro Payments Area (SEPA) transactions remained better contained than on non-SEPA country transactions. It should also be noted that fraud rates for international transactions were higher than the domestic rate, accounting for 54% of total fraud value but only 14% of the total value of transactions.*

  – *The fraud rates for credit transfers and direct debits were still extremely low at 0.0035% and 0.0004%, respectively.*

1 French cardholders defrauded abroad and foreign cardholders defrauded in France.

*In this context, the Observatory carried out two studies in 2018 and 2019, which are presented in **Chapter 3** of this report, on the security of cheques and offline payment means in general and on the security of mobile payments.*

- *As part of the first study, it was found that cheques are incompatible with the implementation of advanced security solutions and therefore remain vulnerable to falsification and counterfeiting. Nevertheless, enhancing security is both possible and necessary, and the Observatory therefore calls on all professionals to put measures in place to identify high-risk transactions, enabling banks, for example, to alert account holders to suspicious movements or warn merchants to refuse a transaction at the point of sale in the event of suspected fraud. In addition, and particularly with regard to cheque payment, users – private individuals, companies or general government administrations – must remain on their guard, for example by being attentive to the loss or theft of chequebooks (as mentioned among the recommended best practices in terms of vigilance presented in **Appendix 1** of this report).*

- *By contrast, mobile phones offer advanced security capabilities for payments and sensitive payment data (including card identifiers), although the level of security of the systems used still varies depending on the technologies adopted. However, the Observatory noted that the fraud rate for mobile payments was particularly well contained in France at 0.03%, rising to 0.04% for all transactions combined. This confirms the relevance of the recommendations made to stakeholders – banks, card payment systems and technological solution providers – called upon to implement strong customer authentication, both to secure user enrolment in mobile phone payment applications (apps) and to identify and warn of high-risk transactions.*

These latter issues underline the importance of the entry into force as from 14 September 2019 of the regulatory technical standards dedicated to security solutions in the second European Payment Services Directive (PSD2). These standards notably provide for the widespread implementation of strong customer authentication for electronic payments, and also of methods for identifying high-risk transactions (which will limit the need for strong customer authentication if fraud rates for remote transactions are maintained at low levels).

In this regard, the Observatory encourages all payment operators to push on with their efforts to comply with the changing regulations. For example, new strong customer authentication solutions will gradually replace the use of a code received by SMS. These solutions may, for example, be based on an app for smartphones or SIM cards (compatible with all mobile

devices) and require biometric verification or the entry of a secret code. Institutions will ensure that they offer solutions adapted to their entire customer-base, including the most vulnerable. However, as part of its commitment to supporting in the best possible conditions a complex transition that avoids penalising e-commerce and its users, the Observatory proposes an ambitious but gradual migration to these new solutions, in accordance with the guidance published by the European Banking Authority in its Opinion[2] of 21 June 2019. The resulting migration plan for France has been approved by all the stakeholders involved, from banks and merchants to card payment systems and consumer associations (see ***Chapter 1****), and should be implemented for a large majority of customers and transactions by December 2020 and fully in place within three years. The Observatory will publish regular updates in its annual report.*

Lastly, the Observatory undertakes to make an active contribution to the objectives of the national cashless payment strategy[3] in favour of the development of innovative and secure payment solutions.

2 The Opinion of the European Banking Authority (EBA) is available on its website: *https://eba.europa.eu*

3 The new national cashless payment strategy for 2019-24 is available online at: *https://www.banque-france.fr/en/financial-stability/national-cashless-payments-committee/national-retail-payments-strategy*

1 Migration plan for authentication solutions based on One-Time Passwords received via SMS (SMS OTP)

Box 1

Summary

- In France, the protection of remote card payments, just like sensitive online bank transactions such as the initiation of a credit transfer, relies on a range of systems including strong customer authentication of transactions deemed to be risky and facilitated in the vast majority of cases by sending one-time passwords by SMS to the lawful cardholder.
- This authentication method has demonstrated its effectiveness in combating online card payment fraud, as the Observatory's figures attest: for the seventh consecutive year, the fraud rate for these payments is in decline, falling to a historic low of 0.173% (the equivalent of one euro of fraud for every EUR 578 worth of transactions).
- European regulatory provisions have been established to further strengthen the security of electronic payments, particularly online, and make internet access to bank services more secure. Thus, from 14 September 2019, arrangements that comply with the new regulations will gradually replace the use of a one-time password received via SMS to authenticate transactions.
- These new arrangements may, for example, be based on an app for smartphones or SIM cards (compatible with all mobile devices) and require biometric verification or the entry of a secret code. Banks and payment service providers will ensure that the solutions they select and offer to their customers are best adapted to their entire customer-base, including the most vulnerable.
- The Observatory aims to support all market players as they move towards these new solutions to strengthen online transaction security, and has therefore developed a multistep migration plan that should be implemented for a large majority of customers and transactions by December 2020 and fully in place within three years.

1.1 Introduction

The second European Payment Services Directive (PSD2), Directive (EU) 2015/2366, which defines strong customer authentication (SCA), entered into force on 13 January 2018. Commission Delegated Regulation (EU) 2018/389 with regard to the regulatory technical standards (RTS) that elaborate on this directive will come into force on 14 September 2019 and will require the application of a "strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse".

The European Banking Authority (EBA) plays a role in promoting European convergence of supervisory practices, creating a level playing field and offering a high level of protection to depositors, investors and consumers. In its Opinion published on 13 June 2018 (EBA-Op-2018-04), the EBA set out its position on the implementation of the RTS, and particularly with regard to strong customer authentication. It specified that entering the details shown on a payment card during an online payment cannot be considered one of the two authentication factors required for the implementation of SCA.

Therefore, the customer authentication solution put in place by France's main banks for online card payments, i.e. entering card details and a one-time password (OTP) received via SMS, can no longer be considered "strong" and therefore is not an SCA solution in accordance with the new regulatory framework. Equally, this same method used to authenticate online bank users when carrying out certain sensitive transactions also fails to comply with the regulations.

In order to meet the RTS application deadline of 14 September 2019, which imposes strong customer authentication while nevertheless recognising that the market needs time to make the necessary adaptations, the Observatory for the Security of Payment Means wished to support the main players affected by the implementation of PSD2 in their migration towards solutions that fully comply with the new regulations.

Projects to add a new authentication factor to an existing arrangement or to implement a new authentication process, in compliance with the SCA definition, both require a significant amount of time for their technical implementation. At the same time, it is also essential that all users utilise the newly deployed solutions effectively.

This migration is a major project requiring a lengthy implementation period, which must be split down into a series of milestones.

1.2 Monitoring migration towards strong customer authentication solutions

In order to monitor the progress made by the main banking institutions in carrying out this migration, the Banque de France has developed indicators that will be added to an adapted 3D Secure questionnaire. This will still be sent to banks twice a year for data collection purposes and will provide the information needed to report on progress on the following aspects:

- the downward trend in the use of non-compliant systems;

Indicators for online card payments and sensitive online bank transactions

a) Online card payments

Monitoring	Indicators
SMS OTP trends	Number of cardholders enrolled in an authentication arrangement when making an online card payment
	Number of cardholders enrolled in a non SCA-compliant authentication arrangement (and not enrolled in a compliant system) when making an online card payment
	Number of online card payments during the past three months
	Number of online card payments during the past three months requiring strong customer authentication in compliance with the regulation
	Number of online card payments during the past three months triggering the use of a non SCA-compliant authentication arrangement
Development of SCA-compliant arrangements	Number of cardholders enrolled in at least one SCA-compliant authentication arrangement when making an online card payment
	Number of online card payments during the past three months triggering the use of an SCA-compliant authentication arrangement

b) Sensitive online bank transactions

Monitoring	Indicators
OTP SMS trends	Number of customers of online banks, or payment initiation or aggregation services enrolled in an authentication arrangement when carrying out sensitive transactions (credit transfer orders, adding account beneficiaries, quarterly renewal of online payment account tokens)
	Number of customers of online banks, or payment initiation or aggregation services enrolled in a non SCA-compliant authentication arrangement (and not enrolled in a compliant system) when carrying out sensitive transactions
	Number of online bank, or payment initiation or aggregation transactions during the past three months
	Number of online bank, or payment initiation or aggregation transactions during the past three months requiring strong customer authentication in compliance with the regulation
	Number of online bank, or payment initiation or aggregation transactions during the past three months triggering the use of a non SCA-compliant authentication arrangement
Development of SCA-compliant arrangements	Number of customers of online banks, or payment initiation or aggregation services enrolled in at least one SCA-compliant authentication arrangement when carrying out sensitive transactions on an online banking site or via an initiation or aggregation service
	Number of online bank, or payment initiation or aggregation transactions during the past three months triggering the use of an SCA-compliant authentication arrangement

Note: SMS OTP, one-time password received by SMS on a mobile phone; SCA – strong customer authentication.

- the development of authentication solutions that comply with the new regulation.

In order to do this, the main French banking institutions will report on the indicators shown in the table (inset) and the Banque de France will compile the results. In addition, the Observatory will ensure that payment market players offer solutions that are properly adapted and accessible to all their customers, particularly those whose equipment and consumer habits could impede the use of advanced technologies.

1.3 Target migration rate

The migration's objectives for the next three years are shown in Charts 1 and 2. They will be monitored at pre-defined stages and summary updates of the results will be published.

The following assumptions are applied in the development of this extended coverage.

- Customers must be equipped with devices that are compatible with a ramp-up of transactions authenticated using these new

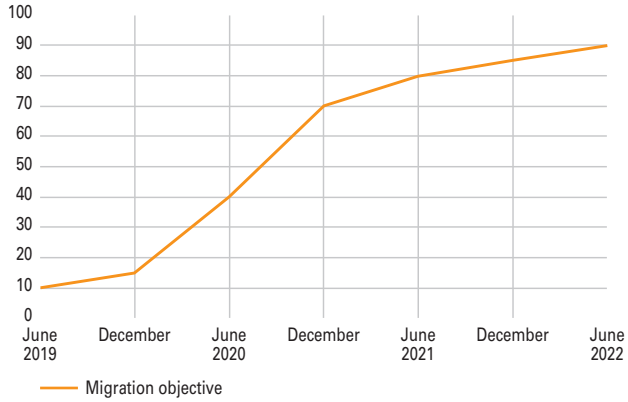
methods. However, cardholders that are already equipped, and thus more used to performing online transactions, are subsequently expected to generate more transactions than those who will not yet have migrated, which explains continued sustained growth in 2021 and beyond.

• While the beginning of the migration will be gradual, it will accelerate as a result of operators' communications and the more widespread introduction of the new arrangements to the general public. However, it is expected that once 80% of customers are equipped, the pace of migration will slow given the greater effort required to get stragglers on board.

• Consequently, the situation will have to be reviewed in June 2021 with regard to the remaining "SMS OTP user customers" in order to determine the best approach to take in light of PSD2 regulatory requirements.

C1 Customer enrolment

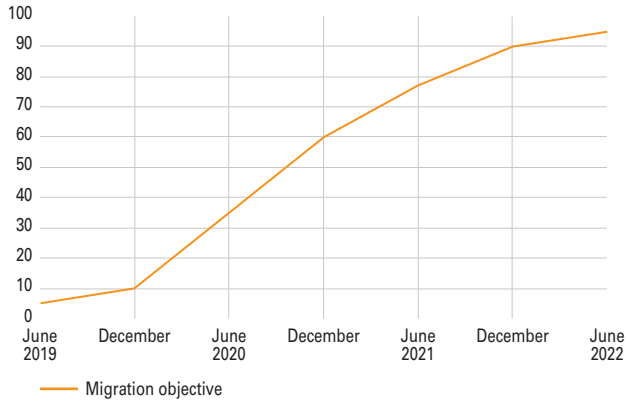
(%)



Source: Observatory for the Security of Payment Means.

C2 Authentication of payments requiring SCA

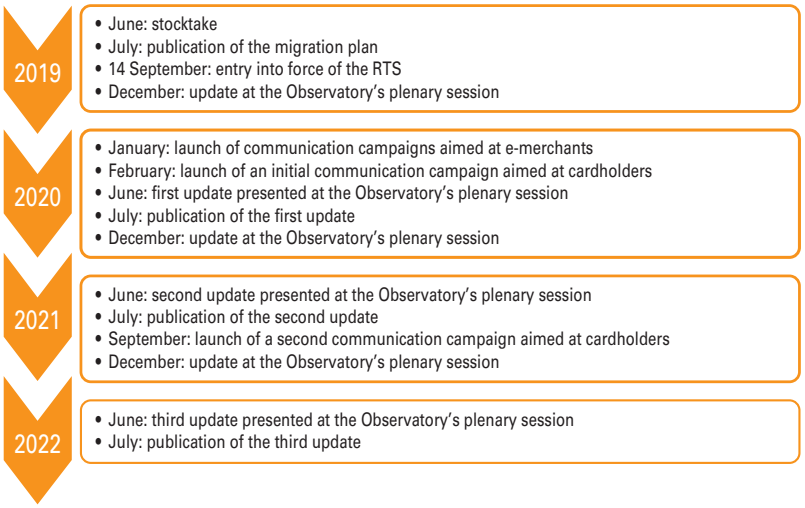
(%)



Source: Observatory for the Security of Payment Means.
Note: SCA – Strong Customer Authentication.

1.4 The migration plan

The Observatory will present updates during its 2019 plenary sessions held in June and December. The migration plan selected for publication in the annual report as well as the list of the main PSD2-compliant strong authentication technologies implemented by payment service providers were presented at the June 2019 meeting. With regard to this last point, on 21 June 2019, the EBA published an opinion supported by Europe's central banks and supervisors outlining the main elements of strong customer authentication under PSD2, with concrete examples, and encouraging industry players to establish a migration plan approved by the competent national authorities.[1] A statement on the progress made on the migration will be published in the Observatory's annual reports.



1 See https://eba.europa.eu

Box 2

The communication plan

The following wording has been suggested for use by Observatory representatives in their communications. They are therefore intended for payment service providers, e-merchants and their customers.

Information for payment service providers and e-merchants

European regulatory provisions have been established to strengthen the security of electronic – particularly online – payments, and make internet access to bank services more secure. Thus, from 14 September 2019, the use of a one-time password received via SMS to authenticate transactions will no longer suffice and will be progressively strengthened by means of a system that complies with the new regulation. These new arrangements may, for example, be based on an app for smartphones or SIM cards (compatible with all mobile devices) and require biometric verification or the entry of a secret code. These solutions are chosen by banks and payment service providers and offered to their customers.

.../...

Information for customers of payment service providers and e-merchants

[This wording is intended for payment service providers and e-merchants to be prominently displayed on their websites]

European regulatory provisions have been established to strengthen the security of electronic – particularly online – payments, and make internet access to bank services more secure. Thus, from 14 September 2019, the use of a one-time password received via SMS to authenticate transactions will no longer suffice and will be progressively strengthened by means of a system that complies with the new regulation.

For further details, please contact your bank or regular payment service provider.

Information for cardholders

European regulatory provisions have been established to strengthen the security of electronic – particularly online – payments. The current arrangement involving the entry of a one-time password received via SMS to authenticate an online card payment is therefore no longer sufficient.

[Your new authentication system will require/will be based on ...]

Information for online bank users

European regulatory provisions have been established to make internet access to bank services more secure. The current arrangement involving the entry of a one-time password received via SMS to ensure the security of certain transactions accessible online is therefore no longer sufficient.

[Your new authentication system will require/will be based on ...]

Information for consumers

European regulatory provisions have been established to strengthen the security of electronic – particularly online – payments, and make internet access to bank services more secure. Thus, from 14 September 2019, the use of a one-time password received via SMS to authenticate transactions will no longer suffice and will be progressively strengthened by means of a system that complies with the new regulation.

These new arrangements may, for example, be based on an app for smartphones or SIM cards (compatible with all mobile devices) and require biometric verification or the entry of a secret code. These solutions are chosen by banks and payment service providers and offered to their customers.

For further details, please contact your bank or regular payment service provider.

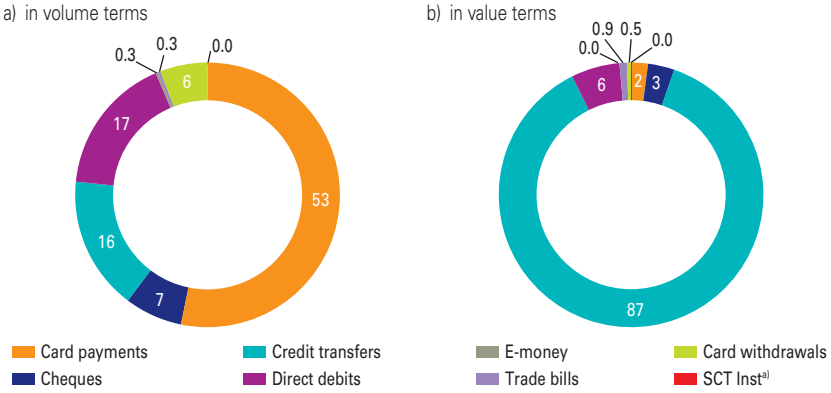
2 Fraud in 2018

DISCLAIMER

Due to a misinterpretation of the Observatory's methodology by a reporting institution, certain data presented in Chapter 2 and Appendix 6 differ from those previously published in the Observatory's annual reports. The corrections made affect the domestic payment card fraud data for the 2015-17 period and are set out in detail in Appendix 6 of this report. This chapter uses the corrected figures.

C1 Use of cashless means of payment in France in 2018

(%)



Source: Observatory for the Security of Payment Means.
a) SCT Inst: SEPA Instant Credit Transfer.

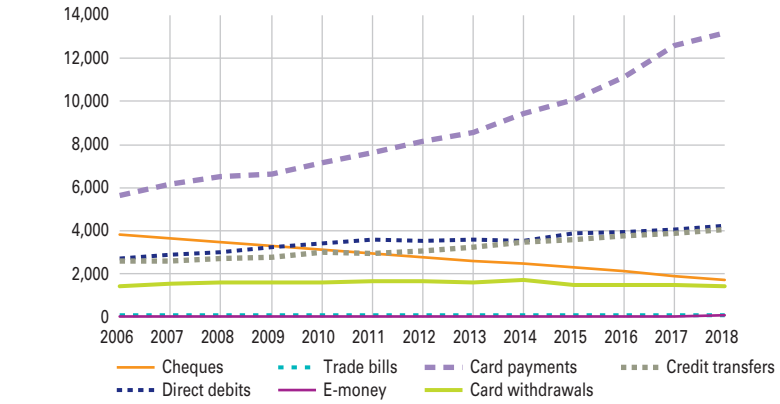
2.1 Overview

Means of payment

The customers (individuals and companies) of French banks and payment service providers carried out 24.7 billion cashless transactions in 2018 totalling EUR 27,704 billion. By comparison with the previous year, transaction volumes rose by 3%

C2 Use of cashless means of payment in France since 2006

(in millions of transactions)



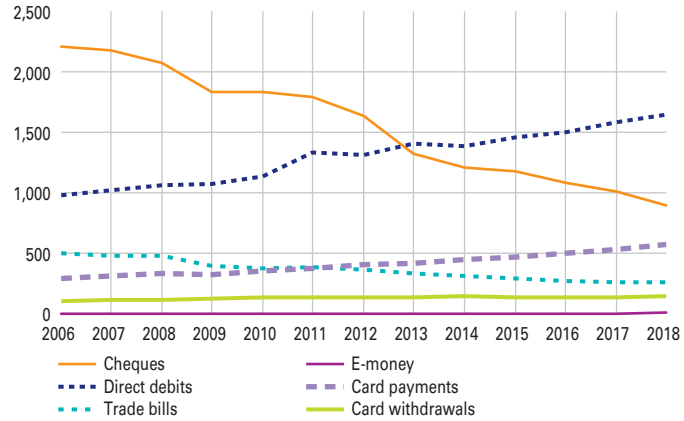
Source: Observatory for the Security of Payment Means.

and the values exchanged increased by 0.4%.

Payments by card remained the preferred payment method of French citizens, who used their card for 53% of all cashless payments for a total value of EUR 568 billion in 2018. Cash withdrawals by card also accounted for 1,439 million transactions in 2018 worth a little over EUR 136 billion.

C3 Value of transactions in France excluding credit transfers

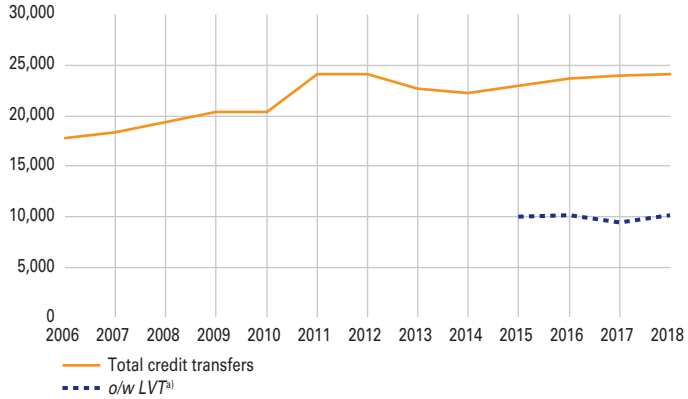
(EUR billions)



Source: Observatory for the Security of Payment Means.

C4 Value of credit transfers in France since 2006

(EUR billions)



Source: Observatory for the Security of Payment Means.
a) LVT: large-value transfers, issued via large-value payment systems (Target2, Euro1); professional payments only.

Credit transfers continued to be the preferred instrument for large-value payments (salary and pension payments, business-to-business payments, etc.) with 87% of the total value of cashless transactions, unchanged from 2017. They maintained their third position in terms of transaction volume, with a 16% share, just after payments by card and direct debits. Credit transfers were primarily domestic (with a 77% share of total credit transfers) with the remaining 23% going abroad to SEPA (Single Euro Payments Area) and non-SEPA countries. More than one-third (42%) of issued credit transfers pass through large-value payment infrastructures. These are exclusively business-to-business transactions with an average value of a little over EUR 1 million. The remainder is mainly composed of SEPA credit transfers, which can be arranged by both businesses and private individuals, with an average value of EUR 2,729, and to a lesser extent other forms of credit transfers, particularly international transfers outside the European Union.

Direct debit remained the second most used cashless payment instrument in terms of volume, accounting for 17% of the total number of transactions and 6% of their total value in 2018. Direct debit transactions were almost exclusively domestic (99%), with cross-border SEPA direct debit transactions accounting for only 1% of all originated flows.

The steady decline in **cheque** use observed over several years again continued in 2018, both in terms of transaction volume (down 9%) and value (down 11%). Cheques were issued to settle 1.7 billion transactions for a total value of EUR 891,052 billion.

Trade bills (bills of exchange and promissory notes) made up less than 1% of cashless transactions both in terms of volume (0.3%) and value (0.9%), with 2018 once again confirming the decline observed over a number of years.

Lastly, although the use of **electronic money** (e-money) was still marginal, it reported a slight rise, continuing the trend begun in 2017, to 65 million transactions (up 18%) with a total value of EUR 1,053 million (up 17%). This expansion was encouraged by the development of peer-to-peer payment solutions.

Fraud targeting payment means

In 2018, cashless transaction fraud amounted to EUR 1.045 billion for 6.7 million fraudulent transactions, up significantly by 36% in value compared with 2017 (EUR 771 million for 5.1 million fraudulent transactions).

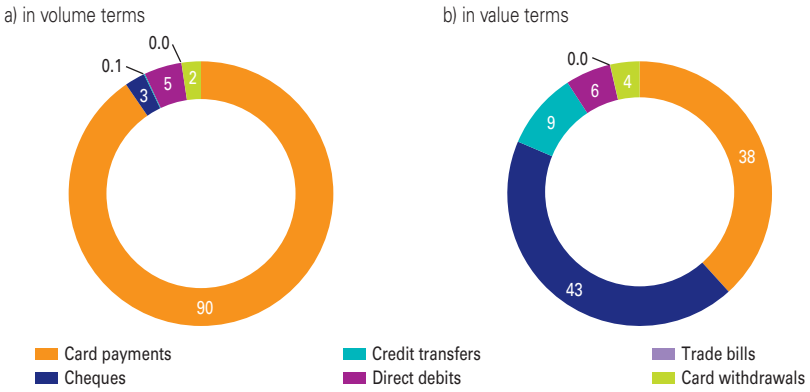
This trend is largely due to **cheques**, which have become the most used means of payment for fraudulent purposes in France. Cheque fraud accounts for 43.1% of total fraud and amounted to EUR 450 million in 2018 (up 52% compared with EUR 296 million in 2017) despite the continued decline in cheque use. The fraud rate for cheques was 0.0505%, or one euro of fraud for every EUR 1,980 worth of payments.

Payment cards[1] accounted for EUR 439 million, or 42% of total fraud in terms of value (38.4% for payments and 3.6% for withdrawals), and, in terms of volume, were used in almost all fraudulent transactions (92.4%). After a second consecutive year of decline in 2017, total fraud on cards issued in France rose year on year in 2018 to EUR 439 million from EUR 387 million (a 13.4% increase on payments and withdrawals made in France and abroad).

1 Cards issued in France.

C5 Breakdown of fraud on cashless means of payment in 2018

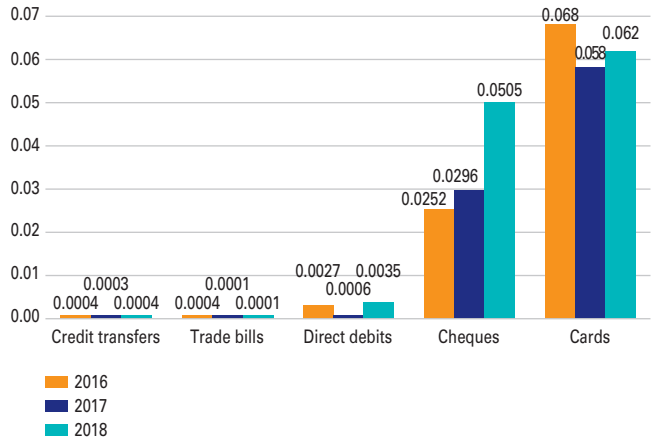
(%)



Source: Observatory for the Security of Payment Means.

C6 Change in fraud rate for each means of payment from 2016 to 2018

(%)



Source: Observatory for the Security of Payment Means.

This means that after remaining relatively constant for several years, the fraud rate for card transactions grew to 0.062%, or one euro of fraud for every EUR 1,612 worth of transactions. However, this average rate incorporates contrasting performances, notably with a very low rate of fraud for point-of-sale payments (0.010%, or one euro of fraud for every EUR 10,000 worth of transactions) but with a much higher rate for remote payments – despite a further significant decline – of 0.173%, or one euro for every EUR 578.

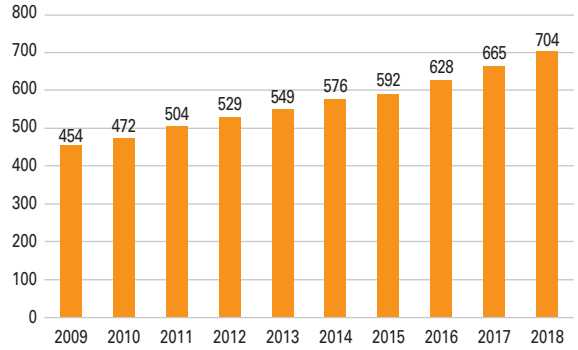
Although at EUR 97 million in 2018 the annual value of **credit transfer** fraud was still well below the levels recorded for cards and cheques, it increased by 24% year on year compared with EUR 78 million in 2017. Nevertheless, it registered the lowest rate of fraud across all payment means available to individuals, at 0.0004% (up from 0.0003% in 2017) or one euro of fraud for every EUR 244,300 paid.

Direct debits once again recorded the lowest annual fraud value of all cashless means of payment available to individuals with EUR 58 million in 2018, despite a very significant 544% increase from EUR 9 million in 2017. The direct debit fraud rate thus rose dramatically to 0.0035% (compared with 0.0006% in 2017), or one euro of fraud for every EUR 28,185 of originated direct debit instructions.

Trade bills were still relatively unaffected by fraud. In 2018, five cases of fraud accounted for EUR 226,000, representing a fraud rate of 0.0001%, or one euro for every EUR 1,115,000 paid.

C7 Total transaction value, French cards

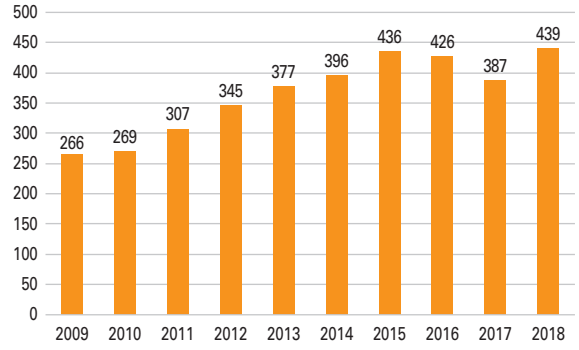
(EUR billions)



Source: Observatory for the Security of Payment Means.

C8 Total fraud value, French cards

(EUR millions)



Source: Observatory for the Security of Payment Means.

Box 1

Fraud statistics for payment cards: 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 2018 statistics calculated by the Observatory thus cover:

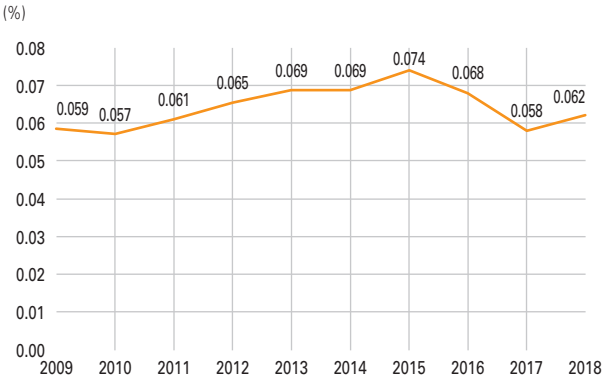
- EUR 683.7 billion in transactions in France and abroad made with 79 million four-party cards issued in France (including 58 million contactless cards);
- EUR 20.8 billion in transactions primarily in France with 9.8 million three-party cards issued in France;
- EUR 55.9 billion in transactions in France with foreign three-party and four-party cards.

Data was gathered from:

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

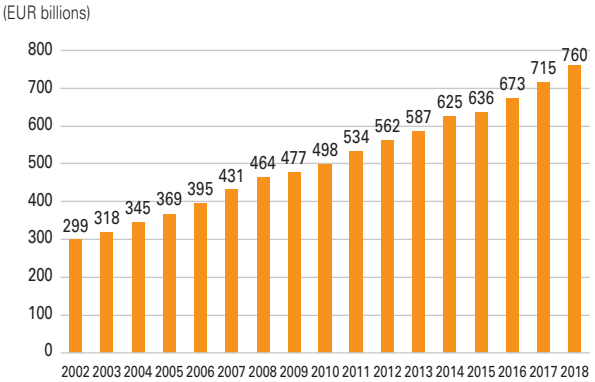
1 "Four-party" card payment schemes involve a large number of issuing and acquiring payment service providers, whereas "three-party" schemes involve a smaller number.

C9 Fraud rate, French cards



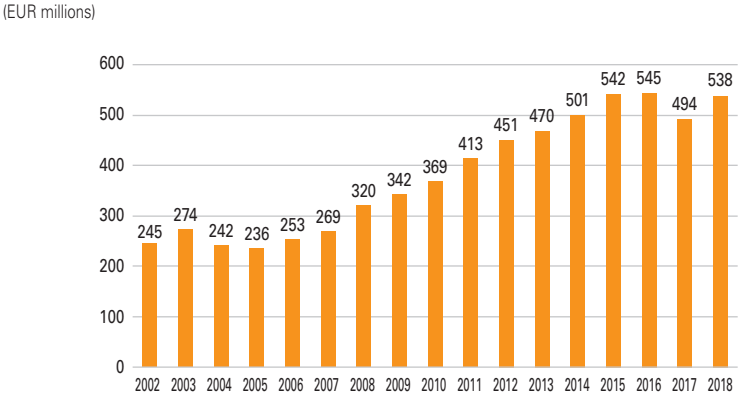
Source: Observatory for the Security of Payment Means.

C10 Total transaction values processed in French payment systems, French and foreign cards



Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

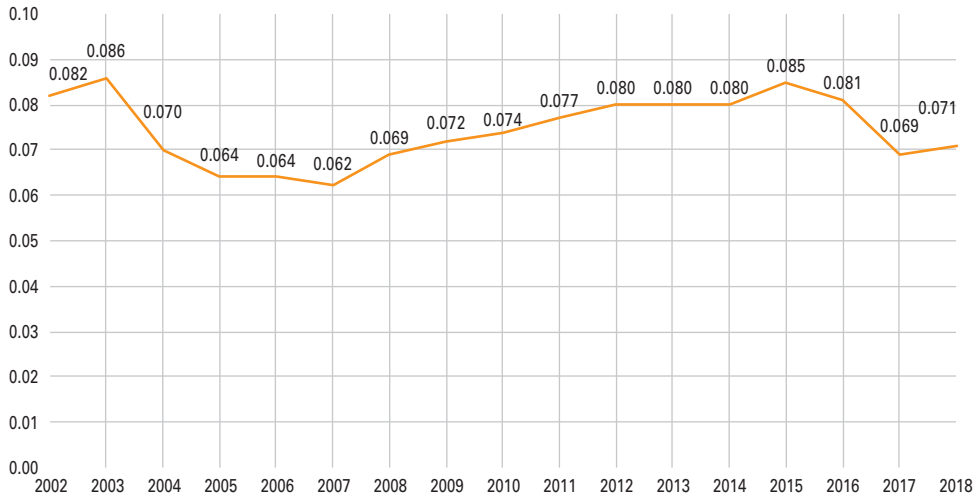
2.2 Card payment and withdrawal fraud

Overview

Following a dip in 2017, fraud targeting payments and withdrawals using French cards in France and abroad picked up in 2018 (up 13.4% compared with 2017) and amounted to EUR 439 million out of a total transaction value of EUR 704.4 billion (up 5.9% on 2017).

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

(%)



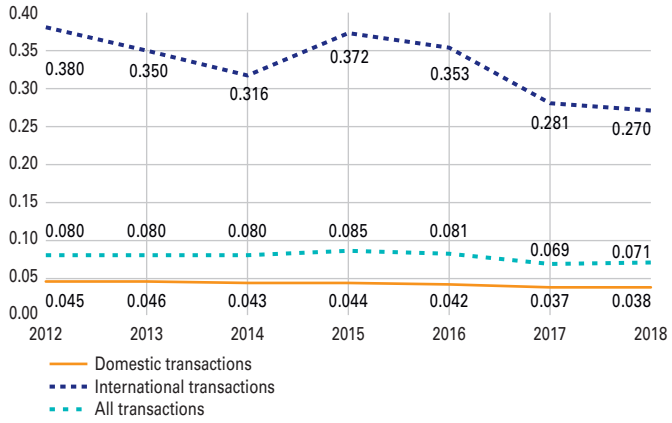
Source: Observatory for the Security of Payment Means.

Consequently, the rate of fraud affecting French payment cards deteriorated very slightly to 0.062%, compared with 0.058% in 2017 (see Chart 9), or one euro for every EUR 1,612 worth of transactions. When transactions carried out in France using cards issued in other countries are also included, the same trend can be seen, with an 8.9% year-on-year rise in the total value of fraud to EUR 538 million in 2018, while the total value of transactions climbed 6.3% to EUR 760 billion.

As a result, the overall fraud rate for transactions processed by French electronic banking systems, which includes payments and withdrawals made in France and abroad using French cards as well as those made in France using foreign cards, saw a very

C13 Fraud rate by geographical area

(%)



Source: Observatory for the Security of Payment Means.

minor increase from 0.069% in 2017 to 0.071% in 2017 (see Chart 12). This corresponds to one euro of fraud for every EUR 1,412 worth of transactions.

Lastly, the number of French cards for which at least one fraudulent transaction was recorded in 2018 increased by 12% compared with 2017 to 1,358,819. However, this increase did not coincide with an upturn in the average value of individual cases of fraud, which remained relatively stable at EUR 70.5 in 2018 compared with EUR 69.8 in 2017. This is due to the strengthening of measures to make card payments more secure, such as stronger authentication of online payments, risk-analysis and transaction scoring systems and SMS alerts sent to cardholders, which has led to more rapid detection and deactivation of compromised cards and has forced fraudsters to step up their fraud attempts while reducing the individual amounts taken in an effort to avoid detection.

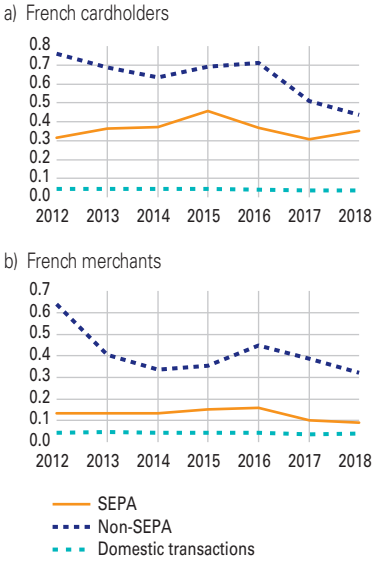
Geographical breakdown of fraud

Following a reduction in domestic transaction fraud in 2017, there was an 8.4% upturn in 2018. The value of fraud on payments and withdrawals made in France using French cards increased to EUR 245.6 million compared with EUR 226.5 million in 2017. However, given the growth in domestic transactions of 5.2% in value terms compared with 2017, the fraud rate is still relatively low at 0.038% – one euro of fraud for approximately EUR 2,600 worth of transactions – and almost unchanged from 2017 (0.037%)

Fraud on international transactions[2] also increased, by 9.2% year on year to a total value of EUR 291.9 million, largely due to the upward trend in international transactions, which grew by 13.4% in value terms compared with 2017. Consequently, fraud on international transactions was better controlled as the fraud rate for 2018 declined to a record low of 0.270%, compared with 0.281% in 2017. Nevertheless, it is important to note that this rate is still high in view of the value of the transactions concerned as international transactions accounted for 54% of the total fraud value even though they made up only 14% of the total value of transactions.

In addition, by geographical area, the following was found:

C14 Fraud rate by geographical area
(%)



Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

- in the case of French cards, a slight increase in the fraud rate for transactions carried out within SEPA,[3] which increased from 0.308% in 2017 to 0.352% in 2018 but which remained lower than for transactions carried out outside SEPA (down in 2018 from 0.511% in 2017 to 0.438%);

2 Payments and withdrawals made abroad using French cards and payments and withdrawals made in France using foreign cards.

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

Box 2

Fraud targeting contactless payments

The boom in the use of contactless payments continued in France, with an increase of 82% in volume and 89% in value. Thus, 2.3 billion contactless payments were recorded in 2018, worth a total of EUR 24.4 billion (compared with 1.2 billion transactions for EUR 12.9 billion in 2017), which corresponds to 6% in value and 21% in volume of all face-to-face payments, or one in five card payments. The average contactless payment value amounted to EUR 10.5 in 2018. The total value of contactless transactions including contactless domestic payments carried out in France using foreign cards and contactless payments carried out abroad using French cards reached EUR 25.8 billion for 2.4 billion transactions. This represents a year-on-year increase of 87% in value and 82% in volume.

At the same time, the fraud rate for domestic contactless payments stayed stable at 0.020% (for a total fraud value of almost EUR 5 million) and remained at a midway level between the overall rate for face-to-face payments (0.010%) and the rate for withdrawals (0.024%), and thus well below the remote payment fraud rate (0.173%). If contactless domestic payments made in France using foreign cards and contactless payments made abroad using French cards are also taken into consideration, the fraud rate remains almost identical to that of 2017, i.e. 0.021%.

In 2018, as in previous years, all contactless payment fraud could be traced back to loss or theft of a card. Card issuers have placed ceilings on individual transactions (usually EUR 30) and on the total consecutive transaction amount possible without entering the PIN (typically EUR 100), thus limiting the loss incurred if a card is lost or stolen. It is also important to remember that cardholders are protected by law in the event of fraud and bear no losses (see Appendix 2).

These figures include payments by mobile phone, which also rose even though their share of total domestic face-to-face transactions remained marginal at 0.10%. In 2018, 10.9 million domestic payments were carried out using mobile devices, representing an almost 2.5-fold increase over 2017, while the total value of those payments amounted to nearly EUR 190.9 million compared with EUR 83.5 million in 2017. Including transactions carried out in France using foreign mobile devices and transactions carried out abroad using French mobile phones, the total value of payments in 2018 comes to EUR 219.6 million for 12.4 million transactions.

In 2018, some cases of fraud were reported on domestic mobile telephony transactions although the total value was minimal (less than EUR 50,000) and the fraud rate amounted to 0.03%. The overall fraud rate for payments by mobile phone across all regions increased from 0.03% in 2017 to 0.04%, with a total fraud value of a little less than EUR 88,000.

Box 3

Domestic remote payment fraud, by sector of activity

The Observatory gathers data providing information on the breakdown of remote payment fraud by sector of activity. These data cover domestic transactions only.

Breakdown of fraud by sector of activity

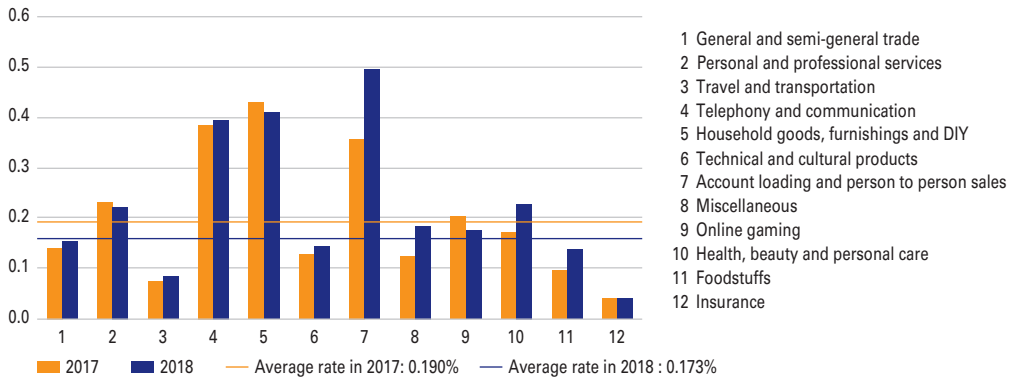
(amount in EUR millions, share in%)

		Amount	Share
1	General and semi-general trade	39.2	22.6
2	Personal and professional services	38.8	22.4
3	Travel and transportation	25.7	14.9
4	Telephony and communication	24.5	14.1
5	Technical and cultural products	13.2	7.6
6	Household goods, furnishings and DIY	8.8	5.1
7	Account loading and person to person sales	7.4	4.3
8	Online gaming	5.3	3.1
9	Miscellaneous	5.3	3.1
10	Health, beauty and personal care	2.3	1.3
11	Foodstuffs	2.2	1.2
12	Insurance	0.6	0.3
Total		**173.3**	**100.0**

"General and semi-general trade", "personal and professional services", "travel and transportation" and "telephony and communication" continued to be the most exposed sectors to remote payment fraud, accounting for 74% of the total fraud value. Based on a comparison of the average fraud rates for each of these activities, we find that "account loading and person to person sales", "technical and cultural products" and "telephony and communication" account for a lower share of total fraud but are victim to a much higher than average fraud rate (see chart below).

Fraud rate for remote sales by sector of activity, domestic transactions

(%)



Source: Observatory for the Security of Payment Means.

• in the case of foreign cards, a reduction in the fraud rate for transactions carried out in France using cards issued outside SEPA (0.323%), which nevertheless remained elevated at 3.5 times higher than the rate for transactions in France using cards issued within SEPA (0.092%).

Breakdown of fraud by transaction type

Fraud targeting domestic transactions

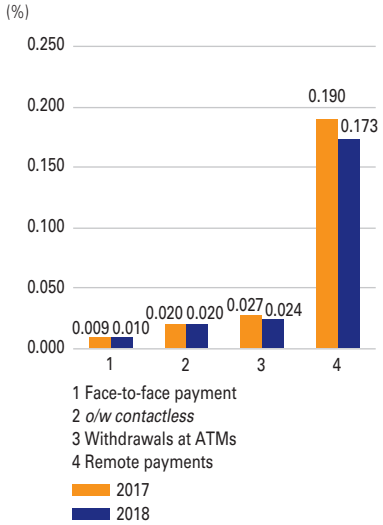
Although the value of fraud on domestic transactions increased in 2018, the fraud rates for the various transaction types improved, with the exception of face-to-face payments and UPTs (unattended payment terminals), which deteriorated very slightly.

The following observations for the different transaction types were noted in 2018.

• With regard to face-to-face payments and UPTs, and despite the increase in fraud in 2018, the fraud rate remained extremely low and almost unchanged year on year at 0.010% (compared with 0.009% in 2017). This is partly due to the growth in contactless payments, which have a significantly higher fraud rate (see Box 2 above). Face-to-face payments and UPTs still account for a major share of total domestic transaction amounts – almost two-thirds – but only 17% of the value of domestic fraud.

• For remote payments, despite an increase in fraud value in 2018, the fraud rate declined for the seventh year running to 0.173% from 0.190% in 2017 as a result of the substantial 22% year-on-year growth in the value of remote transactions. This improvement is the result of issuers', merchants' and companies' efforts to improve customer protection by rolling out strong customer authentication solutions such as 3D-Secure, and risk-analysis and transaction scoring tools, i.e. expert systems capable of assessing the risk level of a given transaction on the basis of its characteristics such as customers' habits, location or equipment used. However, even though remote payment fraud is declining, it still accounts for the majority (70%) of the total value of domestic fraud and its fraud rate remains 17 times higher than the rate for face-to-face payments. The implementation of the strong customer authentication security requirements set out in the second European Payment Services Directive (PSD2) and particularly the entry into force of provisions to ensure the widespread application of strong customer authentication and analysis of risky transactions on 14 September 2019, should lead to a reduction in online payment fraud.

C15 Comparison of fraud rates by domestic transaction type



Source: Observatory for the Security of Payment Means.
Note: ATMs – Automated Teller Machines.

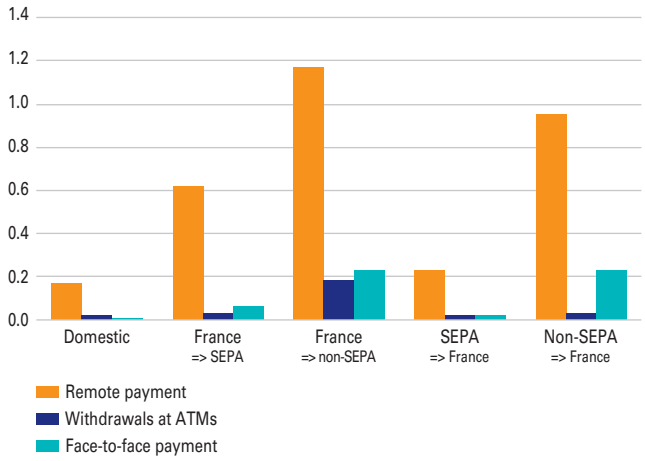
• With regard to withdrawals, the steady decline in the fraud rate that began in 2015 continued in 2018, edging down to 0.024% from 0.027% in 2017.

Fraud targeting international transactions

While fraud on international transactions increased in 2018 and trends varied depending on transaction type and geographical area, fraud continues to be better controlled for transactions within SEPA than for transactions carried out with non-SEPA countries thanks to the efforts made in Europe over the past several years to migrate all cards and payment terminals to the EMV (Europay, MasterCard and Visa)[4] standard and enhance the security of online payments.[5]

C16 Fraud rate by transaction type and geographical origin

(%)



Source: Observatory for the Security of Payment Means.
Notes: See Appendix 5.
SEPA – Single Euro Payments Area; ATMs – Automated Teller Machines.

- In the case of French cards, the increase in the fraud rate for transactions carried out within SEPA can be traced to online transactions, whose fraud value rose from EUR 74.4 million to EUR 118 million in 2018 with a fraud rate of 0.594% (up from 0.527% in 2017), i.e. 3.5 times greater than the fraud rate for this type of transaction at the domestic level. Conversely, fraud on transactions carried out outside SEPA improved from EUR 60.3 million in 2017 to EUR 50.3 million for a fraud rate of 0.438% (down from 0.511% in 2017) but fraud on remote payments increased with a relatively high fraud rate of 1.168%.

- In the case of foreign cards used for transactions in France, fraud rates improved for both cards issued within SEPA (0.092%, down from 0.102% in 2017) and outside (0.323%, compared with 0.386% in 2017), but the fraud rate for remote payments using cards issued outside SEPA continued to be high at 0.947%.

4 EMV is an international technical security standard for smart payment cards, whose specifications were developed by the EMVCo consortium of American Express, JCB Cards, MasterCard and Visa. The EMV standard for face-to-face payments and withdrawals notably provides for the use of a combination of a secure card chip and a secret code, commonly referred to as "Chip and PIN".

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

Box 4

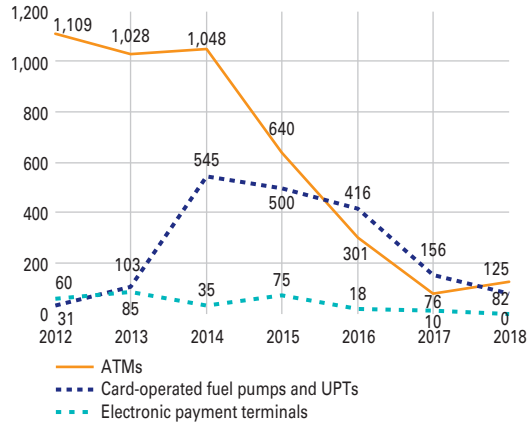
Indicators provided by law enforcement agencies

Automated Teller Machine (ATM) attacks increased in 2018 with 125 cases (after 76 in 2017) but still remained at a relatively moderate level compared with the levels observed prior to 2017. There was also a rise in the use of "jackpotting" techniques to compromise ATMs in 2018 with a wider variety of operating methods employed. "Jackpotting" involves connecting a computer to take control of the ATM and either targeting the dispense calculation function or installing a malware.

By contrast, attacks on card-operated fuel pumps were down to 64 cases in 2018 from 121 in 2017 and attacks on unattended payment terminals (UPTs), such as parking pay points also decreased from 35 cases in 2017 to 18 in 2018. However, no attacks on merchant payment terminals were reported.

Attacks on ATMs and terminals

(number)



Source: Observatory for the Security of Payment Means.
Note: ATMs – Automated Teller Machines; UPTs – unattended payment terminals.

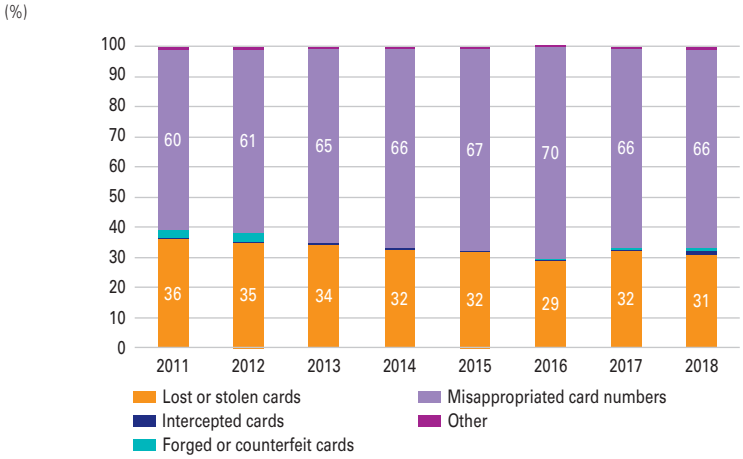
Regardless of the type of payment terminals or ATMs that are compromised, the payment card data thus obtained by criminal networks are then exploited, either to create counterfeit magnetic stripe cards to make payments and withdrawals abroad, chiefly in countries where EMV smartcard technology is not widely used, or to misappropriate card numbers for use in remote payments, particularly on e-commerce sites that have not implemented cardholder authentication solutions.

Breakdown of fraud by transaction type

The misappropriation of card numbers to carry out fraudulent payments was still the most common type of fraud, representing 66% of the total value, and phishing[6] and malwares[7] were still the most used card number misappropriation techniques in 2018. Lost or stolen cards continued to be the second most common source of fraud, making up almost one-third of domestic transaction fraud (31%).

Counterfeit cards accounted for just 1% 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.

C17 Breakdown of card payment fraud by type



Source: Observatory for the Security of Payment Means.
Note: Domestic transactions, excluding withdrawals, in value terms.

Monitoring of authentication solution deployment

The development of online trade has led to the increasing use of cards for remote 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 secure transactions. Against this backdrop and with the objective of stronger remote payment security, the Observatory for Payment Card Security issued recommendations in 2008, aimed at the wider adoption of secure authentication arrangements for cardholders. Statistics developed to monitor the implementation of these recommendations have been kept since 2011.

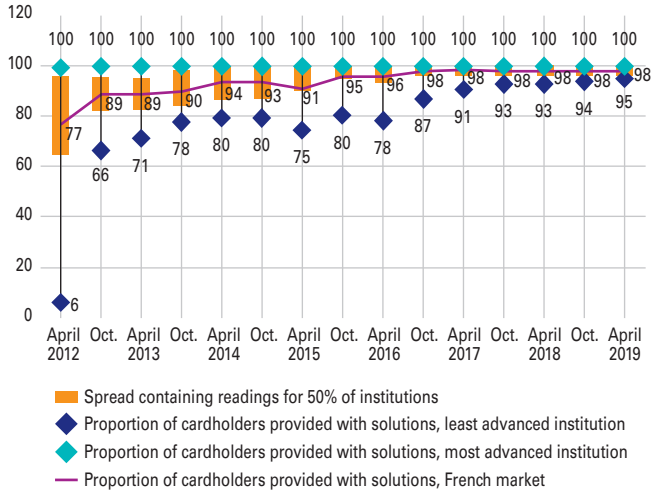
For the November 2018 to April 2019 period, the Observatory's statistical monitoring of the deployment of authentication solutions at the main banking institutions covered 66.7 million payment cards and EUR 61.2 billion worth of transactions (of which EUR 26.4 billion were protected using the 3D-Secure

6 Phishing generally involves sending emails that misuse visual identities and logos (e.g. of a credit institution) that are recognisable to the receiver, inviting their victims to connect to a fraudulent website in order to collect card data.

7 Malicious software targets both the servers of large corporations and the personal computers of private individuals, and, increasingly, mobile phones that are used more and more regularly for payment transactions. One of the most common of these "malwares" is known as "keylogger" and records the keystrokes on a victim's keyboard. They are generally downloaded without the user's knowledge through what appear to be trustworthy sources.

C18 Distribution of cardholders provided with customer authentication solutions

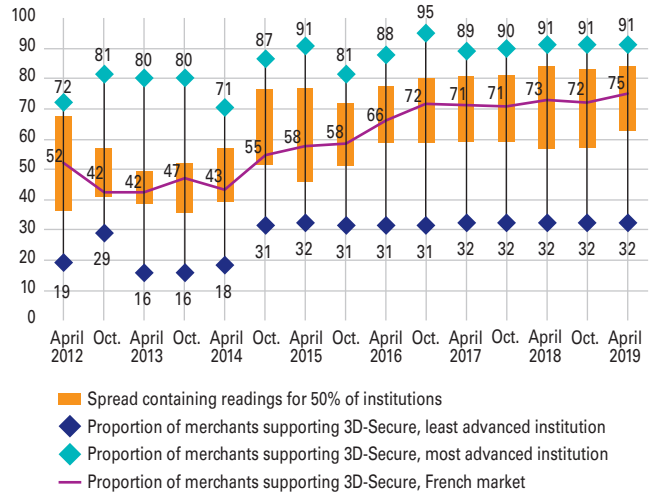
(%)



Source: Observatory for the Security of Payment Means.

C19 Take-up of 3D-Secure by merchants

(%)



Source: Observatory for the Security of Payment Means.

mechanism), making it possible to measure progress in the implementation of secure authentication methods both quantitatively and qualitatively.

At the end of April 2019, the switch by cardholders to these authentication solutions is almost universal, with an average rate of enrolment of 98.4%, covering all cardholders who might carry out transactions online. In the case of e-merchants, while take up of the 3D-Secure mechanism continues to increase and now stands at an average rate of 75%, there are nonetheless gaping disparities between different banks, with rates of between 32% and 91%. It is important to note that e-merchants must have a strong customer authentication solution in place to comply with PSD2.

The Observatory has observed that the failure rate for authenticated transactions, which has settled at 11%, is under control 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 authentication solutions, which is

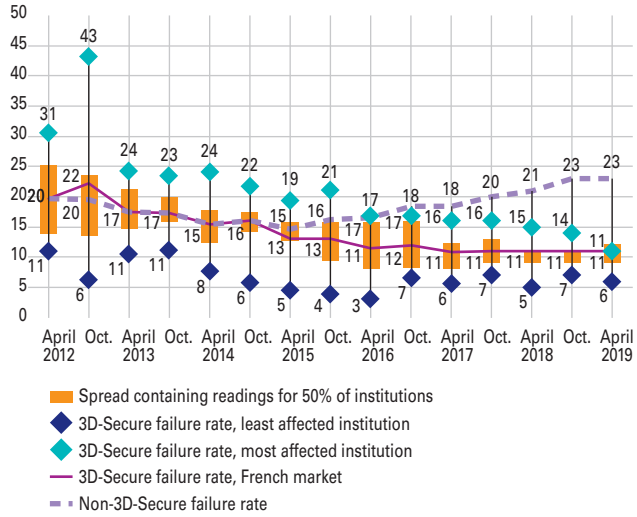
forcing fraudsters to concentrate on websites that are not protected by such measures. This therefore confirms the benefit to e-merchants of using the 3D-Secure mechanism as the failure rate for unsecured transactions increases regularly.

In view of these trends, which are supportive of continued growth in the use of authentication solutions, the share of online payments covered by 3D-Secure authentication has been rising steadily since 2011 and accounted for 43% of the value of remote payments at the end of April 2019.

The fraud rate for domestic transactions authenticated through the 3D-Secure protocol amounted to 0.07% in 2018, almost unchanged from the 2017 rate of 0.06%. This level more closely approximates the fraud rate observed for domestic transactions as a whole, including face-to-face payments (0.038%), rather than the fraud rate for all remote payments (0.173%). This fraud rate hierarchy supports the strategy championed by the Observatory since 2008 of using strong authentication, and which is now part of the security requirements set out in the framework of PSD2, which entered into force in January 2018 across the European Union. With regard to this point, it is important to remember that in its Opinion on the implementation of regulatory technical standards (RTS) published on 13 June 2018, the European Banking Authority (EBA) deemed that the authentication of online card payments using a one-time

C20 Distribution of 3D-Secure failure rates

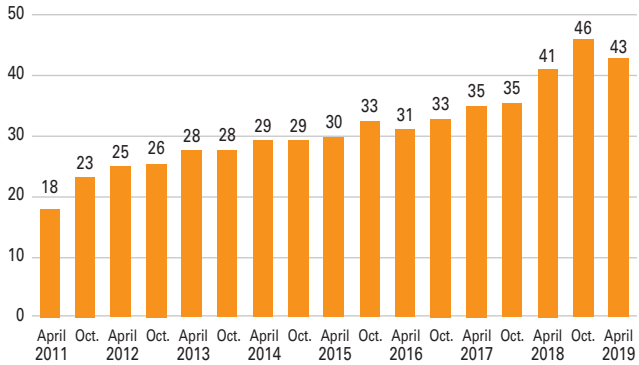
(%)



Source: Observatory for the Security of Payment Means.

C21 Proportion of total online payments authenticated by 3D-Secure

(%)



Source: Observatory for the Security of Payment Means.

password (OTP) received via SMS that is widely used in France does not comply with PSD2 requirements. In order to support the French financial sector in the coordinated implementation of PSD2 strong authentication provisions, the Observatory has drawn up a roadmap, which can be found in Chapter 1 of this report, that sets out the modalities of this migration, both from a technical point of view and in terms of assisting stakeholders, traders and consumers.

2.3 Cheque fraud

Overview

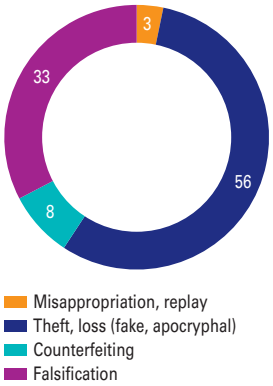
For the third consecutive year, there has been an increase in the value of cheque fraud, which amounted to EUR 450 million in 2018, up 52% year on year. Consequently, and given that cheque use is in decline, the cheque fraud rate rose sharply to 0.0505% in 2018 from 0.0296% in 2017. Cheques are thus the most targeted payment instrument above payment cards (43.1% and 42.0%, respectively, of total fraud value), despite being far less widely used. The cheque is only the fourth most common form of cashless payment used in terms of annual volume of payments and is used 8.5 times less often than the card. The average value of a fraudulent cheque remitted for collection also increased slightly from EUR 2,577 in 2017 to EUR 2,704 in 2018.

Improvements to the manual processing of fraud data have meant that the fraud cases encountered can be better categorised. Thus, as in 2017, two categories of fraud made up the majority of the fraud value in 2018: (i) the fraudulent use of lost or stolen cheques, which increased sharply to 56% of total cheque fraud from 44% in 2017; and (ii) the falsification of validly-issued cheques, which accounted for 33%. Fraud through counterfeiting and misappropriation/replay of cheques continued to be far less common, representing 8% and 3% of total cheque fraud, respectively.

There was a general increase in the average individual value of cheque

C22 Value-based breakdown of cheque fraud by type

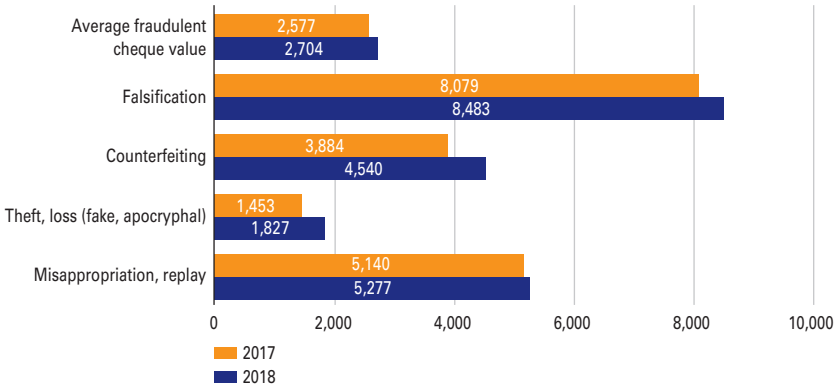
(%)



Source: Observatory for the Security of Payment Means.

C23 Individual fraudulent cheque values by fraud type, 2017-18

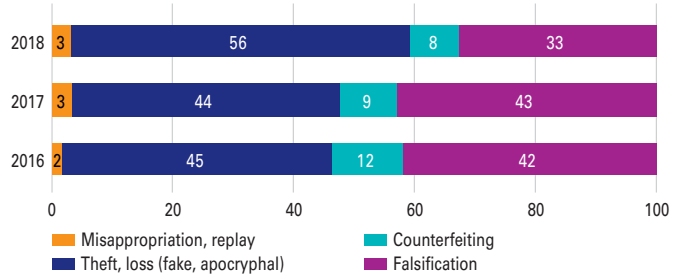
(in EUR)



Source: Observatory for the Security of Payment Means.

C24 Value-based breakdown of cheque fraud by type, 2016-18

(%)



Source: Observatory for the Security of Payment Means.

fraud, with EUR 8,483 for falsified cheques, EUR 4,540 for counterfeit cheques, EUR 1,827 for lost or stolen cheques and EUR 5,277 for misappropriated or replayed cheques.

The Observatory thus reiterates its recommendations, repeated below and in the study presented in Chapter 3 of this report, with regard to offline payment methods.

Main cases of cheque fraud	Preventive 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 two 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.	**Traceable shipment** processes 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 in the event of a delay. **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, over-writing or erasing information contained on it. The fraudster exploits the vulnerabilities of a stolen cheque by, for instance: • scratching or erasing 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 Fichier national des chèques irréguliers (FNCI, the national register of irregular cheques)** via the Banque de France's official prevention service for unpaid cheques.[1]
Counterfeiting of cheques, through the creation from scratch of a false cheque to be drawn on an existing or 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 unusual deposit movements** in light of 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 See https://www.verifiance-fnci.fr

2.4 Credit transfer fraud

Overview

In 2018, fraud on credit transfers issued from accounts held in France amounted to almost EUR 97 million, up 24% from 2017. Consequently, the fraud rate returned to its 2016 level of 0.0004%. These figures confirm that proportionally speaking, credit transfers were still the cashless payment method least affected by fraud, even though they are used to move the most significant overall values (87% of all cashless payments issued in France). The average value of a fraudulent credit transfer declined from EUR 16,864 in 2017 to EUR 12,586.

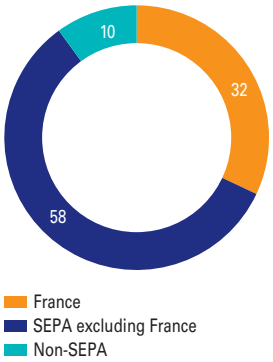
Cross-border credit transfers accounted for a larger proportion of fraud than domestic transfers with 68% of the credit transfer fraud value, even though cross-border transactions made up only 23% of the overall issued transfer amount.

The methodological work undertaken in 2017 to categorise fraudulent credit transfers that means that data is better measured and assigned (see Appendix 6), confirms that fake credit transfers, i.e. the issuance of a fraudulent transfer order by means of cyber-attacks, continues to account for a majority of credit transfer fraud with 52% of the total value (compared with 54% in 2017), followed by fraud by misappropriation (41%, down from 42% in 2017).

Credit transfer fraud is relatively evenly broken down between the various payment channels: transfer initiation from online bank accounts (via the internet or a mobile phone application) was still the most affected channel (up from 38% to 42% in 2018 in terms of total fraud value), while the remainder was divided between secure telematic channels (37% compared with 31% in 2017) and paper-based transfers such as letter or fax, which declined significantly with 22% of total fraud value compared with 31% in 2017. However, given that the use of paper-based transfers is now very limited, accounting for less than 10% of issued credit transfers in terms of value, its associated fraud rate declined only slightly to 0.0010% from 0.0011% in 2017 and is higher than that for credit transfers issued via electronic channels (0.0004%).

C25 Value-based breakdown of credit transfer fraud, by geographical area

(%)

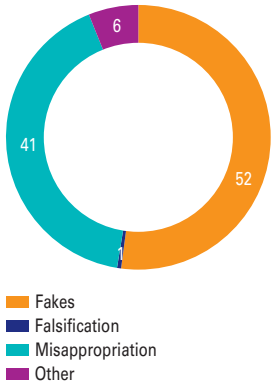


Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

Credit transfer fraud encountered	Preventive measures
In 2018, **misappropriation-type fraud through social engineering techniques** mainly took the following forms: • **CEO fraud**: the fraudster impersonates a senior company executive to trick an employee into making an urgent, confidential credit transfer to a foreign account. To do this, the fraudster uses information that he or she gathers on the company and its executives via the internet or directly from the company itself. • **Bank account details fraud**: the fraudster impersonates a supplier, lessor or any type of creditor and falsely informs the customer, tenant or debtor that there has been a change in the bank account details that they use to pay their bills, invoices or rent, misappropriating the funds for themselves. The fraudster sends the new bank details by email or by post in a properly worded letter from the creditor. • **Technical support scams**: the fraudster impersonates 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. • **Bank advisor scams**: the fraudster uses the bank advisor's telephone number, generally in his or her absence, and contacts the customer to extract information.	**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 service providers to **inform and heighten awareness** among companies and individuals.
In 2018, **cyber-attacks** essentially targeted online banking websites and telematic channels, such as the EBICS system (the Electronic Banking Internet Communication Standard – an interbank communication channel through which businesses can exchange automated data files with banks), and were mainly perpetrated using two methods. • **Malware**: such as Trojan horses, spammers, viruses, etc., which infect a person's or a business' computer without their knowledge when they open a fraudulent email, browse corrupted websites or connect 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. Therefore, when the customer logs into his or her online bank account, the malware can retrieve the ID and password that he or she has entered and use them to log in, 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 emails 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 "smishing" via SMS.	**Deploying a strong authentication system to approve credit transfer orders** entered online. **Triggering time delays or strong customer authentication when new transfer beneficiaries are added** on online banking sites. **Setting maximum transfer ceilings** on online banking sites. **Providing secure solutions to customers** to scan for malware-type infections on their terminals. **Implementing 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 service providers to **inform and heighten awareness** among businesses.

C26 Value-based breakdown of credit transfer fraud, by fraud type

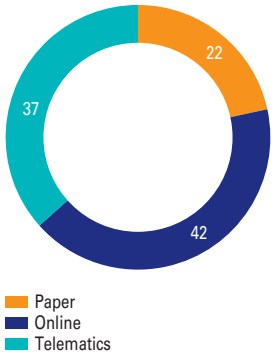
(%)



Source: Observatory for the Security of Payment Means.

C27 Value-based breakdown of credit transfer fraud, by transmission channel

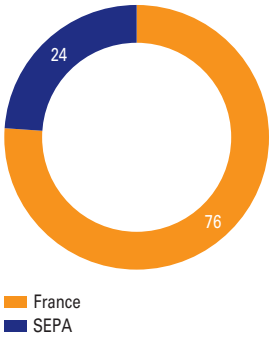
(%)



Source: Observatory for the Security of Payment Means.

C28 Value-based breakdown of direct debit fraud, by geographical area

(%)



Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

Main cases of fraud in 2017 and preventive measures

As in 2017, social engineering[8] and cyber-attacks through malware and phishing were the main techniques used in credit transfer fraud in 2018. The upturn in the number of phishing cases observed in 2017, following a decline in 2016, continued in 2018. Improvements to cyber-attack detection mechanisms should therefore be stepped up to counter fraudsters whose increasingly sophisticated emails can more easily deceive account holders.

2.5 Direct debit fraud

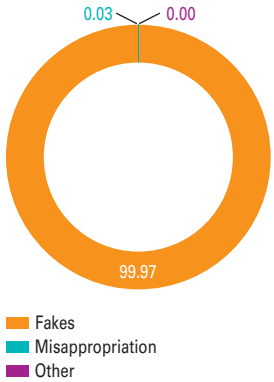
Overview

In 2018, fraud relating to direct debit payments to be debited from accounts held in France increased sharply by 544% from EUR 9 million in 2017 to EUR 58 million and thus returned to the kind of levels observed in 2016 (EUR 40 million) prior to the substantial 78% year-on-year drop. Therefore, given the growth in payment flows, the direct debit fraud rate rose to 0.0035% in 2018 from 0.0006% in 2017, or the equivalent of one euro of fraud for around every EUR 28,184 worth of issued direct debit instructions (compared with one euro of fraud for every EUR 180,000 in 2017). The average value of a fraudulent direct debit transaction amounted to EUR 188 in 2018 compared with EUR 340 in 2017.

8 Social engineering refers to the psychological manipulation of people into performing actions or divulging confidential information.

C29 Value-based breakdown of direct debit fraud, by fraud type

(%)



Source: Observatory for the Security of Payment Means.

The methodological work undertaken in 2017 to categorise fraudulent direct debits that means that data is better measured and assigned, confirms that a large majority of the fraud is attributable to fake direct debit instructions (i.e. the origination of direct debit instructions without a mandate by false creditors), which account for 99.97% of total fraud value.

Lastly, there has been an upturn in domestic direct debit fraud on cross-border transactions between SEPA countries, which until recently had been marginal (24% in 2018 compared with 1% in 2017). Domestic transactions thus accounted for 76% of direct debit fraud in 2018, down from 99% in 2017.

Main cases of fraud in 2018 and preventive measures

Fake direct debits – the illegitimate issuance of direct debit instructions without any authorisation or underlying economic reality – constituted the main fraud technique used to target direct debits in 2018. An increase in these fake direct debits initiated from France to cross-border SEPA countries was thus noted. Two other fraud techniques were also observed, but to a lesser extent: misappropriation by a fraudster of third-party identities and IBANs[9] for subscription to services; and fraudulent collusion between a creditor and a payer.

9 International bank account numbers.

Direct debit fraud encountered	Preventive measures
Illegitimate issuance of direct debit instructions (fake direct debits): a false creditor registers as the originator of a direct debit instruction with a payment service 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, which is assigned once its payment service provider is sure of its ability to do so. **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, which is assigned once its payment service provider is sure of its ability to do so.

3 Technology watch

3.1 The security of offline payment methods

Introduction

Since the first smartcards were introduced in the early 1990s, trends in the development of payment methods have stood out for their use of emerging technologies, such as online, contactless and mobile payments. As a consequence of these changes, payment means are more and more connected, guaranteeing real-time communication between the various parties involved in the transaction: the payer, the beneficiary and their respective account-holding institutions.

However, this evolution must not hide the persistent use of non-connected (offline) payment methods, particularly those that are paper-based: cheques, credit transfers arranged using a slip, order or subscription forms paid by manually completing card number information, etc. These payments meet different needs; both the needs of customers, who are not necessarily adequately equipped to make dematerialised payments, and needs related to specific use cases, which, from the point of view of the parties involved in the transaction, may be better suited to these offline payment methods.

These payment initiation methods, which have thus escaped the digital transformation of payment solutions, now only account for a very small proportion of transaction flows: less than 8% of the volume of transactions issued in 2018 and 11.3% of their total value (7% and 3%, respectively, for cheques alone). However, they are still the preferred target of fraudsters, who from long experience are fully versed in their vulnerabilities, and therefore accounted for 47.9% of total fraud value in 2018.

However, while payments issued electronically are subject to a gamut of security requirements laid down in the regulations, particularly the second European Payment Services Directive (PSD2),[1] and that are intended to combat fraud through the principle of strong customer authentication, offline payments are omitted from these provisions and by definition cannot benefit from these security features.

This study provides an overview of these offline payment methods and notes the various parameters that can contribute to their security.

Overview of offline payment methods and specific associated risks

Scope

This study covers payment means as defined by the *Code monétaire et financier* (French Monetary

1 The contributions of PSD2 in terms of security were the subject of a dedicated Observatory study (see Chapter 1 of the 2017 *Annual Report of the Observatory for the Security of Payment Means*: https://www.banque-france.fr/en/liste-chronologique/annual-activity-report).

and Financial Code) for which the issuance of payment orders relies on offline arrangements, i.e. arrangements that do not ensure an automated and real-time connection between the issuer of the order and the payment service provider (PSP) responsible for executing it. This scope encompasses payments by cheque, by transfer and by card (using paper-based methods or by fax, email or telephone) and excludes the two following methods in particular.

• SEPA (Single Euro Payments Area) direct debits, because, irrespective of the way in which the payer's approval is obtained (which can involve a paper-based mandate), creditors' payment orders are systematically issued to their PSP online. (The Observatory published a thorough analysis of the risks and security measures associated with direct debits in its 2017 Annual Report.)

• Vouchers issued by public and private bodies giving the holder right of access to certain services: while these vouchers are very often incorrectly called "*cheques*" in France (*chèque restaurant*, *chèque énergie*, *chèque voyage*, etc.), they are neither "cheques" nor even means of payment as defined by the regulations and do not fall within the remit of the Observatory.

The cheque and all its different forms

Cheques are generally defined as documents whereby a person, the cheque issuer or **drawer**, instructs a credit institution, the **drawee**, to pay on demand (at sight) a certain sum to a third party, the **beneficiary**, or to the drawer.[2] Although cheques have been frequently revised and standardised to help banks automate their processing and management, it is still the oldest cashless means of payment.

This payment instrument is governed by a complex legal regime codified in Book I, Part III of the French Monetary and Financial

2 See (in French) "*Entreprises en difficulté*", Pérochon (F.), 9th edition, *Manuel* collection, *Librairie générale de droit et de jurisprudence* (LGDJ), 2012; and *Instruments de crédit et de paiement*, Bonhomme (R.), 9th edition, *Exercices pratiques* collection, LGDJ, 2015.

Box 1

Cheque status and milestones

Cheques were introduced in France under the Second Empire with the creation of the major deposit banks; the first text governing their use was a law of 14 June 1865.

Later, the Convention providing a Uniform Law for Cheques enacted in Geneva on 19 March 1931 was introduced in France by decree implementing the law of 30 October 1935. This Convention is considered to be the benchmark in the field.

It was the source of the provisions of the *Code monétaire et financier* (French Monetary and Financial Code) that regulate cheque use in France.

Code, entitled "*Les instruments de monnaie scripturale*" (cashless payment instruments).

In accordance with Article L. 131-2, paragraphs 1 and 2 of the Code, a cheque must bear the word "cheque" and an "explicit instruction to pay a given sum". This instruction is drafted as follows: "*Payez contre ce chèque non endossable sauf au profit d'une banque ou d'un établissement assimilé la somme de...*" ("Pay against this cheque, non-transferable except for the benefit of a bank or similar institution, the sum of..."). Failing this, any payment document that does not bear these particulars, even if the other mandatory information is present (see the paragraph entitled "The cheque" in the section on "Protecting offline payment methods" below), is not a cheque.

The formulations used (the paper document) to allow the account holder to instruct his or her bank to pay the given amount to the beneficiary, are standardised, printed by banks and issued to their customers. They are called "pre-printed forms" (*formules pré-marquées*), and more commonly "cheques". This printed format, which originates from the convention of Geneva, was made compulsory by the decree of 5 November 1998 approving and making mandatory the application of French standards,[3] more precisely French standard NF K11-111, "Banking – Cheque-form for cheques payable in France". The purpose of this standard is to define the form on which cheques are to be written and issued.

There are two characteristics of the cheque format that appear essential, even though they are not compulsory in terms of cheque validity.

• The mention of "*Payez contre ce chèque* ***non endossable sauf au profit d'une banque ou d'un établissement assimilé la somme de...***" is intended to prevent the cheque being transferred to a person other than a bank or similar institution. However, it does not prevent the free circulation of a cheque prior to the designation of the beneficiary, although this type of usage is not recommended for security reasons.

• **Crossing of the cheque** by the bank, and more precisely with two parallel lines pre-printed on the cheque, which in compliance with Article L. 131-45 of the French Monetary and Financial Code, means that a crossed cheque "may be paid by the drawee only to a banker, a payment institution, the head of a Postal Cheque Centre or a customer of the drawee". In compliance with this provision, crossed cheques can only be cashed by the beneficiary's bank. Equally, an account-holding institution may only accept a crossed cheque from its customer or another bank or similar institution, and therefore may only cash the cheque on behalf of these persons.

The format most often made available to customers by their bank is the chequebook. For professionals and businesses, it can also take the form of a cheque-letter. In addition, in specific situations, customers can arrange for banker's drafts to be issued.

• The **cheque-letter** is an automated cheque printing solution offered by banks to corporate clients that issue large volumes of cheques. Using this solution, clients can also have text printed to accompany the cheque and vary the mentions on the cheque. However, prior to using this format,

3 Order published in the *Official Journal of the French Republic*, No. 264, 14 November 1998.

clients must subscribe to certain conditions within the framework of an agreement between the bank and the company.

• **Banker's drafts** are issued by banks on the customer's request in very specific, and generally high-value, cases such as payments to purchase a vehicle or settle professional fees. Banker's drafts also have additional security features.

Cheques (including their variants) are bank instruments whose issuance, by law, is the exclusive domain of credit institutions, which are uniquely authorised, under Article L. 131-1, to "keep accounts on which cheques may be drawn". Consequently, other categories of payment service providers (payment institutions and electronic payment institutions) are not allowed to issue this type of payment means.

Cheque processing circuits

Historically, cheques were exchanged manually between banks for clearing purposes on a daily basis, in clearing houses made available by the Banque de France (Article L. 131-34 of the French Monetary and Financial Code). In practice, each bank presented the different cheques it was responsible for cashing on the other banks at the clearing house. The amount a bank owed to each bank was offset against the amount it was owed by each bank in order to generate a balance. The clearing house then credited or debited the balances to each bank's account through the Banque de France. The paper cheques were thus passed between the banks during sessions held in the clearing houses.

At the time of the changeover to the euro, banks wanted to modernise the system and opted to dematerialise the interbank clearing systems process through the implementation of the image clearing system (ICS)[4] that replaced the clearing houses as from the end of June 2002.[5] Since the completion of this project, payment transactions by cheque are settled as a matter of principle via the ICS in accordance with the provisions of the *Comité de la réglementation bancaire et financière* (CRBF) Regulation No. 2001-04 of 29 October 2001 on cheque clearing. At the same time, in certain cases, and particularly when large sums are involved, cheques are exchanged physically between the collecting bank and the paying bank. In addition, these institutions may also exchange copies of cheques for a variety of reasons (inspections, requisitions, etc.).

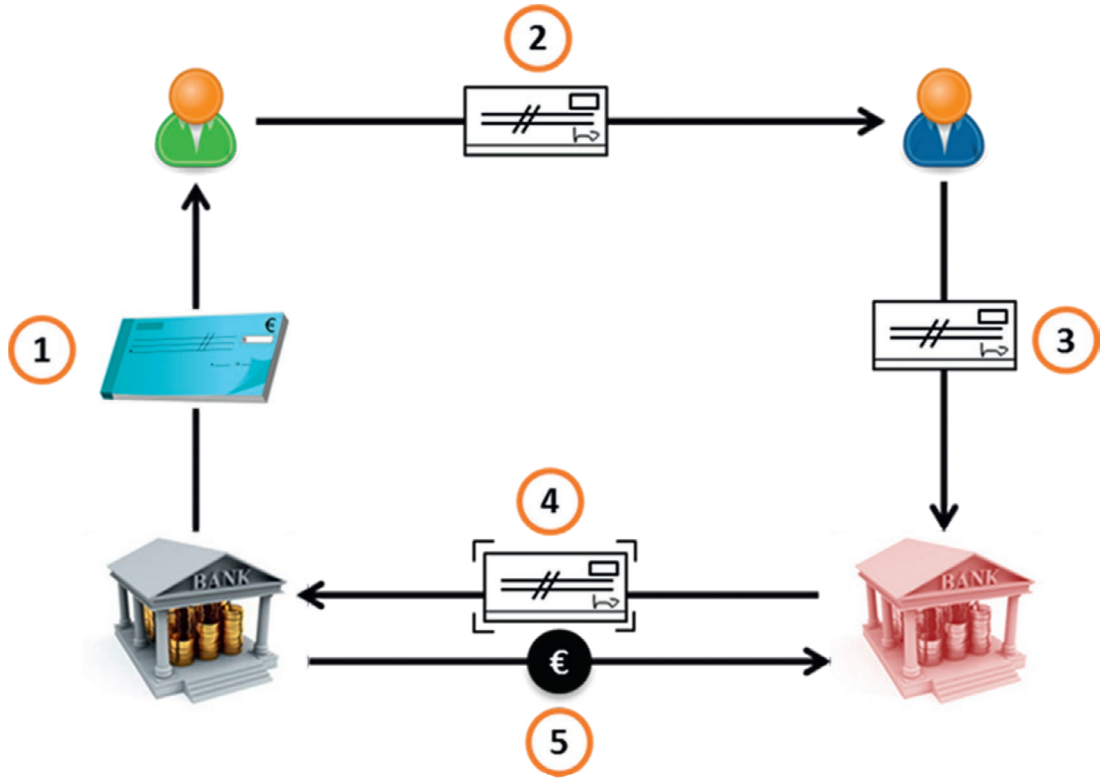
Dematerialising the presentation of cheques for collection between banks has improved customer service and shortened cheque processing times. This four-party payment system is presented schematically in the diagram in Box 2.

4 See the 2002 *Annual Report of the Banque de France* (https://www.banque-france.fr): "The exchange of truncated cheques aims to replace the physical exchange of paper cheques in clearinghouses with the exchange of electronic recordings of the magnetic strip on cheques, plus the payment amount, through the SIT (*système interbancaire de télécompensation*) teleclearing system."

5 Date of completion of the dematerialisation of interbank exchanges of payment means (see "*Le système interbancaire de télécompensation*", *Bulletin de la Banque de France*, No. 107, November 2002).

Box 2

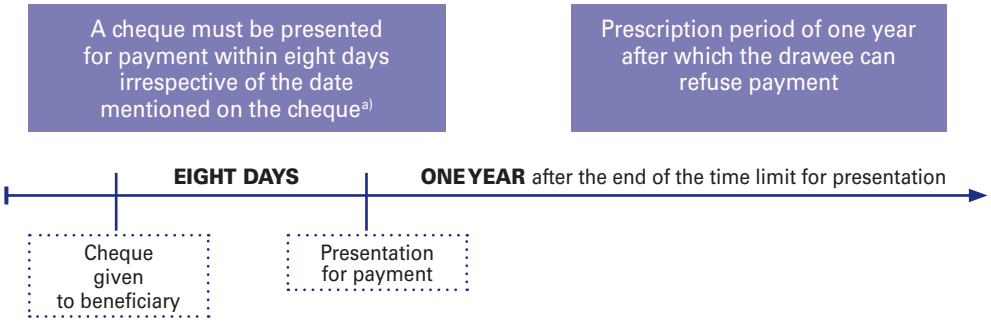
Interbank cheque processing system



1. Prior to payment (as a general rule), the payer is issued a chequebook by its bank.
2. The payer (drawer) completes the cheque and gives it to the beneficiary in settlement of an amount.
3. The beneficiary deposits the cheque at his or her bank, usually with a remittance slip or via a self-service machine.
4. The beneficiary's bank dematerialises the cheque and transmits the cheque image to the payment clearing system.
5. The payer's bank then settles the funds due with the beneficiary's bank.

Box 3

Statutory time limit for cashing cheques



a) This time limit can be extended to 20 days or 70 days depending on whether the cheque is issued in Europe (outside metropolitan France) or outside Europe, or can be extended in cases of *force majeure*.

Presentation period

Once the cheque has been drawn and issued (i.e. once the cheque has been presented to the beneficiary), the beneficiary may present the cheque for payment irrespective of the date mentioned on the cheque. Indeed, a post-dated cheque can be presented and therefore legally paid even before the presumed date of issue.Therefore, post-dating a cheque is not recommended as it has no impact on when the cheque can be presented for payment.

The rules for presentation for payment set a time limit of eight days following the issuance of the cheque or the presumed issuance date (Article L. 131-32, paragraph 1, of the *Code monétaire et financier*, the French Monetary and Financial Code), although this can be extended for a cheque issued outside metropolitan France to either 20 days for a place of issue in Europe or 70 days for a place of issue outside Europe. Although in cases of *force majeure* these time limits can be extended under certain conditions, the beneficiary is advised to present the cheque for payment as quickly as possible.

Prescription period

The presentation period should not be confused with the prescription period for actions of recourse brought by the bearer of the cheque against the drawee. In accordance with Article L. 131-35 of the French Monetary and Financial Code, a cheque presented after the time limit for presentation should nonetheless be honoured by the drawee for a further one-year period. After that, the drawee may invoke the prescription referred to in Article L. 131-59 of the French Monetary and Financial Code and refuse payment.

Cheques use is less common but remains popular in specific situations

Statistics on the use of cashless payment means show that cheques have been in gradual decline for more than 15 years, both in terms of transaction volumes and value. Nevertheless, their use continues to be widespread in France, where in 2018 it accounted for 7% of payment transactions – 1.7 billion issued cheques, down 9% year on year – for a total value of EUR 891 billion (down 11% compared to 2017). The cheque is now the fourth most used means of payment in terms of transaction volumes after being gradually overtaken by cards, then direct debits and credit transfers, giving up the number one position it held at the beginning of the 2000s.

However, certain business practices contribute to the cheque's longevity, as it offers the possibility to:

- pay substantial sums of money (in 2018, the average value of a cheque payment was EUR 510 compared to only EUR 43 for bank cards), particularly at the point of sale due to the spending limits placed on payment cards;
- spread a payment across several instalments, by giving several cheques to the creditor;
- agree with a creditor on a date to cash the cheque (the case of "deferred cheque transactions" carried out by certain merchants);
- pay without first having the beneficiary's bank details;
- attach details of the services or reimbursements made to the payment (see cheque-letters);
- use the cheque number to easily identify payments made in companies' accounting software.

On the other hand, given the risk of non-payment and its vulnerability to fraud, merchants can elect to refuse all payments by cheque, provided that they provide clear, advance notification to customers prior to purchase, i.e. by displaying the terms of payment at the entry to the point of sale.

Furthermore, there are certain situations that may currently force consumers or businesses to use cheques or cash, particularly for the payment of services provided by tradespeople or professionals not equipped with card payment terminals, or the payment of goods and services to itinerant retailers at markets or fairs, for example, or to give a security deposit when leasing premises or renting seasonal property. The work undertaken in this respect within the *Comité national des paiements scripturaux* (CNPS, National Cashless Payments Committee) is intended to promote credible alternative card-payment solutions and also SEPA instruments, such as the instant credit transfer, which will need time to be widely adopted.

In addition, cheques are still offered as gifts at weddings or birthdays, for example, because the people receiving them can use the money as they wish, unlike gift cards, which, while certainly more practical, are generally accepted by a limited number of point of sale and online retailers.

Lastly, very small companies also contribute by issuing large volumes of cheques: research by the CNPS[6]

6 See the 2016 CNPS activity report (*https://www.banque-france.fr*).

found that a quarter of companies with less than ten employees would use cheques for more than half of their transactions, and that this proportion was still 14% for small and medium-sized companies with 50 to 249 employees.

A vulnerability to fraud

Cheques may well only be the fourth most used cashless means of payment but they have become the most used means of payment for fraudulent purposes in France, with an annual fraud value that increased to EUR 450 million in 2018. The fraud rate for cheques steadily increased from 2016 to 2018 to 0.0505%, or one euro of fraud for every EUR 1,980 worth of payments. Cheques thus account for 43% of the value of total fraud on payment means while accounting for only 7% of transaction volumes.

Despite the innovations that banks have brought to bear on handling processes, cheques are still an exclusively paper-based payment instrument, with their status under the convention of Geneva restricting any possibility of full dematerialisation; thus, in contrast to other means of payment, cheques cannot be digitised and their format remains relatively unchanged. Generally, they are always sent out in the form of a "chequebook" of between 20 to 50 cheques, which represents 20 to 50 opportunities for fraud in a very short time if it is lost or stolen, often even before the account holder becomes aware of it. Moreover, a valid cheque intercepted by a fraudster can be falsified using a variety of procedures such as scratching, over-writing or erasing, or rewriting or adding information on the cheque. More sophisticated techniques such as kiting or that are intended for money laundering purposes have also been observed.[7]

"Offline" credit transfers

Credit transfers are payment services provided by the institution managing the payer's payment account, which consist in crediting the payment account of a beneficiary by way of a one-off transaction (single transfer) or a series of transactions (recurring transfer or standing order) from the payer's payment account, based on instructions issued by the payer or his or her authorised representative.

Credit transfer methods

The main channels for issuing credit transfers rely on online interfaces that ensure a direct connection between the customer and his or her account-holding institution:

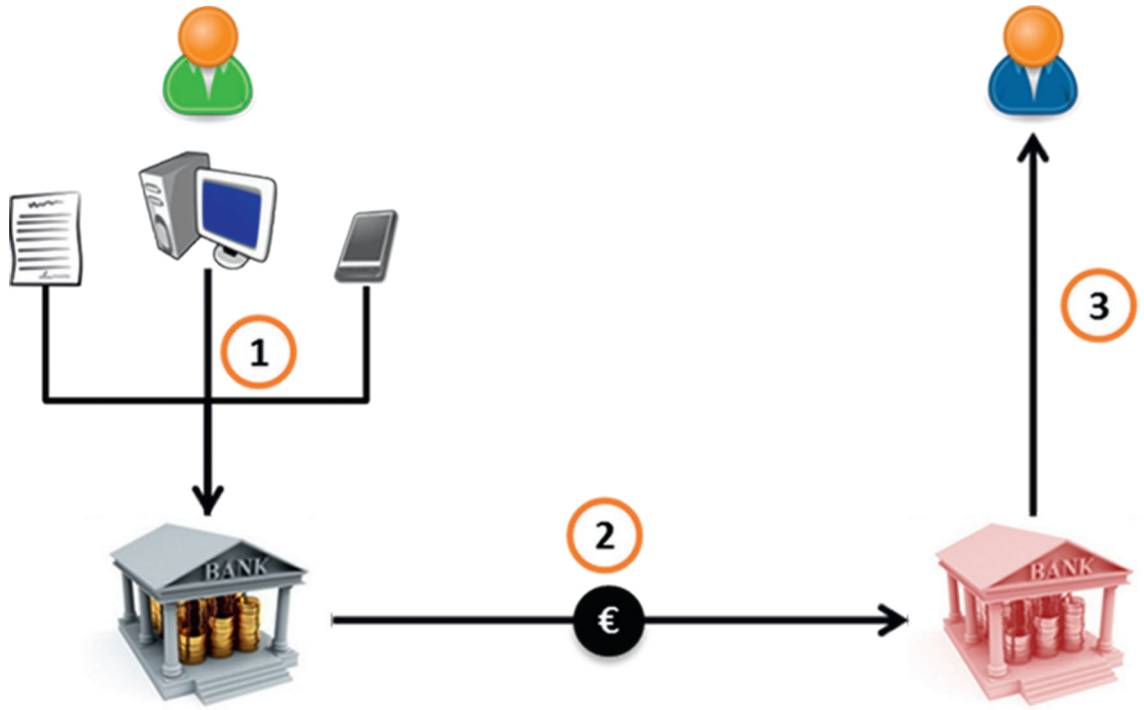
- the automated transmission of files containing several payment orders is used mainly by business customers to pay salaries and pensions or for supplier services and accounts for the majority of transfers issued in France, both in volume (64%) and in value (58%);

- the use of online banking interfaces to issue individual credit transfer orders, which accounts for 33% of issued transfers in volume and 32% in value.

7 These different methods of cheque fraud are presented in Chapter 2 of the 2017 OSMP Annual Report (*https://www.banque-france.fr/sites/default/files/medias/documents/annual-report-2017-osmp2017-gb-20181108.pdf*).

Box 4

The SEPA credit transfer process



1. The payer, account holder or authorised representative draws up the payment order, specifying the account to be debited, the account number or IBAN (International Bank Account Number) to be credited, the amount, the date(s) and if necessary the frequency of the transaction, and transmits the order to its account-holding institution, which debits the payer's account with the amount.

2. The payment order is exchanged through interbank payment circuits, leading to the payment of the specified funds to the beneficiary's account-holding institution.

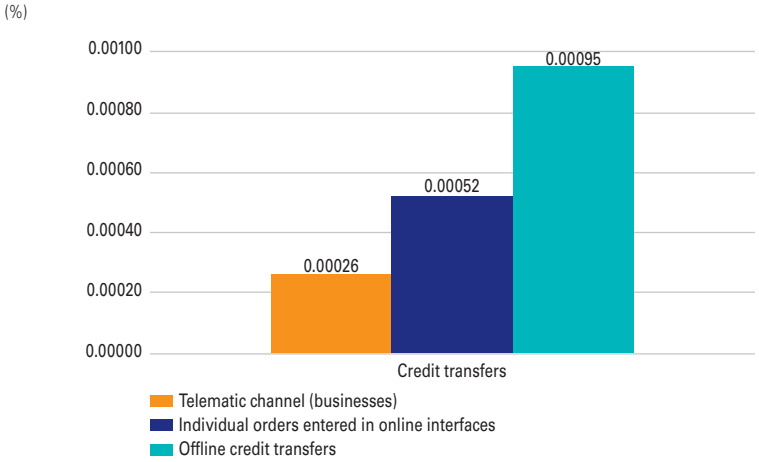
3. The beneficiary's account-holding institution credits the receiving account identified in the payment order.

Credit transfer orders issued "offline" thus account for a very small share of French credit transfers, with 3% of the number of transactions and 9% of exchanged amounts. They are carried out through different channels:

- making orders by telephone or through a branch;
- transmitting credit transfer orders or slips by fax, post or email.

These channels have in common that the account-holding institution is required to re-enter the payment instructions, carried out either by the customer's usual point of contact (counter, advisor, branch) or by a back-office customer transactions service.

C1 Credit transfer fraud rate by initiation channel



Source: Observatory for the Security of Payment Means.

Offline credit transfer fraud

As a reminder,[8] credit transfers registered the lowest rate of fraud across all payment means available to individuals with a fraud rate of 0.0004%, or one euro for every EUR 250,000 paid. Credit transfer fraud is relatively evenly shared between the various channels used by this payment instrument despite offline credit transfers accounting for a very small proportion of issued transfers. The fraud rate for offline credit transfers thus amounts to 0.0010%, which is almost four times greater than the overall fraud rate for this payment method, and is the equivalent of one euro of fraud for every EUR 100,000 paid. Total annual fraud amounted to EUR 21 million.

Fraud on offline transfers can be carried out using two main types of techniques common to all credit transfer methods: (i) the fraudster issues false orders, stealing the identity of the holder of the debited account; and (ii) the fraudster uses social engineering manipulation techniques to trick the account holder into issuing an illegitimate credit transfer order.[8]

"Offline" use of payment cards

Offline card payments are generally referred to as MOTO payments (for mail order/telephone order) as they are carried out through a communication channel such as mail, fax or telephone (spoken exchange). As a general rule, there is no direct contact between the merchant and the payment card or

8 See Chapter 2 of the 2017 OSMP Annual Report (*https://www.banque-france.fr/sites/default/files/medias/documents/annual-report-2017-osmp2017-gb-20181108.pdf*).

its holder at the time the payment is initiated, which has a number of consequences.

• From the payer's point of view, payment information (card number and expiry date) is transmitted through a generally unsecured channel and in the majority of cases has to be processed manually. The cardholder's signature is not required, and receipts do not have to be printed and issued.

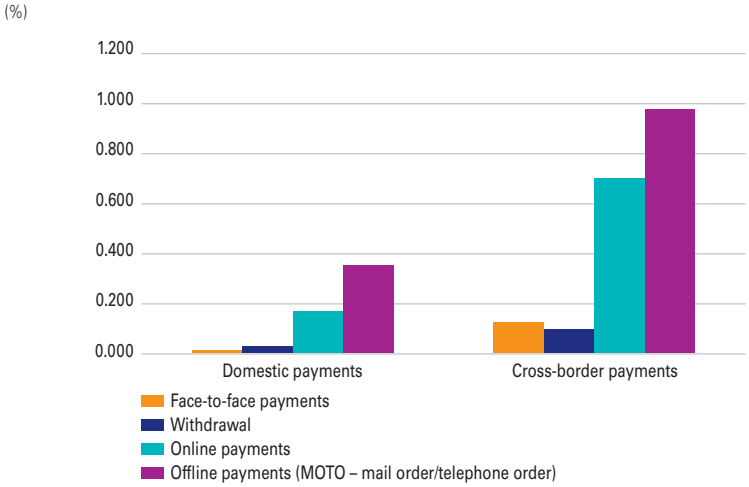
• From the beneficiary's point of view, the company receiving the orders by mail, fax, telephone or other offline means can initiate the transactions either through the activation of the MOTO function if it has a terminal or by transmitting the information to its account-holding institution, either by entering the payment information on its website or by sending files that contain this information via a secure interface or another channel such as fax or mail.

This initiation method is governed by specific card payment system regulations: the Payment Card Industry Security Standards Council (PCI SSC)[9] has published an information supplement[10] outlining security principles for merchants and service providers to ensure they comply with the standard's requirements.

However, despite these security requirements, the fraud rate for offline card payments is far higher than for other card payment methods. French cardholders endured EUR 28.5 million in offline card payment fraud in 2018, accounting for 7.1% of total card fraud, even though these transactions make up only a tiny proportion of the card payments made (0.5% and 0.8% in volume and value, respectively).

In particular, as market players gradually ensure that they comply with the security requirements for online payments (EMV[11] smart card, PCI DSS[12] standards for e-commerce), card fraud has shifted to MOTO payments, particularly cross-border transactions: two

C2 Fraud rate for offline card payments (French cardholders)



Source: Observatory for the Security of Payment Means.

9 The Payment Card Industry Security Standards Council is the leading international body for the promotion of payment security standards, with members from the main card payment systems.

10 See https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf

11 Europay MasterCard Visa.

12 The Payment Card Industry Data Security Standards are a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

thirds of the MOTO fraud affecting French cardholders involves international transactions.

In addition, MOTO payments provide fraudsters with significant opportunities to compromise card numbers, which they then reuse to make other types of fraudulent transactions, including online payments.

Protecting offline payment methods

The cheque

Security provisions from a user perspective

The security measures taken with regard to cheques are partly laid down in the provisions of the French Monetary and Financial Code, which regulate the creation of a cheque. Thus, if a cheque is to be considered valid, certain **mandatory information** is required, stipulated in Article L. 131-2 of the Code:

- the word "cheque" inserted into the text of the instrument and expressed in the language used for the wording of that instrument;
- the explicit instruction to pay a given sum;
- the name of the person or entity that must pay, known as the drawee;
- an indication of the place where the payment must take place;
- an indication of the date and the place where the cheque is drawn;
- the signature of the person issuing the cheque, known as the drawer.

The first four points are pre-printed by the banks on the cheques sent to the customer and therefore present no difficulties for the user (payer or beneficiary). However, the payer should be extremely cautious when completing the rest of the cheque to avoid any attempt at fraud by a third party entering into possession of the cheque (see Appendix 2).

Furthermore, the law **prohibits the addition of certain statements** such as a date for presentation for payment or any stipulation of interest (Articles L. 131-31 and L. 131-8 of the French Monetary and Financial Code). These statements are simply deemed to not be written and therefore null and void, which implies that only the mandatory information is thus recognised as valid.

Lastly, **optional information** can be included alongside the mandatory information.

- The pre-printed elements on cheques issued by banks to their customers, which therefore pose no difficulty (the statement prohibiting the transfer of the cheque to another person other than a bank or similar institution and the crossing of the cheque – see above – which are not required for the validity of the cheque but are a consequence of the wording of Articles L. 131-4 and L. 131-44 of the French Monetary and Financial Code).

- Designating the beneficiary may seem obvious, but it must be expressly stated as a cheque may be payable to a designated person or the bearer (Article L. 131-6 of the Code). A cheque with no indication of the beneficiary is considered a bearer cheque. In addition, a payer (drawer) can write out a cheque for self-withdrawal, making it payable to "Self", or can designate

him or herself as the beneficiary by name in order to transfer funds from one account to another held by the same person in a different bank (Article L. 131-7 of the Code). Nevertheless, designating the beneficiary is still important as it contributes to combating cheques drawn by fraudsters usurping other people's identities.

• The statement certifying that the drawer has adequate funds to cover the cheque at the time of certification (Article L. 131-14 of the Code) must comply with the certification procedure referred to in Article R. 131-2.

Article L. 131-14 states that the drawee can exercise the right to replace the certified cheque with a **banker's draft**. This has become commonplace as it is advantageous

Box 5

Banker's draft

A banker's draft is a cheque issued by a bank drawn on its own funds or those of a correspondent bank to ensure the beneficiary receives payment at any point during its validity. When the banker's draft is issued, the issuing bank debits the account of the requesting customer after checking for adequate funds and blocks that sum until the draft is cashed by the beneficiary.

Practically speaking, the presence of a high-quality watermark comparable to those on bank notes distinguishes a banker's draft from an ordinary cheque. This serves as a guarantee of authenticity.

• The watermark is standardised, with the same pattern and size for all French banks.

• The watermark provides a high degree of protection as it is visible when held against the light and takes up a substantial part of the banker's draft's surface.

• *CHEQUE de BANQUE* (banker's draft) is printed on the back of the cheque and edged above and below by two striped banners.

• This mention is flanked on both sides by two maidens sowing seeds, with the darker and lighter tones in the image on the left reversed in the reflected image on the right.

to the beneficiary who can benefit from a payment guarantee that is not limited to eight days but to one year because the bank covers the cheque amount.

In the case of a large value transaction such as the sale of a car, sellers may sometimes demand payment by banker's draft. After carrying out the usual checks (mandatory and optional information common to both ordinary cheques and banker's drafts and information specific to banker's drafts), the seller should also contact the issuing institution to ensure that the banker's draft is authentic, without using the telephone number on the cheque (by referring to a telephone book or online directory, for example). If doubts persist, it is recommended that the beneficiary holds on to his or her property and postpones the sale.

Precautions for users

In order to combat fraud, precautions must be observed at all levels of the cheque payment process and by all those involved, including bearers, merchants, banks, etc.

The account agreement signed by the customer when opening a bank account must mention the payment means that will be made available. The **terms and conditions of delivery** of a chequebook to a customer may vary from bank to bank and must be set out in the account agreement (whether chequebook renewal is automatic, whether it is sent as an ordinary letter or by registered delivery, whether it has to be collected at a branch, etc.). Customers must also be informed of the precautions to be taken in the event that chequebooks are not received within a certain period of time, particularly if renewals are automatic. Equally, the bank must insist that all unused cheques be returned upon closure of an account (Article L. 131-71 of the French Monetary and Financial Code). Consequently, the **return procedures** must be brought to the customer's attention in order to prevent unreturned cheques from being used for fraudulent purposes.

The customer must also comply with the **safekeeping guidelines** for cheques and chequebooks. In addition to simple common-sense rules such as not leaving chequebooks in plain sight or in unsecured locations (car glove boxes, on top of furniture, etc.), banks generally give their customers more specific advice.

Moreover, different **precautions** should be taken by the payer (drawer) and the beneficiary when cheques are used to settle a transaction.

When the cheque is written, the **drawer** should:

- fill in the cheque, completing any information that is not already pre-printed (the payment amount, beneficiary, date – day/month/year – and place where the cheque is drawn, signature), legibly, leaving no room for interpretation by the drawee;

- limit the risk of the cheque being modified by using a ballpoint pen with indelible black ink and avoiding leaving free space before and after the manually completed details;

- carry an official document in case proof of identity is needed (certain

merchants or high-value cheques may require two);

- follow several recommendations with regard to the amount indicated on the cheque (Article L. 131-10 of the French Monetary and Financial Code):

  – by law the amount does not have to be written in words and numbers and the practice of entering the amount twice is declining due to the expansion of computerised cheque filling systems that only print numbers; however, filling in both lines limits the potential for falsification and thus provides additional protection for the drawee,

  – if there is a difference between the amount written in words and the amount in numbers, the amount written in words takes precedence,

  – if the amount is written several times in words or several times in numbers and there is a difference between the two, the lowest amount is accepted,

  – the use of "blank cheques" where the amount is not filled in until the cheque is cashed, is dangerous and should not be envisaged under any circumstances, even if the beneficiary is a close relative of the drawer (the blank cheque could be lost or stolen, for example),

Box 6

New fraud and scams based on confidence tricks and digital technologies

The Observatory urges all private individuals and companies to be extremely vigilant with regard to increasingly common scams that involve fraudsters using the internet to encourage their victims to cash fraudulent cheques. The scam works in different ways.

- Sending a cheque in payment for a service (such as an online purchase) for an amount greater than that required and asking the beneficiary to reimburse the excess by credit transfer. In this situation, it is recommended that the seller delay sending the goods and arranging the credit transfer for a few days until he or she is sure that the cheque will not be rejected, or even cancel the transaction.

- Recruiting people via social networks to cash cheques on behalf of a third party (for a variety of reasons such as banking difficulties encountered by the requester, bank account held abroad, cheque-cashing unavailable, etc.) and then send the sum (or another amount) to the third party by credit transfer. In this type of situation, those participating in the scam, who may have been lured by the prospect of earning a commission, are contributing to a money laundering scheme while becoming victims of the fraud or even accomplices themselves.

– when the cheque is completed automatically by an in-store cash register system, the customer must check that all the information is correctly entered and that the amount corresponds to the amount due and is clearly legible.

When the cheque is received in payment, the **beneficiary** should:

• thoroughly verify the cheque, including the amount in words and numbers, the signature, the date and the place where the cheque was drawn;

• check the payer's proof of identity, and compare signatures;

• refuse any request to add mentions to the cheque, such as a time limit or other condition for cashing the cheque;

• endorse the cheque with a handwritten signature on the back;

• deposit the cheque within days of receipt to prevent it being lost or stolen, and possibly falsified before being cashed by a fraudster.

Specific precautions applicable to merchants receiving cheques

Most cheque receiving merchants, particularly in the mass retail sector, use an automatic cheque filling system, which may be imperfect and increase the risk of falsification, given that in some cases:

• the amount is written on the cheque in numbers only;

• blue ink is used whereas banks recommend the use of black ink;

• problems with printing (low or poorly distributed ink) or system settings mean that the information provided falls short of acceptable standards.

It is in the merchant's interest to apply these precautions, particularly by performing a thorough inspection, when accepting payments by cheque, and also when the merchant completes the cheque on the customer's behalf via an automatic filling system.

Merchants can protect themselves against irregular cheques by consulting the *Fichier national des chèques irréguliers* (FNCI, the national register of irregular cheques) via the Banque de France's official prevention service for unpaid cheques. Contracts can be arranged through the Vérifiance service at https://www.verifiance-fnci.fr. Merchants may also use other service providers that offer their own risk-analysis based payment guarantee service.

Merchants have the right to refuse payment for purchases by cheque for a variety of reasons.

• Cheques may not be accepted in general (the terms of payment must be clearly displayed at the entry to the point of sale).

• The conditions for accepting a cheque, such as providing proof of identity, have not been met.

• The merchant may deem the cheque irregular after using an expert verification system such as Vérifiance (see Box 7 below) or an alternative solution. The merchant consults the systems by simply scanning the coded line at the bottom of the cheque, and in return receives an assessment of the

Box 7

The national register of irregular cheques (FNCI)

The *Fichier national des chèques irréguliers* (FNCI, the national register of irregular cheques)[1] is an IT file managed by the Banque de France that comprises data submitted by the issuing banks.

It lists so-called "irregular" cheques, i.e. cheques that fall into one of the three following categories:

- cheques that are disputed due to loss or theft;
- cheques drawn on a closed account or on an account that is banned from cheque use;
- cheques identified as fake.

It can also be used to identify the fraudulent use of a chequebook: the *Information multichèques* alert warns when a large number of cheques have been drawn on the same account during a given period. It thus averts the risk of fraudulent chequebook use.

The FNCI can be consulted by:

- cheque beneficiaries subscribed to the Vérifiance (FNCI – Banque de France) service;
- any individual who wishes to know if the details of the account(s) they hold are registered and to verify any information that concerns them under the individual right of access.

1 For further information, see https://particuliers.banque-france.fr/fichiers-dincidents/les-trois-fichiers-dincidents-fcc-ficp-fnci/le-fichier-national-des-cheques-irreguliers-fnci

cheque's regularity, for example by code (Vérifiance uses a colour code system). Here again, merchants are required to inform their customers of the service employed (Vérifiance or other cheque guarantee solutions) by placing stickers in the windows or near the cash registers. Should a merchant refuse a cheque, he or she must provide justification for the refusal and clearly state the service used.

Precautions for banks

Before providing a customer with a chequebook, the bank must consult the *Fichier central des chèques* (FCC, the central cheque register) managed by the Banque de France, which lists all persons banned from issuing cheques (by banks or by court order) or from using a bank card.

As the drawee, before paying a cheque, the drawer's bank must verify that (i) no stop payment request has been made, (ii) the

Box 8

The central cheque register (FCC)

The *Fichier central des chèques* (FCC, the central cheque register)[1] is an IT file managed by the Banque de France that comprises data submitted by the issuing banks.

The FCC lists:

- people banned from having a chequebook because they issued a cheque when they had inadequate funds and have not rectified their situation;
- people whose bank card has been confiscated by their bank due to an incident related to its use;
- people banned by court order from issuing cheques.

The FCC can be consulted by:

- banks, which are required to do so before providing a customer with a chequebook and are free to do so before issuing another payment instrument or granting a loan;
- any individual who wishes to know if they feature on the register under the individual right of access (exercised by contacting the Banque de France).

1 For further information, see https://particuliers.banque-france.fr/fichiers-dincidents/les-trois-fichiers-dincidents-fcc-ficp-fnci/le-fichier-central-des-cheques-fcc

customer has adequate funds in his or her account, and (iii) all mandatory information is included on the cheque.

In addition, in accordance with Article L. 131-35 of the French Monetary and Financial Code, the drawer's bank must pay even after the presentation period expires and generally until the end of the one-year prescription period (see Box 3 above). However, the principle that the order to pay is irrevocable can be derogated if a **stop** is placed on the cheque, blocking the funds held by the drawee.

- This derogation allows the drawer, or even the bearer, to instruct the drawee not to pay a cheque presented for collection. The same article strictly limits the cases when a stop may be placed on a cheque to loss, theft or fraudulent use of the cheque, and the judicial reorganisation, receivership or liquidation of the bearer. Placing a stop on a cheque for any other reason would be considered unlawful and could lead to criminal sanctions.

- However, the justifications for placing a stop on a cheque are strictly interpreted by the courts. With regard to theft or loss, if the drawer intentionally issues a disputed cheque to a beneficiary, he or she cannot subsequently claim that it was taken against his or her will; nor can a loss or theft be invoked in the event that a cheque

is erroneously sent to a beneficiary for whom it was not intended. With regard to the fraudulent use of a cheque, the stop may be upheld in cases of cheque counterfeiting or falsification, and also when the cheque is obtained and used as a result of fraudulent activities.

• Lastly, it is important to note that stopping a cheque in the event of collective proceedings against the beneficiary is intended to prevent the beneficiary from cashing the cheque in the case of his or her divestiture.

All these cheque security rules that concern both users (drawers and beneficiaries) and banks are supplemented by a **cheque monitoring system** put in place by the Banque de France.

In accordance with Article L. 141-4 of the French Monetary and Financial Code establishing its mission to oversee cashless means of payment, the Banque de France ensures that cheques are secure and that the applicable regulations are pertinent. In order to carry out this mission, the Banque de France established the ***référentiel de sécurité du chèque*** (RSC, cheque security oversight framework) that includes a number of security objectives that institutions are required to meet.

This oversight framework revolves around an annual self-assessment by each cheque-paying or cheque-collecting institution of its compliance with the RSC security objectives, performed on the basis of answers to a questionnaire that defines the conditions for the objectives' implementation.

Box 9

Security objectives established in the cheque security oversight framework (RSC)

Nine security objectives are defined in the *référentiel de sécurité du chèque* (RSC, cheque security oversight framework).[1]

Objective 1: governance and organisation

Security governance aims to ensure that optimal, appropriate security measures are in place. The players [contributing to the cheque payment system] must have an official and regularly updated set of documents that define this governance framework and the organisation of cheque payment system security, and that cover all related activities, including those that are outsourced.

1 The cheque security oversight framework is publicly available (in French only) on the Banque de France website: https://www.banque-france.fr/sites/default/files/media/2018/03/13/cheque-referentiel-de-securite_v2017.pdf

.../...

Objective 2: risk assessment

Security management relies on the identification of the assets to be protected, together with an analysis of the risks incurred and the implementation of organisational, technical and procedural measures to ensure this protection. It provides for a regular assessment of the measures deployed to evaluate their effectiveness.

Objective 3: risk control and mitigation

The players should implement adequate security measures to mitigate identified risks in line with the sector's security policies.

Objective 4: incident monitoring and reporting

The players should have a system in place to monitor transaction-related incidents and customer complaints, which provides a comprehensive record of incidents. This monitoring system should include an incident reporting procedure that generates adequate information for governing bodies and also the relevant external stakeholders.

Objective 5: traceability and audit trail

The players should have a procedure in place that ensures all transactions covered by the cheque payment system are traceable with a view to supporting an uninterrupted audit trail.

Objective 6: physical cheque security

The players should ensure the security of the physical cheque payments throughout their lifecycle.

Objective 7: security of transaction environments

The physical and logical environments of the cheque payment system should be secure, and facilitate the guaranteed protection of the physical and logical tools as well as the transactions carried out. They ensure the quality, availability and technical usability of the archived elements.

Objective 8: transaction monitoring mechanism

Transaction monitoring is designed to prevent, detect and block fraudulent payment transaction attempts. This monitoring should be structured around a formal procedure defining the rules and types of alerts.

Objective 9: raising customer awareness of security regulations

Institutions should ensure that their customers are fully aware of the precautions required in the safekeeping of a printed chequebook, the issue or receipt of a cheque, its safekeeping and its presentation for payment.

Offline credit transfers

The protection and security of credit transfer orders must take into account the methods used by fraudsters. In this respect, offline credit transfers present a greater risk:

- of fraudsters stealing the identity of the payer to issue false orders notably by imitating the signature of the lawful holder and his or her proof of identity;

- of fraudsters amending legitimate cheques with the intention of changing the beneficiary prior to processing by the bank.

To do this, fraudsters try to obtain information by telephone, email or face-to-face by impersonating bank or general government officials or by posing as a customer, supplier or even an acquaintance. All account holders should therefore be on their guard when they are asked to divulge sensitive information such as an account number or details of their proof of identity.

From the **payer's** perspective (individuals, companies or general government administrations), preventive measures should be regularly conducted by account-holding institutions in order to:

- make customers aware of the different types of fraud through regular prevention and awareness campaigns (flyers included with account statements, appointments with customers);

- ensure regular updates of customer identification and authentication data (postal address, telephone number, proof of identity, bank details/IBAN, physical and digital elements of authentication) in accordance with the security procedures set out in the account agreement.

In addition, **account-holding institutions** must ensure that their fraud prevention arrangements are always up-to-the-minute, particularly by:

- warning and informing employees of the different types of fraud through regular prevention and awareness campaigns;

- putting in place payment order validation tools (scoring) to detect, check, alert, delay or reject, when necessary, transactions that appear to carry a high risk of fraud;

- training employees in the various procedures to be followed to combat attempted fraud (checks, alerts, confirmation calls, implementation of transaction security tools) on a regular basis;

- limiting acceptance of payment orders by fax, paper documents or mail and implementing two-step validation mechanisms for transactions on the basis of payment amounts;

- encouraging locked lists of beneficiaries and ceilings on credit transfer amounts depending on the type of customer.

Lastly, payment service providers (PSP) that process credit transfer orders are subject to Banque de France payment means security **oversight**, in accordance with the provisions of Article L. 141-4 of the French Monetary and Financial Code. This oversight framework notably requires that each ACPR[13] – authorised PSP in France includes an appendix on internal control in their annual report dealing specifically

13 *Autorité de contrôle* prudentiel *et de résolution* – ACPR, the French Prudential Supervision and Resolution Authority.

with the security of cashless means of payment and presenting the security measures implemented for the issue of credit transfers.

"Offline" use of payment cards

The security features of offline card payment orders both resemble and differ from those presented for offline credit transfers in that, while the initiation channels are broadly similar, the security framework imposed on merchants that receive payment orders is less strict than that of banks or payment institutions.

Fraud on offline card payments, like offline credit transfers, is based on techniques aimed at misappropriating card numbers to carry out fraudulent payments. Fraud prevention therefore relies on the implementation of appropriate protection measures for the systems that store, process and/or transmit cardholder data. These security measures also extend to the recording of telephone calls, storing of letters and controlling the physical call centre spaces, all of which may host card numbers.

The **card-issuing institutions** must ensure that they carry out preventive actions with their **cardholders** (individuals and businesses) with the aim of:

- informing customers of the different types of fraud through regular prevention campaigns;

- encouraging users to communicate their card details as little as possible, particularly the security code;

- offering solutions that incorporate non-replayable data (for example, dynamic security codes for payment cards) to prevent any risk of malicious reuse.

With regard to **merchants**, their **payment service providers** (account-holding institutions and acquirers) must ensure the sound implementation of different fraud prevention measures, particularly:

- in specific cases where no alternative online payment solution is possible, encouraging merchants to check customer-identification features (signatures, visual checks) and to collect only the card data strictly necessary to complete a transaction, while ensuring that transactions are properly categorised (separating MOTO transactions from online payments, in particular) in the payment systems;

- ensuring that merchants and, when necessary, their service providers (call centres, hosting) comply with PCI DSS (Payment Card Industry Data Security Standard) standards for the handling of card data (transmission, storage, archiving, destruction, etc.), which notably provide for the implementation of a security policy (including aspects relating to access to sensitive information and data, business continuity, control, physical and logical security, and staff training or liability) and also specify that the retention of payment card security codes is prohibited;

- warning and informing merchants of the different types of fraud through regular prevention campaigns.

Lastly, as is the case for credit transfers, payment service providers

that offer card issuance or card payment acquisition services are subject to Banque de France payment means security oversight. The appendix to their annual report on the security of cashless means of payment must therefore precisely detail the security measures in place for payment card-related activities.

The Observatory's recommendations

Offline payment methods have been shown to have inherent and characteristic limitations in terms of security: on the one hand, the media used (paper, telephone calls, etc.) are incompatible with the implementation of advanced security solutions and make it easier for fraudsters to falsify and counterfeit payment orders; on the other hand, the associated payment processes require numerous physical and logical interventions, both by the payer and the beneficiary and by their account-holding institutions, thereby multiplying fraudsters' windows of opportunity. In the case of cheques, these vulnerabilities are aggravated by the very large volumes of cheques and chequebooks in circulation, before and after use, giving fraudsters a large range of potential targets, as well as the involvement of operators with inconsistent security levels in the lifecycle of this means of payment, particularly in the routing and distribution channels.

These vulnerabilities and the multiplication of the fraud opportunities they offer warrant constant vigilance from all involved, as the security of these payment methods cannot be fully ensured by the payment sector's professional stakeholders.

- From the perspective of payment service providers, the lack of strong customer authentication at the time of the transaction makes the implementation of advanced solutions to identify risky transactions at the time of processing (i.e. image clearing or entering the credit transfer or card payment order) all the more necessary, providing the possibility, when needed, to delay flows and alert the account holder.

- The Observatory calls on merchants to put in place the means to ensure the transactions they initiate are valid, and in particular to ensure an adequate knowledge of their customers to make up as much as possible for the lack of strong authentication: this mainly involves requesting proof of identity and referring to services so that they can be sure of the validity of cheques for face-to-face payments, or analysing transaction factors (consistency between the identity of the buyer and the holder of the payment means, place of delivery, etc.) for remote purchases. In addition, when merchants store sensitive payment data, such as card numbers or IBANs, they must ensure that the technical measures needed to guarantee their security are in place, following, for example, the requirements of the data security standards.[14] Lastly, the Observatory stresses that MOTO card transactions should be reserved exclusively for remote sales by mail,

14 Payment Card Industry Data Security Standards (PCI DSS) for the retention of card data.

fax or telephone. Any e-commerce or m-commerce transaction should prompt an authenticated, offline payment, in compliance with the provisions of PSD2.

• The Observatory also insist upon the fact that users, be they private individuals, companies or general government administrations, must remain vigilant as to the security of their own payment means, ensuring that they apply the principles set out in Appendix 2 of this report. It is all the more crucial to respect these precautions with regard to offline payment methods, as other stakeholders have less leverage to fight fraud than is the case for online payments.

Lastly, the Observatory reaffirms its commitment to the modernisation efforts undertaken as part of the national payment strategy, aimed at developing alternatives to the use of cheques and other offline payment methods. The development of innovative and digital solutions, appropriate for use in the cases that currently justify the need for offline payments, appears to be the most apt approach to providing better transaction security. The development of ergonomic interbank payment solutions between individuals and businesses based on the use of credit transfers, and more recently instant credit transfers, as well as the development of electronic invoicing (e-invoicing) solutions between businesses, are examples of several appropriate and promising alternatives that can overcome the security limitations encountered in these specific use cases. The Observatory will, however, remain attentive to ensure that these developments do not impair users' access to the payment services they need.

3.2 The security of mobile payments

Introduction

According to the 2018 edition of Digital Market Barometer[15] published by the *Autorité de régulation des communications électroniques et des postes* (Arcep, France's Electronic Communications and Postal Regulatory Authority), 75% of French citizens have a smartphone[16] and for almost half of them it is their preferred means of browsing the internet. With the assurance of knowing that a connected device is in the hands of three out of four French citizens, the number of offers for mobile-phone accessible services has boomed and mobile payment solutions are no exception.

Little by little, smartphones are developing into a universal payment instrument that can be used for remote and in-store purchases, particularly with the widespread application of contactless near-field communication (NFC)[17] technology, for example. Just over a quarter of the population of France (26.2%) made at least one purchase in 2017

15 See https://en.arcep.fr/news/press-releases/p/n/digital-market-barometer-publication-of-the-2018-edition.html

16 The terms "smartphone", "mobile phone", "mobile device" and "mobile" are used interchangeably throughout this report.

17 NFC is the wireless communication technology used when making contactless card payments.

using a mobile according to the *Observatoire du commerce mobile* report for the first half of 2018[18] published by Mobile Marketing Association France. 5.9% of smartphone users in France – more than 2.1 million people – have made payments using NFC contactless technology or a payment application, placing France a little below the European average but at the level of Germany and Italy in terms of mobile payment adoption.

A recent study by the US research firm Forrester[19] also points out these trends, reporting that 80% of mobile transactions in Europe are remote payments. In-store transactions, also known as face-to-face transactions, carried out using mobile payment systems are expected to increase annually by 26% and reach EUR 27 billion in 2022 in seven of the main European countries (France, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom). This would represent 10% of all payments made from a mobile phone and slightly less than money transfers between individuals (EUR 30 billion in 2022).

The Observatory's technology watch[20] on the development of contactless face-to-face payment techniques by mobile phone was set up in 2007, in anticipation of their implementation. As a result, the Observatory published its analyses on the development of face-to-face payment initiation mechanisms for mobile phones based on "card" technologies and their security arrangements in its 2009, 2011 and 2015 Annual Reports. However, the scope of these analyses did not include mobile payments using non-electronic money infrastructures.[21]

This study aims to provide an overview of all the technologies available in France that allow users to initiate payments for goods or services, or to transfer money, using their mobile device. The security issues associated with the implementation of the main mobile payment solutions around today will be presented, excluding (i) payment solutions executed in a mobile internet browser environment[22] and (ii) mobile payment solutions that are little used or not used in France, which may be briefly outlined in the boxes.

Overview of mobile payment solutions

Telephone operator payment on the basis of invoices

Well before the development of smartphones, telecommunications operators had set up a payment system for premium rate phone calls added to the invoiced basic monthly charge. Subsequently, as technologies have evolved, the following services have emerged but the operators' monthly invoices are still used:

- SMS+, for premium SMS messages;

18 See http://www.mmaf.fr/publication/observatoire-du-commerce-mobile-1er-semestre-2018-extrait/

19 See https://www.forrester.com

20 The remit of the Observatory for Payment Card Security was expanded in 2016 when it became the Observatory for the Security of Payment Means.

21 Electronic money technologies refer to the equipment used to carry out card transactions.

22 These are not specific to mobile phones.

• Gallery, for payments in sales outlets using WAP billing;[23]

• Internet+, for payments using mobile internet[24] or Wi-Fi,[25] and facilitating purchases and subscriptions of content or digital services via smartphones.

For the Internet + service on smartphones, the subscriber's telephone number may be requested, as well as his or her internet log-in IDs, particularly when the smartphone is connected via Wi-Fi (and therefore to the customer's home equipment). If the operator deems it necessary, it can send a customer authentication code by SMS. The Observatory encourages mobile network operators to continue to monitor complaints and fraud for this type of payment through the mechanisms in place, and to develop adapted authentication solutions.[26]

The *Association française pour le développement des services et usages multimédias multi-opérateurs* (AFMM, the French association for the development of multi-operator multimedia services and uses) has proposed a code of ethics to be applied to these service offers and integrated into the contracts signed between players in the value chain: operators, aggregators and publishers of services or content. For consumers, the AFMM also provides a reverse phone look-up service on its website, which can be used to trace the Internet+or SMS+solutions that appear on an invoice[27] back to the institution receiving payment, particularly in the event of a dispute.[28]

As these payment methods were implemented by mobile network operators and possibly through the AFMM, and managed contractually with their customers, the Observatory will not consider them in further detail in this study.

Face-to-face payments and UPTs

By contactless communication with NFC technology

NFC technology allows customers to make contactless face-to-face payments and therefore can now be found in the majority of in-store payment terminals. Smartphones with the same technology can thus be used as a payment instrument at point of sale.[29]

23 In France, the wireless application protocol (WAP) was first implemented in 1999 but now appears to be in decline. It is used to adapt internet pages so that they can be consulted from a device connected to a mobile operator network, such as a mobile phone (excluding recent smartphones that are compatible with standard internet protocols). Some sites are inaccessible when using this protocol.

24 Therefore using 3G, 4G, and, in the future, 5G connections, providing access to the internet via mobile operator networks.

25 A medium-distance (several metres) wireless communication technology that gives access to the internet, most often through a terminal connected to a terrestrial communication network.

26 Note that these operator billing payments do not fall within the scope of PSD2.

27 See *https://annuaire.infoconso-multimedia.fr/*

28 It should be noted that major publishers of services or content with a solid reputation have put similar payment methods in place by contracting directly with mobile network operators. They do not appear in the AFMM's reverse phone look-up service and to make a complaint, the user should contact his or her seller or the seller's operator.

29 As a reminder, near-field communication (NFC) technology allows two devices a few centimetres apart to exchange information. All payment terminal manufacturers now offer models that are compatible with the prospect of 100% deployment by 2020, and more and more recent models of smartphones, and even connected objects such as watches or bracelets, allow data to be exchanged using NFC technology. In addition, several EMV electronic money specifications are based on this communication standard.

Box 10

Withdrawals by mobile phone

Since 2014 in France, certain banking institutions have had arrangements in place allowing their customers to carry out withdrawals at certain automated teller machines (ATMs) thanks to the generation of a one-time password accessible on their mobile phone.

Generally, an initial enrolment phase to the mobile withdrawal service is required, during which the customer receives or chooses a secret code (PIN – personal identification number).

The user can then access the service via the bank's website or mobile app to select the amount to be withdrawn and will be given a temporary one-time password. The PIN and the one-time password should then be entered at an ATM affiliated to the user's bank to obtain the cash.

This service can be used to get cash in case a customer has forgotten his or her payment card or in an emergency as a temporary measure after a card is lost or stolen. It also allows a trusted third party, such as a family member travelling or working away, to withdraw cash.

Outside of France, some major banks have developed withdrawal methods that use contactless near-field communication (NFC) technologies and have equipped their ATMs with NFC-compatible readers. The withdrawal is then made in a similar way to contactless payments using a card or mobile phone, i.e. by approaching the card or mobile to the ATM's reader, with (i) authentication of the card or mobile (just as for a payment, using the contactless security features) and (ii) authentication of the transaction by typing the cardholder's PIN at the ATM keyboard. Banks consider that contactless withdrawals offer the advantages of speed, with less time needed to carry out a withdrawal, and security, as fraud carried out by copying the magnetic strip of payment cards (card skimming) is reduced.

However, in order to provide a service that is accessible in all circumstances, it should not have to be permanently connected to a mobile network to operate. This is why the implementation of this type of payment service entails the storage of payment data that are considered sensitive. The Observatory repeats that these sensitive payment data must always be protected by appropriate measures, particularly when they are entered and saved, stored and used.

The main brands of mobile phone as well as the operating systems that these devices use (Android from Google and iOS from Apple)[30] facilitate contactless payment

30 According to Kantar Worldpanel research into final-quarter 2018 sales in France, Android and iOS account for 75.2% and 24.7% of the market, respectively.

through digital wallet solutions, based on the electronic money infrastructure for contactless card payments.[31] However, it is important to note that certain manufacturers such as Apple restrict access to contactless payment functions to their own solutions alone.

In the Android environment, third-party players, independent of Google and mobile phone manufacturers, can offer applications that use the NFC antenna (for those mobiles that have it). Banks and major retailers are thus also able to offer mobile applications that incorporate or are specifically designed to facilitate contactless face-to-face payments. In France, several banks have developed the contactless "*Paylib sans contact*" service through their distance banking application or a dedicated card payment app. Implementing these applications across a vast number of mobile devices with different technical architectures requires ever-greater vigilance with regard to the protection of sensitive payment data. Indeed, for a player to be able to offer a mobile application to all its customers, the app has to be adaptable to all the various smartphones available. Therefore, generally speaking, applications include a range of security measures or options, and during installation only those appropriate to the characteristics of the phone can and will be activated.

By scanning an image-based code

Relying on the electronic money infrastructure is not always considered advantageous when developing a payment solution. Certain players have thus chosen to offer services based on image reading, and more specifically, one-dimensional barcodes compatible with traditional cash registers, or two-dimensional codes, such as QR codes[32] for example (see Box 12), which are increasingly common on transport and entertainment tickets. The interpretation of the information contained in these codes can be used to initiate a card payment transaction, credit transfer, or a simple accounting entry in the books of an electronic money institution.[33] These solutions dispense with the need for NFC-compatible payment terminals and smartphones, but payment devices equipped with optical reading and/or display capabilities are required.

Several solutions of this type exist both in France (Lyf Pay or Lydia) and abroad (Alipay, WeChat Pay in China, Swish in Sweden, etc.).

31 Samsung has also integrated a technology that allows its South Korean users to pay with their mobile phones as if they were using a swipe card (when the strip reader is accessible). These users may therefore have to present their smartphone in front of the reader rather than the NFC antenna, especially in a French store.

32 Quick-response (QR) codes.

33 The institution in question therefore offers a payment solution that requires that both the merchant and the customer open electronic money accounts with that institution. Making a purchase thus involves transferring units of electronic money from the customer's account to the merchant's account.

Box 11

Contactless transactions using mobile devices

First, the near-field communication (NFC) antenna must be enabled. In the case of an Android smartphone, the user must choose an application that will handle the payment or that can designate a priority application for this type of service (and that will then launch automatically). The Observatory therefore feels that the user should be left to prioritise the applications accessing the NFC antenna.

In France, for all contactless transactions of over EUR 30, mobile payment applications systematically apply strong customer authentication (SCA). Some applications allow the user to lower the transaction value at which SCA is required.

When making the payment, the application initiates the transaction when the smartphone is touched to the payment terminal, and then requests authentication from the cardholder. The payment is then validated by touching the smartphone to the terminal a second time.

1. I touch my NFC-enabled mobile to the terminal displaying the contactless symbol.

2. My contactless payment application activates and I enter my code on my mobile.

3. I touch my phone a second time to the terminal. A green light, a beep, and the payment is approved. I take my receipt.

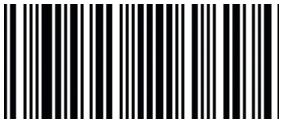
At this point, user authentication can be through the use of a secret code (referred to in this case as "mPIN" for "mobile PIN") or a biometric identifier such as a fingerprint or facial recognition.

The practicalities of this process can differ. For example, the user can open the application and authenticate a transaction on the mobile device before touching it to the payment terminal to complete the transaction in one single smartphone-payment terminal movement. Another possibility, which has not been made available by French institutions, involves touching the smartphone to the payment terminal once and then entering a personal identification number (PIN) on the terminal.

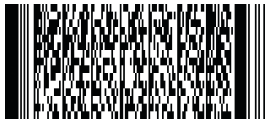
Box 12

Transactions by image reading

Data storage technologies can be applied to images, some of which are shown below.



Barcodes



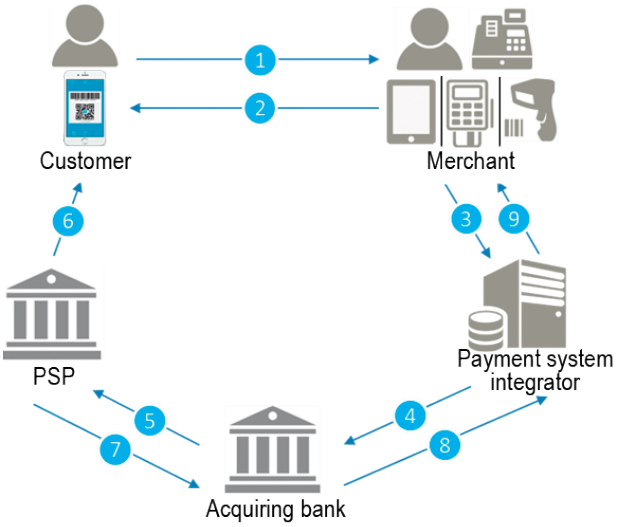
PDF417s

DataMatrix codes

QR codes

Several payment methods can be applied as part of the payment solutions that use these types of images.

The first involves the merchant scanning an image that is presented by the buyer on a physical device or mobile phone at the time of payment. The scan acts as a unique customer identifier. The merchant's terminal then sends an authorisation request to the customer's account-holding institution. The buyer's digital wallet is then debited with the transaction amount and a notification is sent to his mobile application.



1. The customer presents an image to be scanned.
2. The merchant scans the image.
3. The merchant's IT system transfers the data related to the image to his payment system integrator.
4. The integrator sends a payment request to the merchant's (acquiring) bank.
5. The acquiring bank transfers the payment request to the customer's payment service provider (PSP).
6. The PSP sends a notification to its customer.
7. The PSP sends a payment confirmation to the acquiring bank.
8. The acquiring bank transfers the payment confirmation to the integrator.
9. The integrator transmits the payment confirmation to the merchant's IT system.

.../...

The reverse process, which involves using a static image that identifies the merchant, can be found outside France, particularly in Asia. In both cases, security is relatively weak as the original image can be copied and reused.

The second potential payment method involves enhancing transaction security by employing single-use images. While the image verification circuit that triggers payment is identical, authentication elements of the application that generated the image as well as transaction data, and even information on the customer or merchant depending on who presented the image for scanning, are added to the image content. Cryptographic mechanisms ensure the integrity of the data generated and verified by both parties.

Innovative uses

In addition to these arrangements, other mobile phone uses for in-store payments are also emerging. For example, technologies traditionally used for remote transactions are being implemented in in-store payment environments, particularly through the use of geolocation to detect a customer's entry and exit from a store, and therefore trigger a payment if necessary.

In-app payments

The development of mobile services has necessitated payment solutions that can be directly integrated within a given application in order to offer a seamless customer experience.

Box 13

Two other face-to-face mobile payment technologies

Other technologies are also used in solutions rarely found in France, two of which are particularly interesting.

• BLE (Bluetooth Low Energy), also known as Bluetooth 4.0, is mainly used in Scandinavia. This technology facilitates communication at a distance of a few dozen centimetres between devices that have their own power source, which excludes payment cards. Merchants' terminals have to be equipped with a compatible beacon to use BLE technology, which generally involves installing an additional dedicated device.

• Sound wave technology, which uses sound waves to send and receive encrypted payment data from loudspeakers to microphones using a mobile phone. The transaction initiated by the merchant's device generates a sound wave containing encrypted data related to the payment. These waves are received on the customer's mobile phone and the algorithm converts them back into digital data and completes payment. Each transaction has its own unique sound waves and any disturbances during their transmission are managed by error detection codes.

We therefore speak of "in-app" payments. In this context, they are genuine digital wallets used within the given application. The Observatory published a study on the security of digital wallets in its 2011 Annual Report and its findings remain valid.

There are two possible types of in-app digital wallets: those that belong to merchants and those from third parties.

Merchants' in-app wallets

These integrated solutions rely on enrolling customers and recording their card data (number, expiry date and security code) with a PSP or a merchant's technical service provider. The Observatory recommends that anyone using these services makes sure that the application comes from the correct merchant before entering their payment information.

In this context, even though some solutions process payment transactions immediately, others group transactions and wait to send consolidated files during the night or at a fixed time. In the latter case, strong customer authentication by the cardholder's bank is impossible.

Third-parties' in-app wallets

PSPs also provide merchants with interfaces allowing them to integrate their digital wallet solution into applications. The merchant thus relies on the security measures put in place by the PSP's digital wallet.

In-app security measures

The security measures applied to these applications are those directly linked to the digital wallets that they host. As specified in the 2011 study, these measures should primarily cover:

- the protection of sensitive payment data (card numbers, expiry dates, security codes), which should be adapted to the technical environments of mobile devices;
- the enrolment of the payment card, which is generally ensured by the authentication of the cardholder when he or she registers the card;
- the fraudulent use of the application and therefore of the digital wallet, often taken into account when monitoring user activity, if necessary by triggering strong customer authentication in the event of suspected fraud.[34]

Payments between private individuals

The payment methods described above are suitable for payments by a business or by a merchant but, with a few rare exceptions, these solutions do not cover person-to-person (P2P) payments, also known as P2P transfers of money or funds. Three solutions are available to individuals wishing to send funds: (i) by exchanging units of electronic money; (ii) by credit transfer; and (iii) by payment card.

34 PSD2 states that for all transactions initiated by the cardholder, the issuer, when it is deemed necessary, must be able to apply a strong customer authentication.

By electronic money

One approach to providing this service is to open an electronic money (e-money) account with an approved institution. Transferring money between the payment accounts of two customers of the same institution results in a simple accounting entry in the PSP's books. To simplify their use, electronic money institutions provide a mobile app to their customers so they can consult their account balance, review their transaction history and transfer funds. This is how the solutions proposed by Lydia, S-money, Pumpkin, Leetchi, and, initially, PayPal operate.

The Observatory reiterates that this activity requires authorisation from the *Autorité de contrôle prudentiel et de résolution* (ACPR, Prudential Supervision and Resolution Authority).

By credit transfer

Another approach is to arrange a credit transfer to a payment recipient, for which the latter's international bank account number (IBAN) is required. In France, the vast majority of institutions that provide payment services to individuals have a mobile online banking application through which this type of service can be performed. In addition, some banks offer the "*Paylib entre amis*" service, which allows customers to transfer funds to an individual on the basis of that person's mobile phone number (the service ensures that the number corresponds to the IBAN). The advent of instant credit transfers[35] will encourage this type of use.

By payment card

Card payment systems, particularly Visa and Mastercard, have developed solutions that allow an individual's account to be credited in less than 30 minutes on the basis of their card data. The networks concerned ensure that a satisfactory level of security is maintained by insisting that companies wishing to use this solution must seek their authorisation to do so. For example, Leboncoin and Vinted, two platforms for individuals who want to offer goods or services for sale, offer this type of service to their users.

Mobile payment security issues

The main security issue for payments made using a mobile device is the protection of the data used to initiate a transaction. The innovation and maturity of data protection solutions have contributed significantly to the recent boom in mobile payments. However, there is no one-size-fits-all security solution. The different conditions for each mobile payment, which were presented in the previous chapter, require different security features.

For face-to-face payments as well as mobile P2P payments, the most common method used to date is contactless payment through the electronic money infrastructure, using a digital wallet associated with a communication channel. This mainly relies on NFC technology (for face-to-face payments) or QR codes to complete a transaction:

35 Within the Single Euro Payments Area (SEPA), funds can be transferred to a recipient account in less than 10 seconds using the SEPA Instant Credit Transfer.

• securing mobile payments via the NFC channel involves both securing the operating system and payment applications, as well as the smartphone's physical elements, particularly the contactless communication interface;

• securing mobile payments by QR code mainly involves measures that concentrate on protecting the payment applications and the generated codes.

Previous Observatory recommendations with regard to mobile payments

The Observatory issued recommendations on mobile payments in its 2007, 2009, 2012 and 2015 Annual Reports.

While the Observatory encourages players to innovate in the field of mobile face-to-face payments, it restates however that this type of payment solution should only be deployed if an equivalent level of security to that of contactless card payments can be guaranteed. To this end, the Observatory highlighted the need for security standards adapted to these new face-to-face payment systems, which can be applied to evaluate and certify the proposed solutions. Over the past few years, certifications for the security of solutions in their entirety and for the whole lifecycle have been introduced. The Observatory encourages the development of these initiatives, which must be able to take all the new functionalities proposed by the available solutions into consideration.

In this regard, the Observatory raised the need for pilot schemes involving card issuers and card payment schemes to implement the new functionalities and to test the procedures for protecting the various proposed infrastructural models over their lifecycle. These trials attempt to assess the overall level of security offered by the solutions within a contractual framework that protects the pilot providers in the event of fraud or technical problems.

In addition, the Observatory reiterated its commitment to the development of tokenisation solutions,[36] which can provide an additional level of security by reserving the use of a card number for non-contactless payments and by limiting the circulation of sensitive payment data. This recommendation is now a requirement imposed by payment card networks and implemented in the different solutions offering in-store card payment using mobile devices.

The Observatory repeats its commitment to the encryption of communications between mobile devices and payment terminals, even if tokenisation techniques mitigate the risk of data theft. The current EMV (Europay MasterCard VISA)[37] standard that uses NFC technology does not allow for this possibility. This capability should be made available as part of the future update to the EMV standard – EMV second generation. It should however be noted that the terminals will have to be upgraded to support this new

36 Technique involving a single-use or time-limited token that is associated with the card details required for payment.

37 The EMV standards are applied by the industry for the grand majority of technical specifications that govern card payment transactions.

standard's implementation, thus necessitating a major migration over a period of several years.

Enrolling a payment instrument in a digital wallet

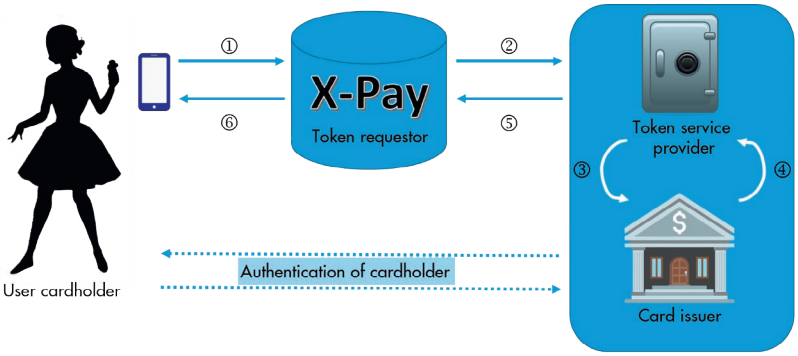
At the moment, at least one payment instrument must be enrolled in a digital wallet before it can be used to pay for a purchase. In addition, there are digital wallets offered mainly by banking or e-money institutions that can be used to pay by bank transfer.

Enrolling a card in a digital wallet involves collecting the data on the card, either through character recognition from a photo or by manual cardholder entry. The NFC capabilities of smartphones and cards could also be put to work in this framework to further streamline the customer experience.[38]

38 Due to the measures in place to protect contactless payment transactions, only specific card data (the card number but not the cardholder's name, for example) could thus be collected.

Box 14

Tokenisation of a card



1. In order to enrol a new card, the mobile app sends a token request containing the payment card details (number, expiry date and security code).
2. The token requestor (TR) sends a request to the token service provider (TSP) of the card-issuing bank to generate a token.
3. The TSP asks the issuer to validate the request, particularly by checking that the card is not reported lost or stolen and by confirming the card details.
4. The issuer approves the token request.
5. After generating a new token, the TSP transmits it to the TR.
6. The TR transmits the token to the mobile app to be used in place of the enrolled card's number.

During this process, the issuer generally asks the cardholder to confirm that he or she has requested the token. This phase can be implemented in different ways, depending on the digital wallet.

Digital wallets apply tokenisation techniques to better secure a card payment when the card is used in-store. Based on the bank identification number,[39] the token requestor (TR) sends a request to the token service provider (TSP) for the card-issuing bank. The TSP is usually the card issuer itself or one of its service providers. In order for this card number "alias" – the token – to be generated, a tokenisation service compatible with the digital wallet must be in place and the result of the risk analysis dedicated to the enrolment process must comply with the issuer's criteria. Without exception, the institutions implement an authentication procedure to ensure that each token request is legitimate.

More precisely, the TSP provides a token, which is valid for a limited period only and can solely be used in conjunction with the digital wallet, as well as other security functions adapted to digital wallets, such as cryptographic keys. These functions form part of the system implemented by the digital wallet publisher to protect sensitive data (using encryption techniques) and to authenticate the mobile device.

Cutting edge mobile payment security solutions

Although in-store payment using a mobile device is gradually becoming more widespread, the security requirements for smart payment cards are stricter than those applied by most mobile applications.

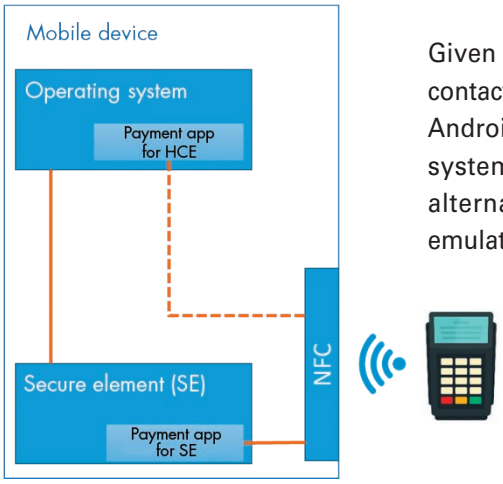
The first technical solutions proposed to reach a level of security similar to that of smart cards all focused on the use of a secure element (SE). A very high degree of certified security was achieved through these solutions, but the technical, organisational and commercial complexity of their application was a major obstacle to their deployment.

HCE (host card emulation) is a service integrated into the

39 The bank identification number (BIN) corresponds to the first six numbers on a card.

Figure 1

Secure element (SE) and host card emulation (HCE)



Given the slow growth in mobile contactless payments, in 2013, the Android mobile phone operating system helped to popularise an alternative solution – host card emulation (HCE) technology.

Note: Host card emulation (HCE) is a service integrated into the mobile device's operating system that allows it to communicate directly with the near-field communication (NFC) interface.

mobile's operating system that allows software applications installed in the mobile to communicate directly with the NFC interface via dedicated application programming interfaces (APIs). Securing mobile payments therefore relies on the security features provided by the operating system but these software features do not offer the same level of security as an SE. Additional security measures have therefore been applied to compensate. So far, the payment industry's most commonly adopted measures to limit the exposure of payment data to HCE-induced risks are data and application scrambling[40] techniques and tokenisation. The tokenisation process is effective as long as the tokens are stored in a trusted space on the phone.

A second technology known as TEE, for "trusted execution environment", is also worthy of mention out of the proposed compensatory security measures. The TEE is a software solution integrated into a number of smartphones, which consists in an execution environment with a security level similar to that of an SE, providing secure memory and storage space for applications. Thus, when the payment application is running, the TEE isolates it (or its most sensitive part) from the rest of the applications running on the mobile phone.

SE, HCE and TEE-based solutions provide security for contactless payments but can only work if there is an NFC controller (a wireless antenna that communicates with the payment terminal). Entry-level smartphones rarely have this component due to cost reasons. Therefore, a number of service providers have decided to develop payment solutions based on QR codes, which have the advantage of working on almost all smartphones. In terms of completing the transaction, this is the most straightforward type of payment for consumers, as once a compatible application has been installed on the smartphone, payment can be initiated by simply taking a photo of a QR code with the smartphone's camera (or by presenting an application-generated code on the mobile device's screen for scanning by the merchant's terminal). The following sections present the operating principles of SE, HCE, TEE and QR code technologies, as well as their advantages and drawbacks.

Secure elements (SE)

Generally speaking, the first solutions for mobile face-to-face payments established the SE as a central component through which all NFC communications, particularly for contactless payment transactions, had to pass. To achieve this, the single wire protocol (SWP) was developed to secure the exchanges between the mobile's NFC component and the SE. These solutions are called "SE-centric".

To carry out secure transactions, a certain number of operations, such as authentication, signature and validation by PIN, must be protected.

40 In this context, the terms obscuration, obfuscation and masking may also be used. These techniques consist in protecting applications against reverse-engineering attacks, which allow a malicious entity to interfere with the normal functioning of a payment application and, for example, to authorise the non-execution of cardholder authentication. Similarly, sensitive data can be fragmented and stored in a dispersed way in the device's memory, complicating their retrieval by an attacker.

This is the role of the SE, which provides cryptographic processing services and a secure memory to store confidential information, such as passwords, encryption keys and personal data.

The SE is a highly secure component that uses the same security principles as those applied in payment card chips. It performs the transaction authentication, data protection and backup functions for secure applications such as payment, access control or electronic identity verification.

In a mobile phone, the SE can take several forms: a SIM card, a mobile component or a memory card.

Three architectures offering SE-type components

Solutions based on SIM card SE technology (SIM-NFC) are distributed and managed in partnership with mobile network operators, who can enable SIM-card use by mobile payment service providers. Mobile network operators were among the very first to promote secure NFC applications and it is entirely natural that their SIM cards are used as the SE. By developing an infrastructure to manage access rights via their mobile networks, and by building on common standards devised through international bodies, mobile network operators account for a very large majority of the market in volume terms. The main advantage of this format is that the applications are hosted directly in the SE, which is itself integrated into the SIM card. In the event of theft or loss of the SIM card, sensitive data remain protected. The main drawback of the SIM-NFC format is the amount of available memory required to enable the correct functioning of some of the applications installed in the SE, which can prove to be insufficient.

Embedded secure elements (eSEs) are becoming increasingly common in new mobile phones equipped with an NFC antenna. The eSE can be integrated into the NFC controller, the mobile's microprocessor or even a separate component. This eSE configuration allows mobile manufacturers to offer their own secure NFC services without the need for a SIM card to provide the means of security. Payment service providers that rely on this technology benefit from enhanced performance thanks to the SE's integration as a component of the device. While payment service providers are no longer forced to enter into a partnership with mobile network operators, they must nevertheless develop partnerships with each mobile phone manufacturer or at least with the leaders of the targeted market.

SEs on microSD slot-in memory cards (SD-SE) provide an alternative to the technologies offered through operators and manufacturers, but are very rarely used.

A payment process involving several players

These three SE architectures may create relationships of interdependence between market players and thus complicate the ecosystem's implementation.

In order to subscribe to the deployed solutions, such as the SIM-NFC – or "SIM-centric" – model launched in France a few years ago, customers must have an NFC antenna-enabled

smartphone, a SIM card with an integrated SE and a contract with a mobile network operator that is a partner of their bank. The mobile network operator, which owns the SIM card, checks eligibility to the requested NFC service in order to allow the bank to remotely administer the payment service on the SIM card. A partnership between the operator and the bank must therefore be in place upstream. The bank can then deliver the mobile payment service by accessing a secure area on the customer's SIM card.

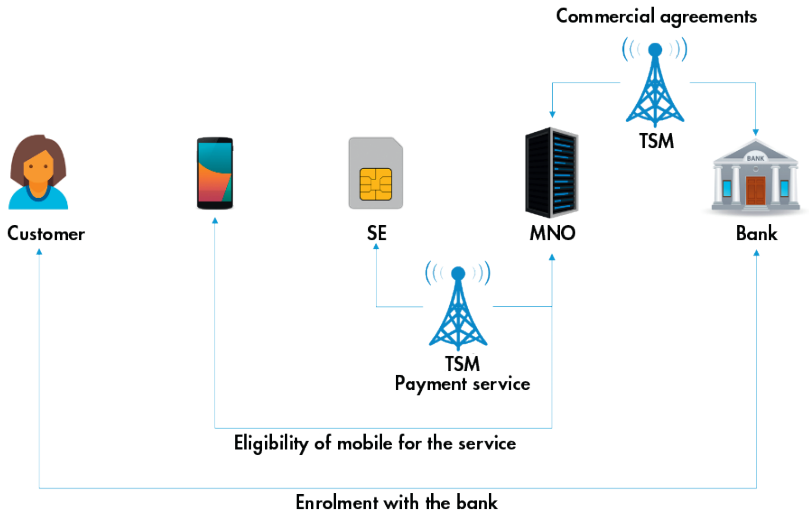
This model has created the need for a new player, the trusted service manager (TSM), responsible for acting as a reliable interface between the different players involved in the operation of a secure NFC application. The TSM manages the technical relationships between the mobile network operator, the bank and other secure service providers in order to make available, download and maintain the applications in the end user's mobile.

However, in practice, the proliferation of the players involved has resulted in problems of interoperability, despite efforts to standardise solutions in the sector. This slow convergence of solutions towards a tried-and-tested standardised framework (use cases and customer paths) has been one of the major obstacles to NFC mobile payments based on these technologies becoming more widely used.

Faced with these obstacles, some market players have developed an alternative to SE solutions and have introduced HCE technology.

Figure 2

NFC mobile network operators for a SIM-centric model



Note: SE – secure element; TSM – trusted service manager.

Mobile payment service operators are known as MNO (mobile network operators).

Host card emulation (HCE)

The specifications for host card emulation (HCE) technology were first put forward in 2012, but it was only when it was adopted by Google within the Android operating system at the end of 2013 that it became widely available.

The HCE architecture breaks from using the SE as a central component and transforms the established model that until now has relied on SE-based architectures, particularly that of SIM-centric solutions, by introducing a specific software layer between (i) the contactless NFC controller and any other physical component present on the mobile and (ii) the mobile payment applications. The mobile network operator's involvement is then limited to its role of providing and managing communication channels with the mobile for data routing while the TSM's role depends on the solution chosen to host the banking application's sensitive data.

Technology that allows a secure but flexible approach

HCE technology offers greater flexibility for hosting the sensitive data associated with the payment application. They can be hosted in (i) the application itself, (ii) an SE[41] or a secure mobile environment such as a TEE, or (iii) the cloud (the "SE in the cloud" solution):

- storing sensitive data in the payment application requires particular vigilance in terms of security and often necessitates combining several types of measures such as, for example, scrambling and encryption techniques (ensuring that particular attention is paid to the management of the cryptographic keys used);

- if the chosen solution is based on the use of an SE or a TEE service, the TSM retains control over the administration of data and cryptographic keys;

- if, on the other hand, the implementation scenario is of the "SE in the cloud" type, where the management of sensitive data is directly supported by a remote service, a TSM is no longer necessary.

SE in the cloud: a secure and remotely hosted payment card software

SEs hosted on a remote server are solutions based on payment card emulation software, which, rather than using a secure element on the mobile, require a mobile internet connection. These solutions, which are becoming more and more common, rely on an integrated secure environment – the TEE – or a minimal software security element on the mobile in order to access a network server that acts as the entire security component. Keys, certificates and transaction rights are thus remotely managed on this secure server, freeing up the security capabilities of the mobile itself, and also of the mobile network operators and smartphone manufacturers to operate the service. This results in greater flexibility of use and easier adaptation to the various generations of smartphones.

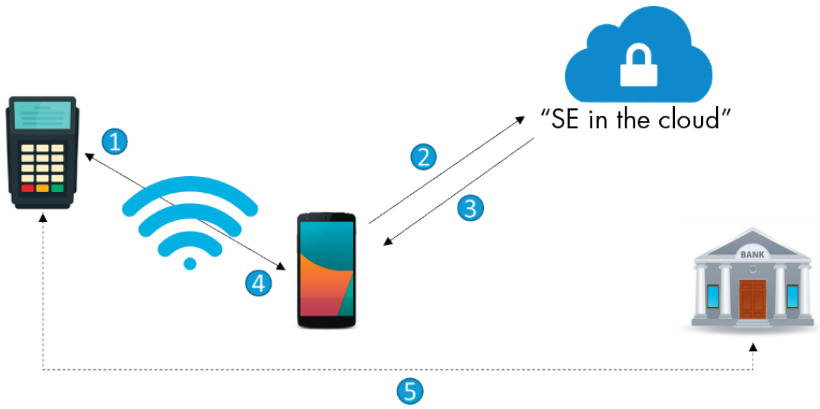
In the case of an SE in the cloud-type HCE solution, the payment process must take network coverage conditions into account to carry out a transaction, which can be done (A) online, or (B) offline.

41 Conceptually, an HCE application can simply act as a function for routing commands to be executed by an application in the SE (in this case, the SE hosts the application and the data).

(A) Online, the transaction is performed synchronously with the SE in the cloud server. When the mobile phone is held close to the electronic payment terminal (EPT), it transmits the contactless request to the application hosted in the operating system (1). The application then handles the call to the remote server that hosts the virtual secure element (2) in order to retrieve the data necessary to perform an EMV transaction in real time and transfer them to the mobile's NFC controller (3). The mobile then transmits the data to the EPT (4). To secure the transaction, certain data, such as the card number, are also sourced from a "tokenisation" service, which generates single-use numbers, thus preventing the same data from being reused for fraudulent purposes. The remainder of the transaction is completed in the same way as a contactless smart card payment by transmitting the transaction to the merchant's service provider (5). In fact, HCE and its SE in the cloud mode actually simply involve the contactless acquisition of remotely stored dematerialised payment card data.

Figure 3

HCE SE in the cloud – online payment



(B) Offline, the initial data recovery phase of the NFC payment application (carried out online) is split from the subsequent transaction completion phase using the recovered data (carried out offline). The first phase is carried out online by querying the remote server (1), which sends back the data that are useful for one or more transactions (2). These data are then loaded on the mobile. The data loaded on the mobile are used at the moment the contactless transaction is carried out (3), with the connection to the mobile operator's network no longer required and the transaction completed as before (4).

However, in the absence of a sufficiently secure space in the mobile, the possibility of using loaded data must be restricted, for example over time. Requirements in this respect have notably been developed by card payment systems such as Visa and Mastercard.

Trusted execution environment (TEE)

The TEE is a space secured by hardware and software devices, included in the mobile's microprocessor. It only provides security-related services and has its own operating environment

Figure 4

HCE SE in the cloud – online retrieval of payment data

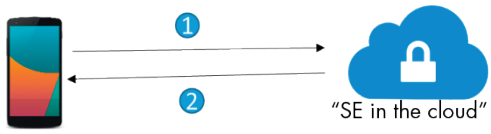
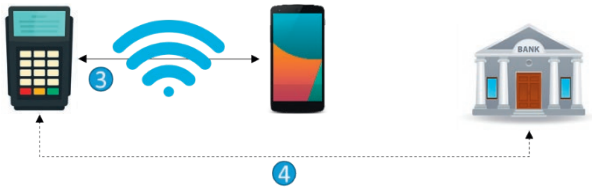


Figure 5

HCE SE in the cloud – offline payment



independent of the operating system. Although there are several TEE implementations on the market, they all follow the same concept.

The role of a TEE is more precisely to control access and to protect data (cryptographic keys, passwords, bank data such as card or payment account identifiers, etc.) and sensitive applications from internal and external attacks on the mobile device by ensuring that they are separated from the rest of the mobile's environment.

Due to its characteristics, TEEs are especially suitable for banking uses and mobile payment applications in particular.

QR codes

Contactless mobile payment technology using QR codes is available to all smartphone owners, including those without a controller or the secure environments described above. It is based on a payment application linked to a payment card or bank account, and on the smartphone's camera module.

The two most common QR code contactless payment models involve (i) the customer presenting the QR code and (ii) the merchant presenting the QR code (see Box 12). These models are covered by EMVCo's QR Code payment specifications, developed to promote greater interoperability between solutions based on this technology.

The need to ensure that unaltered QR codes are used

The content of a QR code cannot be altered without being altered visually. Two QR codes prompting different actions are therefore by necessity different in appearance. However, QR codes cannot be easily deciphered by a human being and it is thus essential that the payment application that uses them, on both

the customer and merchant sides, is authentic. This is the only way to ensure that the generated QR codes are legitimate.

Issues related to the protection of sensitive data

Sensitive data, such as personal information (PIN codes and passwords) and payment card or bank account details, are generally stored in the payment application. These data are encrypted through cryptographic algorithms in order to prevent theft and fraudulent access.

This configuration, where the payment application is installed and executed in the smartphone's operating system while encrypted sensitive data are stored in the smartphone's environment, however, presents a number of risks in terms of data theft and therefore fraud. A more secure solution to protect against such risks would be to deploy the payment application and store sensitive data in a secure environment such as a TEE.

Box 15

Security assessment of mobile payment solutions

The security of these payment solutions depends both on the security assessment of the devices used and also on the security of the solution's lifecycle management processes, particularly the process of user enrolment in payment applications.

As with EMV (Europay MasterCard Visa) smart payment cards, for solutions based on a physical security component, the existing assessment and certification processes, such as those conducted under the aegis of the *Agence nationale de la sécurité des systèmes d'information* (ANSSI, the French National Cybersecurity Agency), guarantee a high degree of device security.

In the case of software solutions, the scope to be considered is broader than for a physical security component, as it has to take the entire system into account, i.e. the payment app and services potentially hosted on remote servers. The assessment process put in place must provide assurance that the level of security of these software solutions is comparable to solutions based on a physical security component.

The main card payment systems (CB bank cards, Visa, Mastercard, American Express) have set up software security solution assessment protocols. The protocols are adapted to these solutions, which develop and evolve more rapidly, and rely on the abilities of testing laboratories, such as those recognised by ANSSI. In addition, certain smartphone manufacturers and mobile security solution providers have decided to have their security solutions (or at least the critical parts) certified by an authority such as ANSSI.

Security measures recommended by the Observatory

The Observatory repeats and expands upon the recommendations it made in its 2011 Annual Report on digital wallets, which were previously limited to the use of payment cards and also adapted to mobile payment solutions, namely the implementation of:

- the protection of sensitive payment data by all the players involved;

- the use of a secure authentication mechanism by a user's payment service provider when the card is enrolled in the payment application;

- risk analyses by the payment solution manager triggering secure authentication for transactions that are considered risky;

- a contractual framework that protects the users of these solutions.

More specifically, the Observatory recommends that reliable mechanisms be put in place that ensure secure storage of confidential data, which include both sensitive payment data and authentication data, particularly those involving biometric factors, which are increasingly exploited as part of mobile payments.

In addition, the Observatory reiterates that the use of biometrics as a component of secure authentication arrangements is subject to the recommendations made in its 2014 Annual Report.

Moreover, the Observatory calls on mobile operating system suppliers, smartphone manufacturers and all other involved parties (such as security or payment solution providers) to make corrective updates to their solutions available to users as soon as a security breach likely to alter the integrity, confidentiality or even availability of the system or data is identified.

Generally speaking, the Observatory encourages mobile payment application providers to make the security measures integrated into their applications more visible to users while stressing the need to deploy effective countermeasures to combat the unauthorised use of these applications.

The Observatory urges players to continue to innovate in the development of solutions that improve both the user experience and payment security, in line with PSD2's regulatory requirements for payment authentication, and with the national payment strategy driven by the National Cashless Payments Committee. In this respect, the Observatory repeats its recommendation on the need for regular assessments of the level of security of payment solutions, particularly on mobile devices.

Lastly, the Observatory advises users of mobile payment applications to:

- regularly update their mobile's operating system;

- choose secret codes, passwords and any other personal data used for mobile authentication processes, or at least their payment applications, with care, avoiding for example, numerical sequences such as "1234",

birthdays or alphabetical sequences, such as "QWERTY", and change them regularly;

• activate, if allowed by the operating system, the remote data deletion option in case of loss or theft of mobiles;

• use only trusted applications, particularly those recommended by payment service providers;

• avoid as much as possible carrying out payment transactions on mobile devices when the communication channel is not dependable (unsecured public Wi-Fi connections, for example).

A1 Security recommendations for the use of payment means

Fraudsters are always trying to find new ways to bypass ever more stringent security mechanisms. This is why the users of cashless payment means (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 fake 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 instrument, 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, remote online payments, 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. 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, particularly the amount, before you sign the cheque.

- Certain 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 cheque. 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 appear to have been tampered with.
- Only follow the instructions displayed on the ATM screen: do not let strangers distract you, even if they are offering assistance.
- If the ATM swallows your card and you cannot retrieve it immediately from the branch, report it right away.

When making online payments

- Do not store your bank details on your computer (card number, account number, IBAN – International Bank Account Number and SWIFT codes, etc.), never send them in an ordinary email 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 and that you are on the correct 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 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 [Magnetic Ink Character Recognition] 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 your card issuer before leaving to find out about any card protection systems that may be implemented.

- Remember to take the international telephone numbers for reporting lost or stolen payment instrument.

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 50 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 within 13 months of the debit date of the contested transaction (time limit set by law), with your account servicing payment service provider (PSP), 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).

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 Payer protection in the event of unauthorised payments

The Order transposing the Second Payment Services Directive (PSD2) which came into force on 13 January 2018, amended the legislative framework concerning payer liability in the event of an unauthorised payment transaction. However, the key principles of the original Payment Services Directive remain unchanged.

The burden of proof lies with the payment service provider (PSP). Accordingly, if a payer denies having authorised a payment transaction, the PSP has to prove that the transaction was authenticated, accurately recorded and entered in the accounts and not affected by a technical failure or some other deficiency. The law strictly governs the arrangements concerning forms of proof, stating that the use of a payment instrument registered by the PSP 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.

The transposition of PSD2 provides that in the event the disputed payment transaction involved a Payment Initiation Service Provider (PISP), the payer must inform his or her account servicing PSP of the payment transaction. The latter is required to arrange repayment and subsequently address the PISP, which has to prove that the payment transaction was authenticated, accurately recorded and entered in the accounts and not affected by a technical failure or some other deficiency.

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).[1]

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

Domestic and intra-Community transactions

These protective measures cover:

- payment transactions made in euro or CFP francs[2] within the territory of the French Republic;[3]

- intra-Community transactions in which the beneficiary and the payer respectively call on a PSP that is located:
  – in metropolitan France, in the French overseas departments or in Saint Martin, on the one hand,
  – in another state party to the EEA agreement on the other,

and carried out in euro or in the domestic currency of one of those states.

As regards unauthorised transactions, i.e. in practice, in cases of loss, theft or misappropriation (including by remote fraudulent use or counterfeiting) of a payment instrument, the user of the payment service must inform the PSP that he or she did not authorise the payment transaction within 13 months of the debit date. The service provider is then required to refund the payer the amount of the unauthorised payment transaction within one business day 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. The transposition of PSD2 provides for a delay in repayment in the event that the PSP has just cause to suspect fraud on the part of the payer. In this case, the Banque de France must be notified. 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 PSP without undue delay on becoming aware of the loss, theft or misappropriation of the payment instrument or of its unauthorised use.

Prior to 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 50, resulting from the payment instrument's use. If the transaction is carried out without using the personalised security credentials if it was impossible for the payer to detect the theft or loss of his or her payment instrument, or if the loss is the result of actions taken by a person under the responsibility of the PSP, the payer shall not be held liable and shall not be liable for any financial losses (even up to the maximum of EUR 50).

2 The CFP (*colonies françaises du Pacifique* – French Pacific colonies) franc or Pacific franc.

3 The Order of 9 August 2017 that transposes DSP2 into French law provides that the majority of its provisions apply to New Caledonia, French Polynesia and the islands of Wallis and Futuna.

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 as agreed with the PSP, whether with intent or through gross negligence.

Lastly, if the PSP 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 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 service 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 service provider or to the entity indicated to the customer by the services provider, as applicable, in the payment service agreement or the deposit account agreement.

Once the user has notified the PSP 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

PSD2 partially extends its scope to payment transactions between a PSP located within the EEA and another located outside the EEA. In this type of payment transaction, often referred to as "one-leg transactions", the Directive's provisions quite broadly apply to that part of the payment transaction that is carried out within the EEA. For example, a payer that has a payment instrument issued by a PSP located in France can benefit from protection even if the payment instrument is used in the United States. Consequently, in the event of an unauthorised payment transaction on behalf of a beneficiary whose PSP is located in the United States (or elsewhere outside of the EEA), the payer can request repayment from his or her PSP located in France under the same conditions as those applicable to domestic or intra-Community payment transactions.

There are specific provisions in place for payment transactions made by card when:

- the issuer is located in Saint Pierre and Miquelon or Saint Barthélemy, on behalf of a beneficiary whose PSP is located in a non-European state,[4] irrespective of the currency denomination of the payment transaction;

- the issuer is located in New Caledonia, French Polynesia or Wallis and Futuna, on behalf of a beneficiary whose PSP is located in a state other than the French Republic, irrespective of the currency used.

In such cases, the maximum amount of EUR 50 applies to unauthorised transactions performed using lost or stolen cards, even if the payment transaction was carried out without using personalised security credentials.

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

4 A non-European state is a state that is not party to the EEA agreement.

A3 Missions and organisational structure of the Observatory

Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the *Code monétaire et financier* (French Monetary and Financial Code) set out the responsibilities, 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 L. 141-4 of the French Monetary and Financial Code has been amended by extending the missions of the Observatory for Payment Card Security to all cashless payment means. Henceforth, in addition to cards issued by payment service providers or equivalent institutions, all other cashless payment means now fall within the scope of the missions of the Observatory for the Security of Payment Means.

In accordance with Article L. 311-3 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 an instrument takes or the technical process used. The means of payment listed below fall within the remit of the Observatory.

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 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.

Trade bills are marketable securities that state that the bearer holds a claim for payment of a sum of money and serves for that payment. Trade bills include bills of exchange and promissory notes.

Responsibilities

Pursuant to Articles L. 141-4 and R. 141-1 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 R. 141-2 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 responses. These opinions may be made public by the Minister.

Composition

The composition of the Observatory is set out in Article R. 142-22 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* (ACPR – the French prudential supervision and resolution authority) or his representative;
- a representative of the *Commission nationale de l'informatique et des libertés* (CNIL – the French data protection body);
- 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 merchants' professional organisations and corporations, notably from the retail sector, the supermarket sector and remote 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 R. 142-23 *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 and 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 *Annual Report of the Observatory for the Security of Payment Means* 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 R. 142-25 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* (ACPR – the French prudential supervision and resolution authority), are appointed for a three-year term by order of the Minister of the Economy. The most recent appointment order was issued on 11 December 2018.

Président
François Villeroy de Galhau
Governor of the Banque de France

Members of Parliament

Éric Bocquet
Senate

Rémi Rebeyrotte
National Assembly

Representatives of the General Secretariat of the ACPR

Édouard Fernandez-Bollo
Secretary General

Geoffroy Goffinet

Representatives of general government

Nominated on the recommendation of the General Secretariat for Defence and National Security:

- The Director General of the French National Cybersecurity Agency or his/her representative:
  Guillaume Poupard
  Vincent Strubel
  José Araujo

Nominated on the recommendation of the Minister of the Economy, Finance and Digital Economy:

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

- The Head of the Treasury
  or his/her representative:
  Odile Renaud-Basso
  Arnaud Delaunay

- The Director General for Enterprises
  or his/her representative:
  Thomas Courbe
  Romain Bonenfant

- The Director General for Competition, Consumer Affairs and the Punishment of Fraud Offences or his/her representative:
  Aurélien Hauser
  Madly Meri

Nominated on the recommendation of the Minister of Justice:

- The Director for Criminal Affairs and Pardons
  or his/her representative:
  Raphaëlle Olive

Nominated on the recommendation of 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

Nominated on the recommendation of the Minister of Defence:

- The Director General of the *Gendarmerie nationale* or his/her representative:
  Arnauld Cheminant
  Cyril Piat

Nominated on the recommendation of the *Commission nationale de l'informatique et des libertés* (CNIL):

- The Head of Economic Affairs
  or his/her representative:
  Clémence Scottez
  David Ruiz

Representatives of issuers of payment means and operators of payment systems

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

Nathalie Chabert
Deputy Delegate General
Association française pour le développement des services et usages multimédias multi-opérateurs (AFMM)

Corinne Denaeyer
Head 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
Director General
American Express France (Amex)

Solveig Honoré Hatton
Vice-President, Business development
MasterCard France

Philippe Laulanie
Executive Director
Groupement des cartes bancaires (GCB)

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

Laurence Matterlin
Head of Risk Management and Fraud Prevention
Natixis Payment Solutions

Gérard Nébouy
Executive Director
Visa Europe France

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

Jean-Marie Vallée
Director General
STET

Narinda You
Head of Strategy and Market Relations
Crédit Agricole

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)

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

Representatives of the Consumer Board of the French National Consumers' Council

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

Morgane Lenain
Lawyer
Union nationale des associations familiales (UNAF)

Mathieu Robin
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)

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 région 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 Methodological approach used to measure fraud on cashless payment means

General framework

Definition of payment means 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 their illegitimate use and/or effective illegitimate use**:

- **resulting in financial loss**: for the account-holding institution 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 remote payments, 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 institution 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.

Types of payment means fraud

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

- **fakes** (theft, loss, counterfeit): fraud involving the issuance of false payment orders either through a physical payment instrument (card, chequebook, etc.) that has been lost, stolen or counterfeited, or through the misappropriation of data or banking credentials;

1 See *https://www.banque-france.fr/en/annual-report-2015* (page 11).

- **falsification**: fraud involving the use of a falsified 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 in 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.

Measurement of payment card fraud

Transactions covered

Payment card fraud, as measured in this report, covers payments (face-to-face and remote) 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 transaction acceptor – the merchant or ATM – is located 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).

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

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

Source of fraud data

The Observatory gathers payment card fraud data:

- from the CB Bank Card Consortium (*Groupement des cartes bancaires CB*), Mastercard and Visa for their members' transactions;
- 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 remote payments, the merchant's sector of activity.

Type 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.
Falsified or counterfeit cards	Falsification of a payment card consists in modifying an authentic card's magnetic strip 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 or her knowledge or created through card number generation[b] and used in remote transactions.
Unallocated card numbers	Use of a true card number (or personal account number – PAN) that has not been attributed to a cardholder, generally in remote 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 use
Face-to-face payment	Payments made at a point of sale or through an unattended payment terminal (UPT), including contactless payments.
Remote payment	Payments carried out online, by mail, by fax or telephone, or any other means.
Withdrawal	Cash withdrawals at ATMs.

Geographical area	Description
Domestic transaction	Both the issuer and the acceptor are established in France. However, for remote payments, the fraudster may operate from abroad.
International France → SEPA transaction	The issuer is established in France and the acceptor abroad within SEPA.
International France → non-SEPA transaction	The issuer is established in France and the acceptor abroad outside SEPA.
International SEPA → France transaction	The issuer is established abroad within SEPA and the acceptor in France.
International non-SEPA → France transaction	The issuer is established abroad outside SEPA and the acceptor in France.

Note: SEPA – Single Euro Payments Area.

Merchant's sector of activity for remote payments	Description
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 and 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 and mobile telephony equipment and services.
Travel and transportation	Rail, air and sea.
Other	

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 or her payment account or electronic purse to the account of a third-party beneficiary. This includes Single Euro Payments Area (SEPA) credit transfers and SEPA instant 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 service providers.[4]

Analysis of fraud

Credit transfer fraud is analysed by referring to the fraud types, geographical areas of issuance and transfer destination and the initiation channels used.

Types of credit transfer fraud	Forms of fraud
Fakes	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 that of the lawful payment beneficiary or that does not correspond to any economic reality.
Geographical area of issuance and credit transfer destination	**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 using mail, forms, 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).

Note: SEPA – Single Euro Payments Area.

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 L. 518-1 of the French 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.

Measurement of direct debit fraud

Payment instruments covered

Direct debit fraud, as measured in this report, covers payment orders given by a creditor to their payment service provider for them to debit the account of a debtor, in accordance with the authorisation (or direct debit mandate) signed by the debtor. This category is made up of SEPA direct debits.

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 service providers.

Analysis of fraud

Direct debit fraud is analysed by referring to the fraud types, geographical areas of issuance and direct debit destination and the authorisation channels used.

Types of direct debit fraud	Forms of fraud
Fakes	The creditor-fraudster originates direct debit instructions using illegally obtained account numbers, without any authorisation or underlying economic reality.
Misappropriation	The payer-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 or her.
Replay	The creditor-fraudster 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 direct debit destination	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.

Note: SEPA – Single Euro Payments Area.

Authorisation channels used	Procedures for use
Paper	Direct debit mandates sent using mail, forms, email, fax or phone.
Online	Direct debit mandates sent via an online bank or a mobile payment application.
Telematics	Direct debit mandates sent via electronic channels other than online banking and mobile payment application channels.

Measurement of cheque fraud

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

Scope of fraud

Cheque fraud, as measured in this report, covers cheques payable in France, in euro or a foreign currency (in this case, the cheque is drawn on a payment account held in a foreign currency), falling within the legal framework set forth in Articles L. 131-1 to 88 of the French Monetary and Financial Code. This specifically 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 L. 525-4 of the French 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.

Sources 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 service providers. These payment service 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).

Analysis of fraud data

Cheque fraud data are analysed by referring to the main fraud types defined by the Observatory. The following table summarises the typology of the most common forms of fraud observed.

Types of cheque fraud	Forms of fraud
Fakes (theft, loss, counterfeit or 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.
	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).
	Fake 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, over-writing 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.
	Lost or stolen valid cheque, intercepted on its way 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.

Measurement of trade bill fraud

Payment instruments covered

Trade bill 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: electronic payment orders 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.

Types and source of fraud data

The types of trade bill fraud are the same as those defined for cheques.

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

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, for instance on prepaid cards;
- 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.

A6 Statistics

Overview

T1 Cashless payment means used in France in 2018

(number in millions, amount in EUR billions, average amount in EUR, change in %)

	Number of transactions		Transaction amounts		Average amount
	2018	Change 2018/2017	2018	Change 2018/2017	
Card payments[a)]	13,179	+5	568	+7.0	43
Direct debits	4,211	+3	1,644	+4.0	391
Credit transfers	4,037	+4	24,211	+0.6	5,997
o/w LVT[b)]	*10*	*0*	*10,130*	*+7.0*	*1,038,473*
Cheques	1,747	-9	891	-11.0	510
Trade bills	81	0	252	-3.0	3,150
E-money	65	+18	1	+17.0	16
Total	**23,320**	**+3**	**27,567**	**+0.5**	**1,182**
Card withdrawals[a)]	1,439	-3	137	+1.0	94
Total transactions	**24,759**	**+3**	**27,704**	**+0.5**	**1,119**

Source: Observatory for the Security of Payment Means.
a) Cards issued in France only.
b) LVT: large-value transfers, issued via large-value payment systems (Target2, Euro1). Professional payments only.

T2 Breakdown of payment means fraud in amount and volume in 2018

(amount in EUR, volume in units, share in %, average amount in EUR)

	Amount		Volume		Average amount
	2018	Share	2018	Share	
Card payments[a)]	401,604,986	38	6,068,959	90	66
Cheques	450,108,464	43	166,421	3	2,704
Credit transfers	97,307,108	9	7,731	0	12,586
Direct debits	58,346,253	6	309,377	5	188
Trade bills	226,217	0	5	0	45,243
Total payments	**1,007,593,028**	**96**	**6,552,493**	**98**	**154**
Card withdrawals[a)]	37,630,659	4	158,908	2	237
Total transactions	**1,044,953,687**	**100**	**6,711,401**	**100**	**156**

Source: Observatory for the Security of Payment Means.
a) 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 2018, there were 88.8 million cards in circulation, of which:

- 79 million four-party cards ("CB", Mastercard, Visa, etc.);
- 9.8 million three-party cards.

Around 1,358,819 cards were cancelled as they were reported lost or stolen[1] in 2018.

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	10,739.13	407.58	281.25	14.14	59.85	4.58
Remote payments excluding online	31.86	2.39	21.04	1.53	4.35	0.41
Remote payments online	1,504.89	95.78	340.04	18.70	27.62	2.07
Withdrawals	1,383.99	129.63	32.45	3.69	21.24	3.16
Sub-total	**13,659.87**	**635.38**	**674.78**	**38.06**	**113.06**	**10.22**
Three-party cards						
Face-to-face payments and UPT	125.65	14.40	10.64	1.46	6.42	1.04
Remote payments excluding online	3.03	0.31	2.48	0.03	0.25	0.02
Remote payments online	11.10	1.98	8.44	1.17	1.35	0.20
Withdrawals	1.73	0.16	0.00	0.00	0.00	0.00
Sub-total	**141.51**	**16.85**	**21.56**	**2.66**	**8.02**	**1.26**
Total	**13,801.38**	**652.23**	**696.34**	**40.72**	**121.08**	**11.48**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

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	10,739.13	407.58	308.82	17.32	92.74	8.48
Remote payments excluding online	31.86	2.39	9.95	1.73	5.32	1.30
Remote payments online	1,504.90	95.78	101.70	10.46	32.40	3.86
Withdrawals	1,384.00	129.63	24.88	4.26	7.82	1.94
Sub-total	**13,659.89**	**635.38**	**445.35**	**33.77**	**138.28**	**15.58**
Three-party cards						
Face-to-face payments and UPT	125.65	14.40	9.19	1.56	10.98	4.27
Remote payments excluding online	3.03	0.31	0.24	0.01	0.14	0.00
Remote payments online	11.10	1.98	1.83	0.29	0.97	0.24
Withdrawals	1.73	0.16	0.00	0.00	0.49	0.22
Sub-total	**141.51**	**16.85**	**11.26**	**1.86**	**12.58**	**4.73**
Total	**13,801.40**	**652.23**	**456.61**	**35.63**	**150.86**	**20.31**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

T5 Breakdown of fraud by card type

(rate in %, amount in brackets in EUR millions)

	Fraud rate (and amount)											
	2013		2014		2015		2016		2017		2018	
Four-party cards	0.080	(455.9)	0.080	(486.4)	0.086	(526.8)	0.082	(531.3)	0.070	(482.2)	0.072	(526.5)
Three-party cards	0.065	(14.0)	0.062	(14.2)	0.068	(15.5)	0.060	(13.5)	0.043	(11.6)	0.040	(11.0)
Total	**0.080**	**(469.9)**	**0.080**	**(500.6)**	**0.085**	**(542.3)**	**0.081**	**(544.8)**	**0.069**	**(493.8)**	**0.071**	**(537.5)**

Source: Observatory for the Security of Payment Means.

T6 Geographical breakdown of fraud

(rate in %, amount in brackets in EUR millions)

	Fraud rate (and amount)											
	2013		2014		2015		2016		2017		2018	
Domestic transactions (French card and French acceptor)	0.046	(238.6)	0.043	(234.6)	0.044	(244.4)	0.042	(244.5)	0.037	(226.5)	0.038	(245.6)
International transactions	0.350	(231.3)	0.316	(266.0)	0.372	(297.9)	0.353	(300.3)	0.281	(267.3)	0.270	(291.9)
o/w French card and non-SEPA acceptor	*0.688*	*(70.2)*	*0.636*	*(70.0)*	*0.692*	*(74.5)*	*0.713*	*(68.0)*	*0.511*	*(60.3)*	*0.438*	*(50.3)*
o/w French card and SEPA acceptor	*0.366*	*(67.9)*	*0.374*	*(91.0)*	*0.459*	*(116.8)*	*0.370*	*(113.9)*	*0.308*	*(100.7)*	*0.352*	*(143.3)*
o/w foreign non-SEPA card and French acceptor	*0.404*	*(64.1)*	*0.336*	*(65.6)*	*0.353*	*(69.7)*	*0.449*	*(73.7)*	*0.386*	*(74.1)*	*0.323*	*(65.5)*
o/w foreign SEPA card and French acceptor	*0.135*	*(29.1)*	*0.134*	*(39.3)*	*0.153*	*(36.9)*	*0.158*	*(44.7)*	*0.102*	*(32.3)*	*0.092*	*(32.8)*
Total	**0.080**	**(469.9)**	**0.080**	**(500.6)**	**0.085**	**(542.3)**	**0.081**	**(544.8)**	**0.069**	**(493.8)**	**0.071**	**(537.5)**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

T7 Breakdown of domestic fraud by transaction type

(rate in %, amount in brackets in EUR millions)

	Fraud rate (and amount)											
	2013		2014		2015		2016		2017		2018	
French card – French acceptor												
Payments	0.050	(199.9)	0.046	(193.2)	0.047	(204.5)	0.045	(208.6)	0.039	(191.9)	0.041	(214.7)
o/w face-to-face and UPT	*0.013*	*(45.8)*	*0.010*	*(37.1)*	*0.012*	*(43.4)*	*0.009*	*(33.6)*	*0.009*	*(35.8)*	*0.010*	*(41.4)*
o/w remote	*0.269*	*(154.2)*	*0.248*	*(156.0)*	*0.244*	*(161.1)*	*0.241*	*(175.0)*	*0.190*	*(156.1)*	*0.173*	*(173.3)*
– o/w by post/phone	*1.122*	*(29.2)*	*0.147*	*(2.8)*[a)]	*0.372*	*(9.1)*	*0.280*	*(9.3)*	*0.357*	*(7.4)*	*0.351*	*(9.5)*
– o/w online	*0.229*	*(125.0)*	*0.251*	*(153.2)*[a)]	*0.239*	*(152.0)*	*0.239*	*(165.7)*	*0.186*	*(148.7)*	*0.168*	*(163.8)*
Withdrawals	0.033	(38.6)	0.034	(41.5)	0.033	(39.9)	0.029	(35.9)	0.027	(34.6)	0.024	(30.9)
Total	**0.046**	**(238.6)**	**0.043**	**(234.6)**	**0.044**	**(244.4)**	**0.042**	**(244.5)**	**0.037**	**(226.5)**	**0.038**	**245.6**

Source: Observatory for the Security of Payment Means.
a) The substantial decline between 2013 and 2014 in the amount of fraud in remote payments made by post or phone and the corresponding increase in the amount for online 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.
Note: UPT – unattended payment terminal.

T8 Breakdown of international fraud by transaction type – French cards

(rate in %, amount in brackets in EUR millions)

	Fraud rate (and amount)									
	2014		2015		2016		2017		2018	
French card – Foreign non-SEPA acceptor										
Payments	0.532	(41.7)	0.735	(56.3)	0.862	(56.2)	0.608	(53.3)	0.534	(44.4)
o/w face-to-face and UPT	*0.350*	*(19.2)*	*0.509*	*(25.8)*	*0.485*	*(22.9)*	*0.252*	*(12.7)*	*0.230*	*(12.9)*
o/w remote	*0.960*	*(22.5)*	*1.174*	*(30.5)*	*1.862*	*(33.3)*	*1.096*	*(40.6)*	*1.168*	*(31.5)*
– o/w by post/phone	*4.955*	*(7.5)*	*2.345*	*(9.5)*	*2.783*	*(9.4)*	*1.499*	*(8.4)*	*1.127*	*(4.8)*
– o/w online	*0.682*	*(14.9)*	*0.959*	*(21.1)*	*1.648*	*(23.9)*	*1.025*	*(32.3)*	*1.175*	*(26.7)*
Withdrawals	0.890	(28.3)	0.586	(18.1)	0.390	(11.8)	0.229	(7.0)	0.184	(5.9)
Total	**0.636**	**(70.0)**	**0.692**	**(74.4)**	**0.713**	**(68.0)**	**0.511**	**(60.3)**	**0.438**	**50.3**
French card – Foreign SEPA acceptor										
Payments	0.434	(89.8)	0.526	(115.7)	0.422	(112.9)	0.342	(99.8)	0.385	(142.4)
o/w face-to-face and UPT	*0.067*	*(7.8)*	*0.071*	*(8.0)*	*0.066*	*(8.3)*	*0.075*	*(10.5)*	*0.066*	*(10.2)*
o/w remote	*0.910*	*(82.0)*	*1.004*	*(107.7)*	*0.754*	*(104.5)*	*0.591*	*(89.2)*	*0.617*	*(132.2)*
– o/w by post/phone	*1.317*	*(13.9)*	*1.399*	*(18.7)*	*1.317*	*(19.7)*	*1.489*	*(14.9)*	*0.911*	*(14.2)*
– o/w online	*0.856*	*(68.1)*	*0.948*	*(89.0)*	*0.687*	*(84.9)*	*0.527*	*(74.4)*	*0.594*	*(118.0)*
Withdrawals	0.033	(1.2)	0.033	(1.1)	0.024	(0.9)	0.025	(0.9)	0.025	(0.9)
Total	**0.374**	**(91.0)**	**0.459**	**(116.8)**	**0.370**	**(113.8)**	**0.308**	**(100.7)**	**0.352**	**(143.3)**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

T9 Breakdown of international fraud by transaction type – Foreign cards

(rate in %, amount in brackets in EUR millions)

	Fraud rate (and amount)									
	2014		2015		2016		2017		2018	
Foreign non-SEPA card – French acceptor										
Payments	0.380	(65.0)	0.391	(68.1)	0.507	(73.2)	0.429	(73.3)	0.357	(64.8)
o/w face-to-face and UPT	*0.162*	*(21.9)*	*0.168*	*(22.8)*	*0.169*	*(17.4)*	*0.135*	*(16.3)*	*0.108*	*(13.7)*
o/w remote	*1.213*	*(43.1)*	*1.185*	*(45.3)*	*1.341*	*(55.8)*	*1.143*	*(57.0)*	*0.947*	*(51.1)*
– o/w by post/phone	*1.018*	*(7.7)*	*1.159*	*(10.8)*	*1.748*	*(18.2)*	*1.488*	*(19.8)*	*0.886*	*(11.5)*
– o/w online	*1.265*	*(35.4)*	*1.193*	*(34.5)*	*1.206*	*(37.7)*	*1.017*	*(37.2)*	*0.967*	*(39.6)*
Withdrawals	0.026	(0.6)	0.069	(1.6)	0.024	(0.5)	0.038	(0.8)	0.031	(0.7)
Total	**0.336**	**(65.6)**	**0.353**	**(69.7)**	**0.449**	**(73.7)**	**0.386**	**(74.1)**	**0.323**	**(65.5)**
Foreign SEPA card – French acceptor										
Payments	0.156	(38.5)	0.175	(36.0)	0.178	(43.8)	0.114	(31.5)	0.102	(32.0)
o/w face-to-face and UPT	*0.026*	*(5.1)*	*0.033*	*(4.8)*	*0.024*	*(3.7)*	*0.018*	*(3.5)*	*0.018*	*(3.4)*
o/w remote	*0.476*	*(33.1)*	*0.528*	*(31.3)*	*0.456*	*(40.0)*	*0.337*	*(28.0)*	*0.229*	*(28.6)*
– o/w by post/phone	*0.397*	*(4.8)*	*0.734*	*(7.7)*	*0.695*	*(11.0)*	*0.564*	*(8.9)*	*0.357*	*(6.2)*
– o/w online	*0.492*	*(28.6)*	*0.484*	*(23.6)*	*0.403*	*(29.0)*	*0.284*	*(19.1)*	*0.208*	*(22.4)*
Withdrawals	0.018	(0.9)	0.025	(0.9)	0.024	(0.9)	0.019	(0.7)	0.019	*(0.8)*
Total	**0.134**	**(39.3)**	**0.153**	**(36.9)**	**0.158**	**(44.7)**	**0.102**	**(32.3)**	**0.092**	**(32.8)**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

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

(amount in EUR millions, share in %)

2018	All card types		Four-party cards		Three-party cards	
	Amount	Share	Amount	Share	Amount	Share
Lost or stolen cards	76.4	31.1	76.1	31.4	0.3	9.5
Intercepted cards	1.5	0.6	1.4	0.6	0.1	3.4
Forged or counterfeit cards	1.4	0.6	1.3	0.6	0.1	1.9
Misappropriated card numbers	164.0	66.7	163.0	67.2	1.0	30.2
Other	2.4	1.0	0.6	0.2	1.8	55.0
Total	**245.7**	**100.0**	**242.4**	**100.0**	**3.3**	**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	971.1	39,404.0	88.9	9,900.5	72.6	12,522.1
Lost or stolen cards	904.3	35,770.9	53.3	4,659.6	16.2	2,960.6
Intercepted cards	14.6	979.3	0.4	101.6	0.3	53.3
Forged or counterfeit cards	30.0	863.0	11.8	1,801.5	42.9	6,945.0
Misappropriated card numbers	17.3	1,321.7	18.4	2,514.5	8.7	1,826.2
Other	4.9	469.1	5.0	823.3	4.5	737.0
Remote payments excluding online	157.8	9,190.4	194.0	13,523.9	37.3	4,577.8
Lost or stolen cards	98.2	5,343.5	11.7	1,036.9	3.7	367.6
Intercepted cards	0.1	4.7	0.1	6.8	0.0	3.2
Forged or counterfeit cards	0.4	77.6	2.9	296.1	1.2	132.0
Misappropriated card numbers	59.0	3,760.1	178.9	12,157.1	32.2	4,066.8
Other	0.1	4.5	0.4	27.0	0.2	8.2
Remote payments online	2,177.9	162,975.9	2,002.0	116,824.5	317.4	26,288.1
Lost or stolen cards	41.8	4,670.2	95.7	6,698.5	16.5	1,538.0
Intercepted cards	0.1	6.2	0.8	33.3	0.1	4.3
Forged or counterfeit cards	4.3	380.9	27.1	2,359.4	6.3	531.2
Misappropriated card numbers	2,131.3	157,883.0	1,876.3	107,599.6	293.6	24,123.5
Other	0.4	35.6	2.1	133.7	0.9	91.1
Withdrawals	109.0	30,786.3	4.2	904.1	44.8	5,833.1
Lost or stolen cards	107.0	30,267.8	3.0	733.2	5.2	805.4
Intercepted cards	1.2	413.6	0.1	19.4	0.3	25.6
Forged or counterfeit cards	0.0	6.5	0.2	23.1	36.5	4,626.0
Misappropriated card numbers	0.1	7.3	0.3	28.8	0.8	101.3
Other	0.7	91.1	0.6	99.6	2.0	274.8
Total	**3,415.8**	**242,356.6**	**2,289.1**	**141,153.0**	**472.1**	**49,221.1**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

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	971.1	39,404.0	27.6	3,275.3	56.6	12,541.2
Lost or stolen cards	904.3	35,770.9	15.9	1,977.9	31.2	6,986.2
Intercepted cards	14.6	979.3	0.5	61.2	0.5	66.4
Forged or counterfeit cards	30.0	863.0	4.2	281.3	16.1	3,579.2
Misappropriated card numbers	17.3	1,321.7	6.6	833.3	7.0	1,609.5
Other	4.9	469.1	0.4	121.6	1.8	299.9
Remote payments excluding online	157.8	9,190.4	19.3	5,806.7	24.6	10,430.6
Lost or stolen cards	98.2	5,343.5	0.5	94.8	1.2	524.8
Intercepted cards	0.1	4.7	0.1	8.6	0.0	5.0
Forged or counterfeit cards	0.4	77.6	0.9	317.1	2.1	782.7
Misappropriated card numbers	59.0	3,760.1	17.7	5,351.5	21.1	9,020.1
Other	0.1	4.5	0.1	34.7	0.2	98.0
Remote payments online	2,177.9	162,975.9	135.5	21,860.6	216.3	38,508.3
Lost or stolen cards	41.8	4,670.2	2.2	267.0	9.0	1,401.5
Intercepted cards	0.1	6.2	0.3	20.7	0.3	43.8
Forged or counterfeit cards	4.3	380.9	4.3	686.0	19.7	3,710.0
Misappropriated card numbers	2,131.3	157,883.0	127.7	20,681.3	185.6	32,879.1
Other	0.4	35.6	1.0	205.6	1.7	474.0
Withdrawals	109.0	30,786.3	3.1	795.0	1.4	557.2
Lost or stolen cards	107.0	30,267.8	2.7	700.7	0.8	222.9
Intercepted cards	1.2	413.6	0.1	24.5	0.0	26.1
Forged or counterfeit cards	0.0	6.5	0.1	24.8	0.4	140.1
Misappropriated card numbers	0.1	7.3	0.2	34.6	0.0	6.7
Other	0.7	91.1	0.0	10.4	0.2	161.4
Total	**3,415.8**	**242,356.6**	**185.5**	**31,737.6**	**298.9**	**62,037.3**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

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	6.5	1,979.0	1.3	361.7	2.6	379.5
Lost or stolen cards	1.0	207.6	0.6	111.6	0.7	139.4
Intercepted cards	0.1	64.3	0.0	3.8	0.0	1.1
Forged or counterfeit cards	0.1	56.6	0.2	72.0	1.3	130.2
Misappropriated card numbers	0.4	34.4	0.3	127.4	0.6	104.5
Other	4.9	1,616.1	0.2	46.8	0.0	4.32
Remote payments excluding online	2.1	321.6	12.4	690.7	3.1	257.6
Lost or stolen cards	0.1	12.3	0.7	27.0	0.2	6.6
Intercepted cards	0.0	1.4	0.0	0.2	0.0	0.1
Forged or counterfeit cards	0.0	2.0	0.2	11.3	0.1	6.3
Misappropriated card numbers	1.8	286.3	11.1	641.0	2.8	243.7
Other	0.2	19.6	0.4	11.2	0.0	0.9
Remote payments online	2.4	849.0	15.3	1,137.9	4.4	420.1
Lost or stolen cards	0.1	29.0	0.5	27.8	0.2	8.2
Intercepted cards	0.0	3.1	0.0	0.9	0.0	0.0
Forged or counterfeit cards	0.1	4.2	0.2	9.2	0.1	5.2
Misappropriated card numbers	1.9	659.1	14.1	1,002.7	4.0	398.2
Other	0.3	153.6	0.5	97.3	0.1	8.5
Withdrawals	0.8	107.0	0.0	0.0	0.0	0.0
Lost or stolen cards	0.4	61.4	0.0	0.0	0.0	0.0
Intercepted cards	0.4	41.1	0.0	0.0	0.0	0.0
Forged or counterfeit cards	0.0	0.0	0.0	0.0	0.0	0.0
Misappropriated card numbers	0.0	4.5	0.0	0.0	0.0	0.0
Other	0.0	0.0	0.0	0.0	0.0	0.0
Total	**11.8**	**3,256.6**	**29.0**	**2,190.3**	**10.1**	**1,057.2**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

T14 Breakdown of third-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	6.5	1,979.0	0.3	93.7	2.8	1,192.1
Lost or stolen cards	1.0	207.6	0.1	63.7	1.0	505.6
Intercepted cards	0.1	64.3	0.0	1.3	0.0	0.4
Forged or counterfeit cards	0.1	56.6	0.0	5.8	1.3	560.8
Misappropriated card numbers	0.4	34.4	0.2	20.9	0.3	100.5
Other	4.9	1,616.1	0.0	2.0	0.2	24.8
Remote payments excluding online	2.1	321.2	0.9	438.4	2.3	1,086.7
Lost or stolen cards	0.1	12.3	0.0	5.5	0.1	32.3
Intercepted cards	0.0	1.4	0.0	0.0	0.0	0.3
Forged or counterfeit cards	0.0	2.0	0.0	3.9	0.4	159.7
Misappropriated card numbers	1.8	286.3	0.9	426.0	1.8	860.5
Other	0.2	19.6	0.0	3.0	0.0	33.9
Remote payments online	2.4	849.0	1.2	500.4	3.8	1,124.9
Lost or stolen cards	0.1	29.0	0.0	0.8	0.1	16.9
Intercepted cards	0.0	3.1	0.0	1.2	0.0	1.7
Forged or counterfeit cards	0.1	4.2	0.0	10.5	0.8	167.8
Misappropriated card numbers	1.9	659.1	1.2	480.6	2.9	926.1
Other	0.3	153.6	0.0	7.3	0.0	12.4
Withdrawals	0.8	107.0	0.0	0.0	0.3	107.3
Lost or stolen cards	0.4	61.4	0.0	0.0	0.0	0.0
Intercepted cards	0.4	41.1	0.0	0.0	0.0	0.0
Forged or counterfeit cards	0.0	0.0	0.0	0.0	0.3	103.1
Misappropriated card numbers	0.0	4.5	0.0	0.0	0.0	0.0
Other	0.0	0.0	0.0	0.0	0.0	4.2
Total	**11.8**	**3,256.2**	**2.4**	**1,032.5**	**9.2**	**3,511.0**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area; UPT – unattended payment terminal.

Fraud statistics for credit transfers

T15 Geographical breakdown of credit transfer fraud

(amount in EUR, share in %)

	2018	
	Amount	Share
France	31,359,143	32
SEPA outside France	56,882,385	58
Non-SEPA	9,065,580	10
Total	**97,307,108**	**100**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

Fraud statistics for direct debits

T16 Geographical breakdown of direct debit fraud

(amount in EUR, share in %)

	2018	
	Amount	Share
France	44,399,031	76
SEPA outside France	13,946,376	24
Total	**58,346,253**	**100**

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

Fraud statistics for cheques

T17 Breakdown by fraud type in 2018

(amount in EUR, share of amount in %, volume in units, average amount in EUR)

	Amount	Share	Volume	Average amount
Misappropriation, replay	14,741,262	3	2,793	5,277
Theft, loss (fake, apocryphal)	252,890,727	56	138,358	1,827
Counterfeiting	36,739,051	8	8,092	4,540
Falsification	145,737,424	33	17,178	8,483
Total	**450,108,464**	**100**	**166,421**	**2,704**

Source: Observatory for the Security of Payment Means.

2015-17 card fraud data – correction

Due to a misinterpretation of the Observatory's methodology by a reporting institution, certain data previously published in the Observatory's annual reports have been corrected. As a result, the domestic fraud (French card and French acceptor) amounts for 2015, 2016 and 2017 have been revised upwards by EUR 19.4 million, EUR 27.4 million and EUR 26.8 million, respectively. The following tables and charts present the various corrections made to the figures published for 2015, 2016 and 2017 based on the amended domestic fraud amounts.

T18 Corrected fraud figures for 2015 to 2017

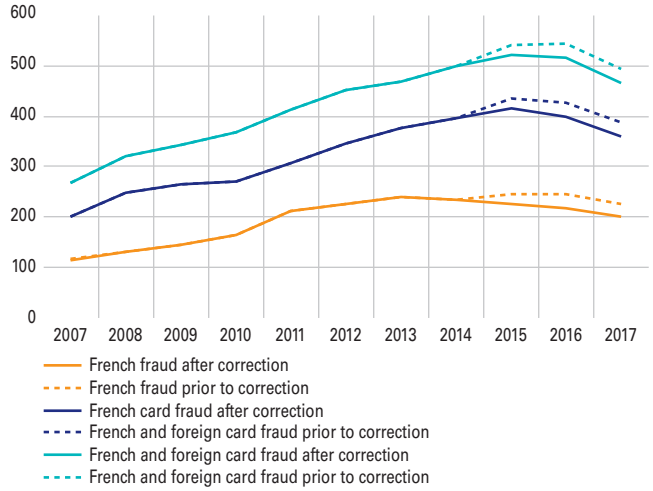
(EUR millions)

	2015	2016	2017
French card – French acceptor	**244.4**	**244.5**	**226.5**
o/w face-to-face and UPT	*43.4*	*33.6*	*35.8*
o/w remote payments excluding online	*9.1*	*9.3*	*7.4*
o/w remote payments online	*152.0*	*165.7*	*148.7*
o/w withdrawals	*39.9*	*35.9*	*34.6*
French card – French and foreign SEPA and non-SEPA acceptors	**435.7**	**426.4**	**387.4**
French and foreign cards – French and foreign SEPA and non-SEPA acceptors	**542.3**	**544.8**	**493.8**

Source: Observatory for the Security of Payment Means.
Note: UPT – unattended payment terminal; SEPA – Single Euro Payments Area.

C1 Change in fraud figures, after correction, for 2015 to 2017

(EUR millions)



Source: Observatory for the Security of Payment Means.

T19 Corrected fraud rate for 2015 to 2017

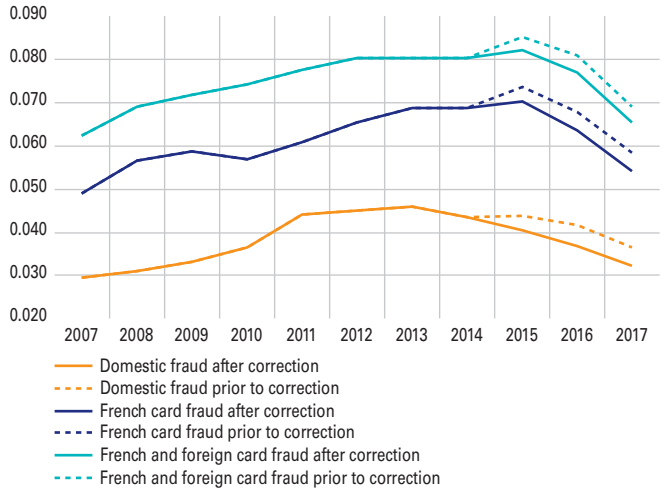
(%)

	2015	2016	2017
Domestic fraud rate – French card, French acceptor	**0.044**	**0.042**	**0.037**
o/w face-to-face and UPT	*0.012*	*0.009*	*0.009*
o/w remote	*0.244*	*0.241*	*0.190*
o/w withdrawals	*0.033*	*0.029*	*0.027*
Fraud rate – French cards and French and foreign SEPA and non-SEPA acceptors	**0.074**	**0.068**	**0.058**
Fraud rate – French and foreign cards and French and foreign SEPA and non-SEPA acceptors	**0.085**	**0.081**	**0.069**

Source: Observatory for the Security of Payment Means.
Note: UPT – unattended payment terminal; SEPA – Single Euro Payments Area.

C2 Change in fraud rate, after correction, for 2015 to 2017

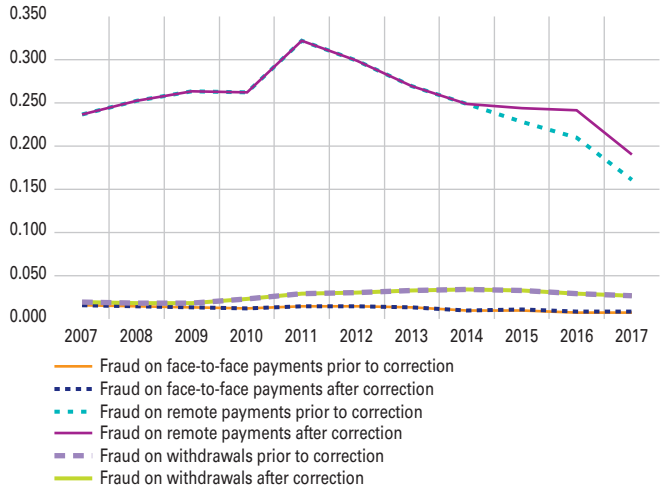
(%)



Source: Observatory for the Security of Payment Means.

C3 Change in domestic fraud rate by transaction type, after correction, for 2015 to 2017

(%)



Source: Observatory for the Security of Payment Means.

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

Managing Editor
Nathalie Aufauvre
Director General, Financial Stability and Market Operations
Banque de France

Editor-in-Chief
Valérie Fasquelle
Director of Payment Systems and Market Infrastructure
Banque de France

Editorial Secretariat
Véronique Bugaj, Olivier Catau, Guylène Chotard,
Caroline Corcy, Tony Dare, Bernard Darrius,
Florian Dintilhac, Christelle Guiheneuc, Trân Huynh,
Julien Lasalle, Lucas Nozahic, Scott Oldale,
Alexandre Stervinou, Mathieu Vileyn

Technical production
Studio Creation
Press and Communication Directorate
Banque de France

Contact
Observatory for the Security of Payment Means
011-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Website
www.observatoire-paiements.fr

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