2013 ANNUAL REPORT
OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

Observatoire
de la sécurité
des cartes de paiement

31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01
Code Courrier : 11-2323

Annual report 2013
of the Observatory for payment card security

addressed to

The Minister of the Economy,
Industrial Renewal and Digital Technology
The Minister of Finance and Public Accounts
The President of the Senate
The President of the National Assembly

by

Christian Noyer,
Governor of the Banque de France,
President of the Observatory for Payment Card Security

*The Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement – *OSCP – hereinafter the Observatory), referred to in section I of Article L. 141-4 of France's* Monetary and Financial Code*, was created by the Everyday Security Act 2001-1062 of 15 November 2001. The Observatory is meant to promote information-sharing and consultation between all parties concerned by the smooth operation and security of card payment schemes (consumers, merchants, issuers and public authorities).*

Pursuant to the sixth indent of the above-mentioned article, the present document reports on the activities of the Observatory. It is addressed to the Ministers of the Economy and Finance and transmitted to Parliament.

NB: For the purposes of its work, the Observatory makes a distinction between "four-party" and "three-party" card payment schemes. Four-party cards are issued and acquired by a large number of payment service providers. Three-party cards are issued and acquired by a small number of payment service providers.

Contents

The 11th Annual Report of the Observatory for Payment Card Security, *covering the 2013 financial year, contains four sections, summarised as follows.*

Part 1: taking stock of measures to protect internet card payments

The pronounced decline in the fraud rate for internet card payments in 2013 testifies to the progress made in enhancing protection in this area.

Virtually all cardholders now have cards that offer strong authentication solutions.

Meanwhile, the failure rate for authenticated transactions has fallen significantly and is now on par with the failure rate for non-authenticated transactions.

This is a very positive signal for merchants and shows that the use of strong authentication is no longer a hindrance to the development of e-commerce.

However, these encouraging developments are being held back by the low proportion – just 43% – of online merchants that support strong authentication solutions.

Accordingly, the Observatory urges all stakeholders to act swiftly to introduce authentication solutions by 1 February 2015, which is the implementation date for the recommendations for the security of internet payments issued by the European forum on the security of retail payments (SecuRe Pay).

Part 2: fraud statistics for 2013

The fraud rate for card payments and withdrawals remained stable at 0.080% in 2013.

However, the steady overall rate masked several different trends:

- *a contained increase in fraud in domestic transactions, characterised by a simultaneous decrease in fraud rates for face-to-face payments and card-not-present (CNP) payments. The fraud rate for internet payments fell for the second year running, declining to 0.229% from 0.290% in 2012, although one-third of the decline is attributable to changes to data collection methods.*[1]

However, the amount of CNP payment fraud continued to rise, particularly in the case of internet payments. CNP payments still account for the lion's share of the amount of fraud (64.6%) but just 11% of the total value of payments. Accordingly, the Observatory urges all participants to keep up their efforts to improve the protection of these payments and reiterates its recommendations to e-merchants to swiftly adopt strong authentication solutions for the most at-risk transactions;

1 A change in the methodology used by the "CB" Bank Card Consortium to assess the breakdown within CNP payments between online payments and those conducted by mail or over the phone (MO/TO) led to a downward revision in the amount of MO/TO payments, with the residual amount being carried over to online payments. As would be expected, this has resulted in a decline in the online fraud rate owing to the increase in the total volume of business.

- *a sharp decline in the fraud rate for international transactions, which concealed contrasting trends.*

The fraud rate for payments in France involving cards issued outside the Single European Payments Area (SEPA) has fallen significantly since 2012, thanks in particular to adoption of the EMV standard by a growing number of countries, with the notable exception of the United States. Fraud rates for face-to-face payments within SEPA have declined steadily since 2011 for the same reason.

Conversely, the fraud rate for CNP payments involving French cards within SEPA rose significantly. Implementation by 1 February 2015 at the latest of SecuRe Pay's recommendations for the security of internet payments should help to fight CNP payment fraud more effectively within SEPA.

Part 3: technology watch on the security of payment terminals and strong cardholder authentication techniques

Security of payment terminals: *given the sharp increase over the last two years in the number of cases where payment terminals have been compromised, the Observatory decided to review the implementation of its previous recommendations for payment terminal security and update its analyses in the light of developments in fraud techniques as presented in its 2012 Annual Report.*

In view of the uptrend in attacks on payment terminals, the Observatory calls on all parties to exercise increased vigilance. In particular, it recommends that the processes used by card payment schemes to approve acceptance devices be strengthened to more effectively manage terminals that are either defective or reaching the end of their life. The Observatory also stresses that efforts to improve hardware traceability must continue and be completed as soon as possible.

Strong cardholder authentication techniques: *since the CNP sales sector remains especially exposed to fraud, the Observatory decided to take stock of the strong authentication techniques implemented by French card payment schemes and issuers.*

Having noted that sending a one-time password by text message to a mobile phone or smartphone is currently the most widely used solution in France, the Observatory calls for continued efforts to make mobile phones more secure for one-time authentication. The Observatory also noted that the huge increase in online payments made using mobile phones might spur the development of other solutions, since text message approaches are not very user-friendly in this type of situation. These alternative solutions include digital wallets, whose security was the subject of recommendations by the Observatory in 2011 and more recently by SecuRe Pay.

Furthermore, the Observatory also notes that recent technological developments aimed at integrating biometric solutions in smartphones could play a role going forward in protecting mobile payments, provided the selected authentication solutions are extremely robust from a security perspective and could not be easily circumvented by exploiting security weaknesses in the biometric solutions or their associated peripheral components. The introduction of security evaluation and certification processes for these elements could help to achieve this outcome.

Part 4: protection of personal data in anti-fraud data processing operations

Against the backdrop of rapid developments in CNP fraud prevention technologies, the Observatory examined the effects of the rules applicable to the processing of personal data in the context of fraud prevention.

In the absence of an equivalent to the EMV standard to protect CNP payments, fraud prevention systems have expanded the scope and nature of personal data gathered during online card payments to increase the level of certainty about the identity of the person initiating the payment transaction. While this has enabled the introduction of more sophisticated and effective data processing operations aimed at fraud prevention, it does raise data privacy issues. For this reason, the French Data Protection Agency (CNIL) is reviewing these new processing operations pursuant to France's data privacy legislation.

The CNIL recently began work on streamlining the disclosure requirements for fraud prevention data processing using personal data. This exercise will provide an opportunity to address the need to clarify the responsibilities of parties using outside service providers, the question of pooling fraud data to improve effectiveness, the possibility, where appropriate, of using new identification data obtained using new technologies, as well as the need to clarify the rules concerning the retention period for personal data in the context of anti-fraud data processing operations. The CNIL's work is expected to lead to the adoption of a "single" authorisation that will offer a more effective framework for gathering and processing data to ensure that fraud prevention, which is a legitimate goal of professionals, is proportionate to individuals' privacy rights.

When it comes to striking this balance, the use of strong cardholder authentication solutions such as 3D-Secure when carrying out the payment may help to limit the need for excessive collection of personal data.

Taking stock of measures to protect internet card payments

The Observatory regularly monitors fraud in card-not-present (CNP) payments as well as the anti-fraud methods deployed by participants in the payment chain.

Among the measures recommended by the Observatory, the most commonly-used approach is the phasing-in of strong cardholder authentication based on one-time codes wherever possible and appropriate.

This chapter describes the progress made in implementing this recommendation (1|) along with initiatives by the Observatory and the Banque de France to make e-merchants more aware about the need to enhance the security of internet payments (2|).

1| Progress in enhancing the security of internet card payments

The security of internet card payments improved markedly in 2013, as the fraud rate decreased by 21%[1] to 0.229% of the total value of transactions (cf. Chapter 2 of this report). While the decline in the fraud rate is encouraging and continues the trend that began in 2012, the rate is still more than 20 times higher than the fraud rate for face-to-face payments.

For this reason, phasing in strong cardholder authentication wherever possible and appropriate remains a priority for the Observatory. Note that this priority has now been taken up at European level, as recommendations issued by SecuRe Pay[2] call for strong authentication to be phased in for the most at-risk internet card payments by 1 February 2015.

Accordingly, the Observatory has been gathering half-yearly statistics from the main banks and their technical providers to monitor the roll-out of authentication solutions.

This statistical monitoring exercise, which covers 57.3 million payment cards and EUR 34.3 billion in payments (including EUR 10.1 billion in payments protected by 3D-Secure[3]), offers a means to measure quantitative and qualitative progress in the implementation of strong authentication solutions.

The seventh data gathering exercise, which covered the period from 1 November 2013 to 30 April 2014, highlighted three key points.

1|1 Almost all cardholders have now been provided with at least one strong authentication solution

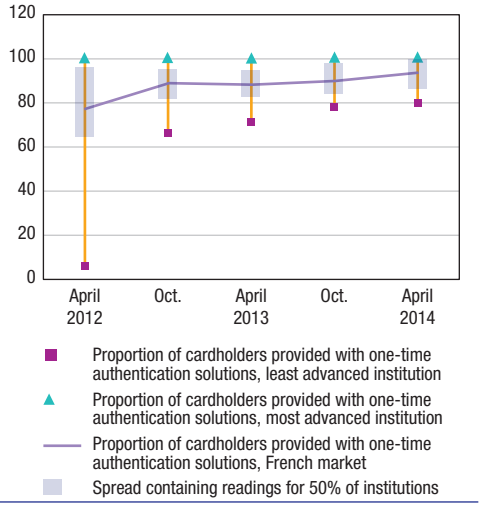
In the space of two years, the average proportion of cardholders provided with at least one functional strong authentication solution has sharply increased, rising from 77.0% to 93.7%. This rate was broadly uniform across surveyed institutions. The rate is close to 100% among cardholders who actually carried out an online payment transaction in the last six months. By far the most common solution is authentication by text message.[4]

1 Part of the decline was due to a change in measurement methodology (cf. Chapter 2 of this report).
2 *https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf*
3 Interbank protocol for the protection of online card payments enabling cardholder authentication.
4 Cf. Chapter 3 of this report: "Stocktaking of strong cardholder authentication techniques".

Chart 1

Distribution of cardholders provided with one-time authentication solutions

(%)

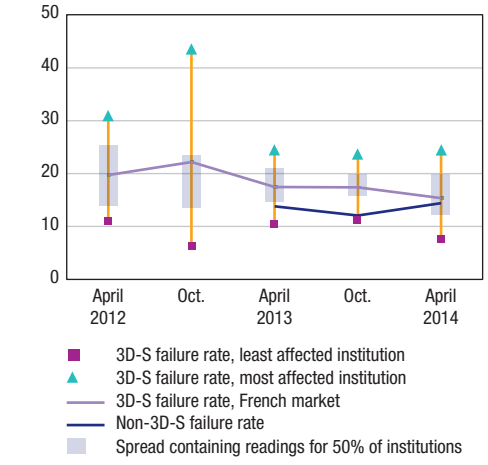


Source: Observatory for Payment Card Security.

Chart 2

Distribution of 3D-Secure (3D-S) failure rates

(%)



Source: Observatory for Payment Card Security.

1|2 The failure rate for transactions subject to strong authentication is drawing closer to the failure rate for non-secured transactions

The Observatory has observed a positive improvement in the failure rate[5] for authenticated payments over the data collection periods, with the rate falling from 18.0% in 2011 to 15.3% during the most recent exercise.

Moreover, the spread in failure rates across surveyed institutions has narrowed sharply, reflecting a better understanding of strong authentication solutions among cardholders, notably thanks to the phasing-in of 3D-Secure by large e-merchants.

As a result, the failure rate for authenticated transactions is now on a par with the rate for non-authenticated transactions, for which data were collected by the Observatory for the first time and which stands at 14.3%. **The Observatory accordingly notes that implementation of strong cardholder authentication wherever possible and appropriate is no longer a hindrance to the development of e-commerce.**

The Observatory will however continue to monitor the positive trend in the failure rate and pursue initiatives aimed at enhancing the protection of online payments, particularly within its e-commerce working group.

1|3 The share of transactions authenticated by 3D-Secure continues to increase in value terms, but the proportion of e-merchants that support the solution remains the same

The share of authenticated transactions went up in value terms from 27.5% to 29.7% over the space of a year. This increase may explain the decrease in the online fraud rate in 2013.

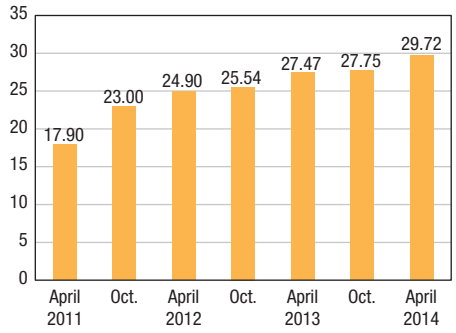
Even so, the proportion of e-merchants that support strong authentication solutions remained unchanged at around 43%, which is viewed as too low for the purposes of fraud prevention.

5 Causes of failure include cases where the cardholder abandons his or her attempt (all causes), technical problems (all causes), attempted fraud, and incorrect data entry.

Chart 3

Proportion of 3D-Secure payments (value terms)

(%)



Source: Observatory for Payment Card Security.

2| Initiatives conducted by the Observatory and the Banque de France to encourage e-merchants to enhance the security of internet payments

The Banque de France and the "CB" Bank Card Consortium pursued initiatives undertaken in 2013 under the aegis of the Observatory, notably conducting bilateral meetings with e-merchants suffering especially high amounts and/or rates of fraud.

The aim was to raise awareness among e-merchants and their payment service providers about the question of fraud in CNP sales and to establish action plans to lower fraud rates, notably by deploying strong authentication for the highest-risk payments.

The following conclusions emerged from the latest round of meetings:

• aside from its financial impact, internet payment fraud hinders the development of e-commerce more broadly by affecting its image and undermining confidence among internet users, and by raising fears among professionals of damage to their business resulting from an organised attack and massive compromise of payment data. Accordingly, fraud prevention is identified as a strategic challenge;

• interviewed e-merchants suffering from high rates of fraud agreed to deploy strong cardholder authentication solutions, at least for the highest-risk transactions. High-risk transactions are typically identified using transaction scoring tools;[6]

• e-merchants that had experienced spikes in fraud acknowledged the effectiveness of strong cardholder authentication, in particular when activated using a risk-based approach.

E-merchants also highlighted three ways to further improve fraud prevention in internet card payments:

• difficulties in implementing text message-based strong authentication with new sales channels such as mobile sales (smartphones) have created the need for new authentication solutions that can be used with all sales channels. Pending the emergence of these new solutions, e-merchants said that digital wallets could address the need to protect the mobile sales channel under certain conditions;[7]

• the use by issuers of weak authentication methods (e.g. authentication using a static password such as a birthday), generally for small value transactions, may be the cause of some fraud. Although e-merchants are still guaranteed payment in the event of fraud resulting from such weak authentication methods, identifying the type of authentication used in the messages processed by payment systems could help to make systems for analysing transactions more reliable;

• some e-merchants once again pointed[8] to the problems posed in some sectors by the use of anonymous prepaid cards and reiterated their request to be able to identify prepaid cards in order to monitor them more carefully.

6 Cf. Chapter 4 of this report on the protection of personal data in the context of fraud prevention systems.
7 Cf. Chapter 3 of the 2011 report: "Digital wallets and card payments".
8 Cf. Chapter 1 of the 2012 Annual Report: "Stocktaking of measures to protect internet card payments".

3| Conclusion

The most recent data gathering exercise conducted by the Observatory among banks and their technical service providers reveals **a substantial decline in the fraud rate for internet card payments, which may be attributable to the increased proportion in value terms of payments protected by strong authentication.**

Noting that the failure rate for authenticated payments is no longer a hindrance to the implementation of strong authentication and that the fraud rate for internet payments remains almost 20 times higher than the level for face-to-face payments, **the Observatory urges all payment chain participants to keep up efforts to enhance the security of internet payments.**

Given that only 43% of e-commerce websites support strong authentication, the widespread introduction by merchants of these solutions remains a priority for the Observatory. These measures are now being taken forward within a European framework as the SecuRe Pay forum has issued recommendations calling for the wide-scale adoption of strong cardholder authentication for internet payments wherever possible and appropriate **by 1 February 2015.**

Fraud statistics for 2013

The Observatory has compiled fraud statistics for three-party and four-party cards since 2003, using data collected from issuers and merchants. The statistics use harmonised definitions and typologies that were established in the Observatory's first year of operation and that are provided in Appendix 6 to this report. A summary of the 2013 statistics is presented below. It includes an overview of the different fraud trends for three-party cards and four-party cards, fraud trends for domestic and international, face-to-face and card-not-present (CNP) transactions, as well as payment and withdrawal transactions, and fraud trends for different types of fraud involving lost or stolen cards, intercepted cards, forged or counterfeit cards, and misappropriated card numbers.

In addition, Appendix 5 to this report presents a series of detailed fraud indicators.

Note also that on 25 February 2014 the European Central Bank (ECB) published the third Eurosystem report[1] on payment card fraud within the European Union (EU), covering the period from 2008 to 2012.

While the methodologies used by the Observatory and the Eurosystem are very similar overall, it is important to note the differences before comparing the main published indicators:

- the ECB report only takes account of fraud in transactions (payments and withdrawals) made using

Box 1

Fraud statistics: respondents

In order to ensure the quality and representativeness of its fraud statistics, the Observatory gathers data from all issuers of four-party and three-party cards.

The statistics calculated by the Observatory thus cover:

- *EUR 532.2 billion in transactions in France and in other countries made with 68.4 million four-party cards issued in France (including 1.87 million electronic purses and 20.2 million contactless cards);*
- *EUR 17 billion in transactions primarily in France made with 17.1 million three-party cards issued in France;*
- *EUR 37.3 billion in transactions in France made with foreign three-party and four-party cards.*

Data were gathered from:

- *ten three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance (Finaref and Sofinco), Cofidis, Cofinoga, Diners Club, Franfinance, JCB and UnionPay International;*
- *the 130 members of the "CB" Bank Card Consortium. The data were collected through the consortium, and from MasterCard and Visa Europe France;*
- *issuers of Moneo, an electronic purse.*

1 Report available in English on the ECB website: *http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf*

cards issued within SEPA whereas the Observatory also considers fraud in transactions carried out in France using cards issued outside of SEPA;

• the Observatory also counts the fraudulent opening of accounts (e.g. opening an account using fake personal and proof of address data) among payment card fraud techniques, while the ECB considers this as credit fraud.

1| Overview

The total value of card payments amounted to EUR 586.5 billion in 2013, up 4.4% compared with 2012. The annual growth rate was slightly lower than in 2012 (5.2%) and below the five-year average (5.5%).

The total amount of fraud increased by a similar amount, rising 4.3% compared with 2012 to reach EUR 469.9 million in 2013.

As a result, the fraud rate for card payments and withdrawals in 2013 recorded by French schemes was unchanged at 0.080%, after increasing for five years in a row.

The rate of issuer fraud, which covers all fraudulent payments and withdrawals made in France and in other countries with cards issued in France, was 0.069% in 2013, and issuer fraud totalled EUR 376.6 million (compared with 0.065% and EUR 345.2 million in 2012).

The rate of acquirer fraud, which covers all fraudulent payments and withdrawals made in France with all cards, regardless of their geographical origin,[2] fell slightly to 0.059% in 2013, and acquirer fraud totalled EUR 331.9 million (compared with 0.062% and EUR 331.8 million in 2012).

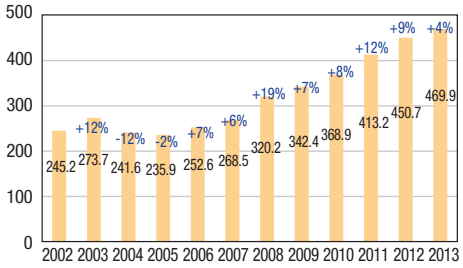
The number of cards for which at least one fraudulent transaction was recorded in 2013 climbed by 12% compared with 2012 to 861,000.

The average value of a fraudulent transaction fell to EUR 116 from EUR 125 in 2012.

Chart 2

Amount of fraud

(EUR millions)

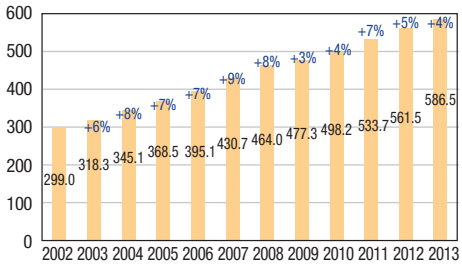


Source: Observatory for Payment Card Security.

Chart 1

Value of transactions

(EUR billions)

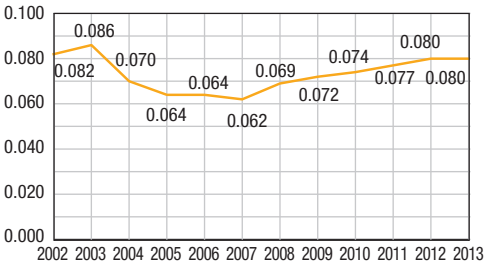


Source: Observatory for Payment Card Security.

Chart 3

Fraud rate all card and transaction types

(%)



Source: Observatory for Payment Card Security.

2 Because cards issued in France are counted twice, i.e. in issuer and acquirer fraud, the sum of issuer fraud (EUR 376.6 million) and acquirer fraud (EUR 331.9 million) is greater than the total amount of fraud (EUR 469.9 million). Similarly, the average issuer fraud rate (0.069%) and acquirer fraud rate (0.059%) is lower than the average fraud rate (0.080%) because both fraud rates include domestic transactions, which have the lowest fraud rate (0.046% compared with 0.350% for international transactions – see Table 2 on the geographical breakdown of fraud).

2| Breakdown of fraud by card type

The fraud rate for four-party cards was unchanged from 2012 at 0.080% in 2013, after rising for five years in a row. The fraud rate for three-party cards was 0.065% in 2013 (compared with 0.076% in 2012), declining for the second year running after increasing for four consecutive years.

Issuer and acquirer fraud rates for four-party cards were 0.069%[3] and 0.060%[4] respectively, compared with 0.066% and 0.062% in 2012. The average value of a fraudulent transaction was EUR 113, after EUR 122 in 2012.

Issuer and acquirer fraud rates for three-party cards were 0.044%[5] and 0.057%[6] respectively, compared with 0.051% and 0.068% in 2012. The average value of a fraudulent transaction was EUR 352 in 2013, after EUR 344 in 2012.

Table 1

Breakdown of fraud by card type

(% rate, amounts in EUR millions)

	2009	2010	2011	2012	2013
Four-party cards	0.072 (324.3)	0.074 (351.5)	0.077 (394.9)	0.080 (434.4)	**0.080 (455.8)**
Three-party cards	0.068 (18.2)	0.080 (17.4)	0.083 (18.3)	0.076 (16.3)	**0.065 (14.0)**
Total	0.072 (342.4)	0.074 (368.9)	0.077 (413.2)	0.080 (450.7)	**0.080 (469.9)**

Source: Observatory for Payment Card Security.

3| Geographical breakdown of fraud

The amount of fraud in international transactions (EUR 231.3 million in 2013) remains slightly lower than fraud in domestic transactions (EUR 238.6 million in 2013). Even so, because

Table 2

Geographical breakdown of fraud

(% rate, amounts in EUR millions)

	2009	2010	2011	2012	2013
Domestic transactions	**0.033 (144.0)**	**0.036 (163.8)**	**0.044 (211.5)**	**0.045 (226.4)**	**0.046 (238.6)**
International transactions	**0.449 (198.4)**	**0.423 (205.0)**	**0.367 (201.7)**	**0.380 (224.3)**	**0.350 (231.3)**
– o/w French issuer and foreign acquirer[a)]	0.594 (121.6)	0.728 (54.9)	0.638 (51.0)	0.759 (62.5)	0.688 (70.2)
– o/w French issuer and SEPA acquirer	–	0.331 (50.6)	0.255 (44.3)	0.316 (56.3)	0.366 (67.9)
– o/w foreign issuer[b)] and French acquirer	0.324 (76.8)	0.831 (64.5)	0.892 (81.3)	0.639 (78.2)	0.404 (64.1)
– o/w SEPA issuer and French acquirer	–	0.195 (35.0)	0.122 (25.1)	0.132 (27.3)	0.135 (29.1)
Total	**0.072 (342.4)**	**0.074 (368.9)**	**0.077 (413.2)**	**0.080 (450.7)**	**0.080 (469.9)**

a) Non-SEPA acquirer only from 2010.
b) Non-SEPA issuer only from 2010.
Source: Observatory for Payment Card Security.

3 The issuer fraud rate for four-party cards is lower than the average fraud rate for cards of the same type because the latter additionally includes transactions carried out in France with cards issued abroad, which have a higher fraud rate than that of transactions carried out using French cards in all countries.

4 The acquirer fraud rate for four-party cards is lower than the average fraud rate for cards of the same type because the latter additionally includes transactions carried out abroad using cards issued in France, which have a higher fraud rate than that of transactions carried out in France using cards issued in all countries. See also note 2 regarding average issuer and acquirer fraud rates.

5 See note 3 regarding four-party cards, which also applies to three-party cards.

6 See note 4 regarding four-party cards, which also applies to three-party cards.

of the transaction values involved, the fraud rate for international transactions, at 0.350%, was still around eight times higher than the rate for domestic transactions (0.046%).

International transactions thus account for 49.2% of the total amount of fraud, even though they make up just over 11.3% of the total value of card transactions.

Fraud remained lower for transactions carried out within SEPA compared with transactions in countries outside SEPA, although the gap is narrowing thanks to efforts made by countries around the world, with the notable exception of the United States, to migrate cards and terminals to the EMV standard. Work in France aimed at improving the detection of attempted fraud targeting non-SEPA transactions has also helped reduce the gap:

• the fraud rate for transactions in France using foreign cards issued outside SEPA (0.404%) is three times higher than the rate for transactions carried out using foreign cards issued in SEPA (0.135%);

• the fraud rate for transactions outside SEPA with cards issued in France (0.688%) is around two times higher than the rate for transactions conducted within SEPA with the same types of cards (0.366%).

These results reward the efforts made over recent years in Europe to migrate cards and payment terminals to the EMV standard.

In this regard, note that in 2012, Visa, MasterCard, American Express and Discover (Diners Club International) announced a set of incentives to encourage EMV adoption in the United States by October 2015 at the latest (see Chapter 2, 3|, page 20 of the 2012 Annual Report).

4| Breakdown of fraud by transaction type

The Observatory's classification of card payment transactions distinguishes face-to-face payments and unattended payment terminal (UPT) payments made at a point of sale (POS) or at fuel pumps, ticket machines, etc., from CNP payments made on the internet, by post, telephone, fax, etc., and withdrawals. For the sake of clarity, the following section distinguishes national data from cross-border data.

In the case of domestic transactions (cf. Table 3), the figures show that:

• the fraud rate for face-to-face and UPT payments decreased to 0.013%. These types of payments accounted for over 66% of the value of domestic transactions but just 19% of the total amount of fraud.

The fraud rate for withdrawals increased by 6% compared with 2012 to 0.033%. This mainly reflected the continued high number of attacks on automated teller machines (ATMs) – approximately 1,000 in 2013 – and POS (about 200 in 2013, or twice as many as in 2012), which have become preferred targets for organised fraud rings, and the continued high number of thefts of cards with PINs.

In response to the continuation of trends that were already in evidence in 2011 and 2012, the Observatory once again urges cardholders to be on their guard and apply the recommended best practices when making payments to a merchant or when making withdrawals (see Appendix 1).

• the fraud rate for CNP payments fell to 0.269%, but was still 20 times higher than the rate for face-to-face payments. The fraud rate for internet payments, in particular, declined to 0.229% from 0.290% in 2012,[7] while the rate for payments by mail or phone remained at a higher level (1.122% in 2013). The results for internet payments reflect efforts by issuers and e-merchants to deploy solutions such as 3D-Secure that enable strong cardholder authentication for the most at-risk payments. Amid sustained growth in electronic commerce, CNP payments accounted for just 11% of the value of domestic transactions but for 64.6% of the total amount of fraud.

In view of the level of fraud recorded through this payment channel, the Observatory reiterates its recommendations aimed at encouraging e-merchants,

7 Approximately one-third of this decline was however attributable to a methodological change made in 2013. See note to Table 3.

Table 3

Breakdown of domestic fraud by transaction type

(% rate, amounts in EUR millions)

	2009	2010	2011	2012	2013
Payments	0.038 (123.2)	0.041 (137.3)	0.049 (177.8)	0.049 (190.0)	0.050 (199.9)
o/w face-to-face and UPT	0.014 (41.0)	0.012 (36.2)	0.015 (48.1)	0.015 (51.2)	0.013 (45.8)
o/w card-not-present	0.263 (82.2)	0.262 (101.1)	0.321 (129.6)	0.299 (138.8)	0.269 (154.2)
o/w by post/phone	*0.263* *(30.3)*	*0.231* *(27.3)*	*0.259* *(25.4)*	*0.338* *(29.4)*	*1.122* [a] *(29.2)*
o/w internet	*0.263* *(51.9)*	*0.276* *(73.9)*	*0.341* *(104.2)*	*0.290* *(109.4)*	*0.229* *(125.0)*
Withdrawals	0.019 (20.8)	0.024 (26.5)	0.029 (33.7)	0.031 (36.4)	0.033 (38.6)
Total	**0.033** **(144.0)**	**0.036** **(163.8)**	**0.044** **(211.5)**	**0.045** **(226.4)**	**0.046** **(238.6)**

a) The sharp increase compared with 2012 in the fraud rate for CNP payments made by post or phone is largely attributable to the change in the methodology used by the "CB" Bank Card Consortium to measure the share of such transactions within CNP transactions. The correction led to a sharp downward revision in their amount, which was divided by approximately three, with online payments increasing commensurately. The same methodological change accounted for about one-third of the decline in the fraud rate for internet payments, with the other two-thirds reflecting fraud prevention efforts by participants in 2013.
Source: Observatory for Payment Card Security.

particularly the largest ones, to deploy solutions such as 3D-Secure that enable strong authentication of cardholders for the most at-risk payments (cf. Chapter 1 of this report).

In the case of international transactions (cf. Table 4), the Observatory only has a detailed breakdown of fraud by transaction type for transactions made with French cards in other countries.

Fraud in CNP payments to foreign e-merchants made using French cards surged to EUR 81.2 million in 2013 compared with EUR 61.6 million in 2012. One explanation for this may be that criminals have shifted their focus to target foreign e-merchant websites as online commerce sites in France have phased in solutions to protect internet payments.

Fraud rates for CNP payments were especially high outside SEPA (0.848%), but there was also a sharp increase in the fraud rate for CNP payments made using French cards within SEPA (0.937% in 2013 compared with 0.735% in 2012). The deployment of strong authentication solutions, spurred on by the recommendations of the SecuRe Pay forum (see Chapter 1), should however help to reverse this trend in SEPA.

There was a decline in fraud in face-to-face payments and withdrawals using French cards within SEPA, where EMV has now been extensively adopted.

5| Breakdown by fraud type

The Observatory breaks down fraud into the following types:

- lost or stolen cards that fraudsters use without the knowledge of the lawful cardholders;
- intercepted cards stolen when issuers mail them to lawful cardholders;
- forged or counterfeit cards, when an authentic payment card is forged by modifying magnetic stripe data, embossing or programming. A counterfeit card is produced using data gathered by the fraudster;

Table 4

Breakdown of international fraud by transaction type

(% rate, amounts in EUR millions)

French issuer – Foreign acquirer	2010	2011	2012	2013
Payments	0.795	0.561	0.687	0.547
	(39.8)	(30.5)	(37.8)	(40.3)
o/w face-to-face and UPT	0.655	0.369	0.456	0.377
	(25.8)	(16.0)	(19.8)	(17.7)
o/w card-not-present	1.310	1.320	1.551	0.848
	(14.0)	(14.5)	(18.0)	(22.6)
o/w by post/phone	*1.193*	*1.011*	*1.150*	*1.234*
	(3.8)	*(3.1)*	*(4.0)*	*(6.4)*
o/w internet	*1.360*	*1.440*	*1.720*	*0.751*
	(10.2)	*(11.4)*	*(14.1)*	*(16.2)*
Withdrawals	0.596	0.800	0.904	1.054
	(15.1)	(20.5)	(24.7)	(29.9)
Total	**0.728**	**0.638**	**0.759**	**0.688**
	(54.9)	**(51.0)**	**(62.5)**	**(70.2)**
French issuer – SEPA acquirer				
Payments	0.396	0.300	0.372	0.434
	(49.1)	(43.1)	(55.3)	(66.8)
o/w face-to-face and UPT	0.112	0.140	0.131	0.089
	(9.2)	(12.6)	(11.7)	(8.2)
o/w card-not-present	0.944	0.571	0.735	0.937
	(40.0)	(30.5)	(43.6)	(58.6)
o/w by post/phone	*0.566*	*0.643*	*0.532*	*1.566*
	(4.0)	*(5.6)*	*(6.5)*	*(11.3)*
o/w internet	*1.021*	*0.557*	*0.788*	*0.856*
	(36.0)	*(24.9)*	*(37.1)*	*(47.3)*
Withdrawals	0.052	0.040	0.036	0.036
	(1.5)	(1.2)	(1.1)	(1.1)
Total	**0.331**	**0.255**	**0.316**	**0.366**
	(50.6)	**(44.3)**	**(56.3)**	**(67.9)**
Foreign issuer – French acquirer				
Payments	0.982	1.056	0.739	0.451
	(63.2)	(80.7)	(77.7)	(63.2)
Withdrawals	0.103	0.042	0.033	0.051
	(1.4)	(0.6)	(0.6)	(0.9)
Total	**0.831**	**0.892**	**0.639**	**0.404**
	(64.5)	**(81.3)**	**(78.2)**	**(64.1)**
SEPA issuer – French acquirer				
Payments	0.239	0.155	0.158	0.158
	(33.8)	(24.3)	(26.6)	(28.2)
Withdrawals	0.032	0.017	0.017	0.025
	(1.2)	(0.8)	(0.7)	(0.9)
Total	**0.195**	**0.122**	**0.132**	**0.135**
	(35.0)	**(25.1)**	**(27.3)**	**(29.1)**

Source: Observatory for Payment Card Security.

Box 2

Domestic fraud rate for CNP sales, by sector of activity

The Observatory has gathered data that provide information about the distribution of fraud in CNP payments by sector.[1] These data cover domestic transactions only.

Table
Domestic fraud in CNP payments, by sector of activity

(amounts in EUR millions, % shares)

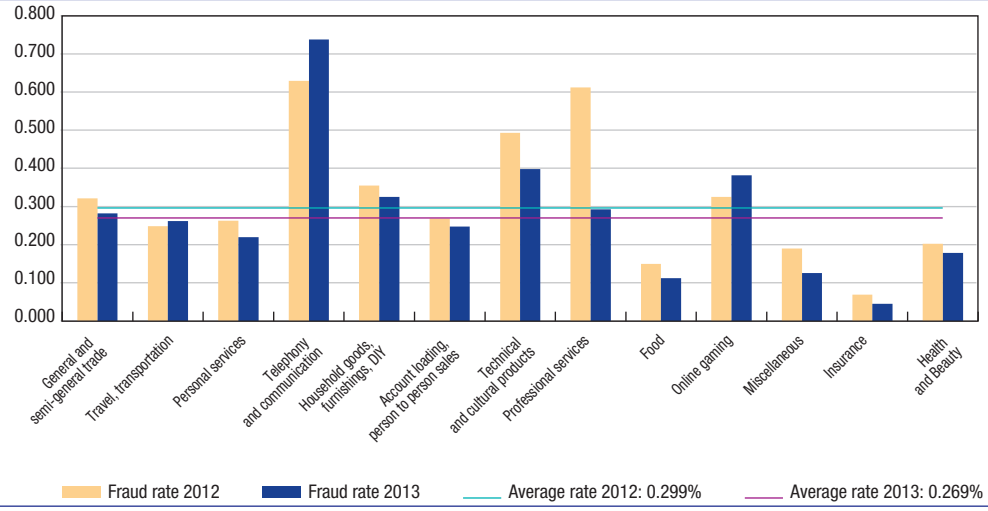
Sector	Fraud amount	Sector share of fraud
General and semi-general trade	32.1	21.1
Travel, transportation	31.0	20.3
Personal services	27.6	18.1
Telephony and communication	17.9	11.8
Household goods, furnishings, DIY	12.9	8.5
Account loading, person to person sales	9.4	6.2
Technical and cultural products	7.1	4.7
Professional services	4.1	2.7
Food	3.6	2.4
Online gaming	3.4	2.3
Miscellaneous	2.5	1.6
Insurance	0.4	0.3
Health and Beauty	0.2	0.1
Total	**152.3**	**100.0**

The general and semi-general trade, travel/transportation, personal services and telephony and communication sectors were the most exposed to internet fraud, accounting for 71% of the total. A comparison of average fraud rates for each sector of activity provides additional information, revealing that some sectors, including technical and cultural products and online gaming, have considerable exposure despite accounting for a small portion of the total fraud amount.

Fraud rates were down in all sectors with the notable exception of telephony and communication and online gaming, which have also had persistently higher-than-average fraud rates. The Observatory calls on firms in these two sectors to step up fraud prevention measures.

Chart
Domestic fraud rates in CNP payments, by sector of activity

(%)



1 *Cf. Appendix 6 for sector descriptions.*

• misappropriated card numbers, when a card number is copied without the cardholder's knowledge or created through card generation processes (which use programs to generate random card numbers) and then used for CNP transactions;

• "other" fraud, which covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts by means of identity theft.

Chart 4 shows national fraud trends for all payment cards. The breakdown covers payments only.

Fraud involving the use of misappropriated card numbers for CNP payments is the most common type of fraud (64.6%) and increased slightly compared with 2012.

Accordingly, the Observatory reiterates its recommendation that e-merchants roll out solutions such as 3D-Secure that enable strong authentication of cardholders.

After increasing in 2011, fraud involving lost or stolen cards fell in 2012 and declined further in 2013, from 34.9% to 34.2% of fraudulent domestic payments.

Counterfeit cards accounted for just 0.2% of fraudulent domestic payments, falling sharply in comparison with 2012 (2.6%). The decrease is mainly attributable to the adoption of smartcard technologies by a number of three-party card schemes and by enhanced security for existing EMV smartcards.[8]

"Other" fraud was down. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for a substantial percentage (around 33%) of the fraud involving these cards.

Table 5

Breakdown of domestic payment fraud by fraud type and by type of card in 2013

(amounts in EUR millions, % shares)

	All types of cards		Four-party cards		Three-party cards	
	Amount	Share	Amount	Share	Amount	Share
Lost or stolen cards	81.7	34.2	81.0	34.6	0.6	14.7
Intercepted cards	0.9	0.4	0.6	0.3	0.3	7.4
Forged or counterfeit cards	0.5	0.2	0.2	0.1	0.3	6.5
Misappropriated numbers	154.0	64.6	152.3	65.1	1.7	38.5
Other	1.5	0.6	0.0	0.0	1.5	32.9
Total	238.6	100.0	234.1	100.0	4.4	100.0

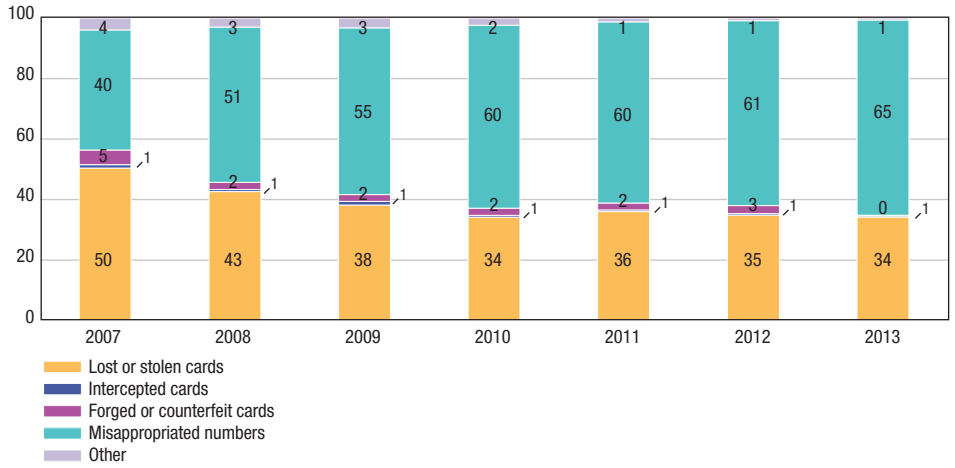
Source: Observatory for Payment Card Security.

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

Chart 4

Breakdown by fraud type (domestic transactions, fraud amount)

(%)



Source: Observatory for Payment Card Security.

Box 3

Indicators provided by law enforcement agencies

In 2013, law enforcement agencies recorded a further decrease in arrests connected with bank card fraud, reporting 103 arrests, compared with 122 in 2012, 234 in 2011, 235 in 2010, 190 in 2009 and 154 in 2008. The decline reflects stiffer prison sentences being handed down by the courts, which caused counterfeiting of foreign bank cards to fall sharply from end-2011 onwards.

ATM attacks fell slightly to 1,028 in 2013, compared with 1,109 in 2012, 634 in 2011, 527 in 2010, 526 in 2009, 427 in 2008, 411 in 2007, 526 in 2006, 200 in 2005 and 80 in 2004. There were also 188 attacks on POS (compared with 91 in 2012 and 30 in 2011) including 85 on payment terminals (60 in 2012) and 103 on card-operated fuel pumps (31 in 2012). These figures corroborate the statistical uptrend noted by the Observatory in fraud in withdrawals and CNP payments made outside SEPA using French cards.

Technology watch

1| The security of payment terminals

Payment terminals evolve regularly, reflecting technological changes connected with payment cards (in particular the growing use of the near field communication – NFC – protocol), the use of new devices such as mobile phones (which can also be used in NFC contactless mode) to initiate payments, and, more recently, the development of solutions that can turn mobile phones into payment terminals, meeting the need to expand the options for card acceptance in environments where conventional payment terminals have yet to establish themselves.

The Observatory has examined several of these developments in recent years, looking in particular at unattended payment terminal (UPT) networks (2008 Annual Report, Chapter 3, p. 35), "thin" payment terminals (2009 Report, Chapter 3, p. 36) and mobile phones as payment terminals (2011 Report, Chapter 3, p. 29).

Given the sharp increase over the last two years in the number of cases where payment terminals have been compromised (188 attacks on point of sale – POS – in 2013 compared with just 30 in 2011), the Observatory decided as part of its 2013-2014 work programme to review implementation of its previous recommendations for the security of payment terminals and update its analyses in the light of developments in fraud techniques as presented in its 2012 Annual Report (Chapter 3, 2|, p. 31).

1|1 Recap of the different types of payment terminals

Electronic payment terminals (EPTs) enable a merchant with a physical POS to accept card payments. They typically have several interfaces for interacting with the holder's payment instrument:[1] a smartcard coupler, a magnetic stripe reader, an NFC antenna if the terminal supports contactless payments, plus a keypad to enter the personal identification number (PIN) associated with the payment instrument and a printer to generate the customer's receipt. They display information for the holder and for the merchant (for example, the payment amount and the result of the authorisation request), recognise and approve the payment instrument, and transmit transaction data to the acquirer's servers.

Some models also accept a handwritten signature by the holder or offer biometric recognition functions to identify the holder.

There are usually considered to be two types of payment terminals:

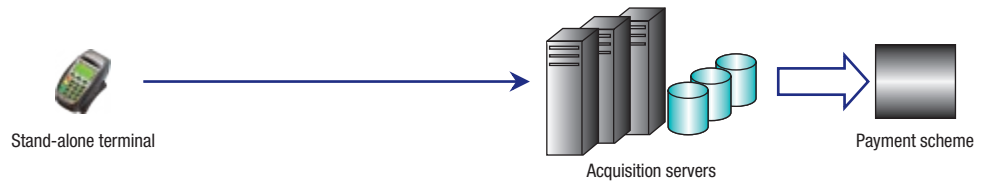
• stand-alone EPTs: these are dedicated solely to payment transactions. They are sophisticated devices that can conduct numerous checks to verify the authenticity of the card and its holder. They interact with the chip on the payment instrument and activate complex cryptographic control mechanisms to determine whether the card is valid and whether the holder is truly the card's owner. They also implement the processing operations required to approve payments, including in offline mode, and dialogue directly with the acquisition servers of the merchant's acquiring institution;

• clustered or concentrated EPTs: these chiefly perform the functions required to interface with the payment instrument and the holder, including cryptographic control mechanisms. Most of the other security functions (for example, checks to see that the instrument is valid) are executed on a remote electronic payment concentrator to which the terminal is connected at all times. The concentrator, which may be located with the merchant or an external service provider, provides the link to the acquiring servers of the merchant's acquiring institution. This approach lowers costs and facilitates the management of application changes in situations where the merchant has several acceptance points (e.g. several cash registers) because modifications can be carried out in a centralised manner either by conducting an update on the

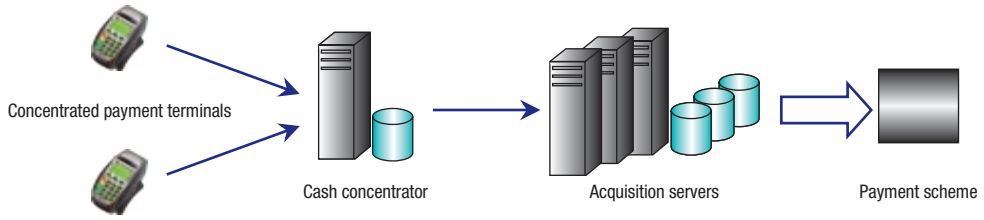
1 Most often a card or, where applicable, a mobile phone.

Box 1

Operating principle: stand-alone terminal



Operating principle: clustered or concentrated terminals



server or by updating all the terminals from the server. Terminals operating in this mode are mainly used by large retailers, motorway toll stations, and automated fuel pumps. Solutions used to turn a smartphone into an acceptance system for card payments are generally counted in this category.

1|2 Recap of the main risks and measures used to protect against them

For more information on this topic, see the chapter on fraud techniques in the Observatory's 2012 Annual Report (Chapter 3, p. 31). To briefly recap, attacks on payment terminals may be physical or logical and may target the terminal directly, the link used to exchange data between the terminal and the cash concentrator, or even the cash concentrator itself.

Direct attacks on terminals may seek to:

- capture data that are then used to counterfeit payment cards or make fraudulent CNP payments;
- fool the merchant into thinking that the payment was approved;
- force the payment terminal to accept a payment made using a counterfeit and/or forged card, by disabling the control functions that should have caused the payment to be rejected;
- modify the transaction amount.

Measures implemented to protect terminals against physical attacks may be based on:

- protection against physical access to the terminal's internal components;
- measures to combat the introduction of malware;
- network protection measures, particularly in the case of concentrated terminals;
- measures to prevent substitution of payment terminals at the POS;
- guidelines for cardholders and merchants on exercising vigilance.

All card payment schemes operating in France require payment terminals to be approved before their use by merchants to accept payments made with cards

issued by members of the scheme. This approval is based on a prior security evaluation of the hardware with respect to the requirements established by the card payment scheme operator. The evaluation is intended to ensure that the protection mechanisms implemented by the manufacturer for the specific terminal model comply with the said requirements and meet the requisite level of robustness.

1|3 Review of the implementation of the Observatory's previous recommendations (2008 to 2012)

1|3|1 Terminal approval process

In the CB scheme, the "CB" Bank Card Consortium sets the approval admissibility requirements for payment terminals, which include, among other things:

- EMV Level 2[2] compliance assessed by an EMV testing firm;

- compliance with the CB electronic payment manual, which sets out the functional requirements that apply to payment terminals for payment acceptance under the CB standard;

- compliance with the Payment Card Industry – PIN Transaction Security Point of Interaction (PCI[3] PTS POI) standard, whose aim is to protect the holder's PIN and account data within the terminal.

In practice, these rules are compatible with the approval rules used by the international card payment schemes.

Approval is extended whenever the associated certifications are renewed. If a security or functional certification expires, the approved product changes status and may no longer be marketed. Card payment scheme operators may also set end-of-life dates for terminals.

These rules seek to ensure that the level of physical protection for approved payment terminals guarantees a high level of security for processed data.

The rules also apply to solutions used to turn a smartphone into a payment terminal. In its 2011 Annual Report, the Observatory conducted a study on the appearance of these acceptance methods and noted that since smartphones are inherently multi-application, multi-tasking devices without secure elements, they are in principle ill-suited to the customary requirements for conventional payment terminals, which are specifically designed for their function. In particular, unless smartphones are connected to a specific device, the question of full compliance with PCI security requirements remains outstanding (for more details, see the 2011 Annual Report, Chapter 3, p. 29).

Certification and approval processes cover *"recognition of the latest developments"*, as previously recommended by the Observatory. Checks are based on evaluations performed by testing firms, which are chosen by terminal manufacturers using criteria established by card payment scheme operators in accordance with the methodologies stipulated in the standards. In June 2013, the new version of the PCI PTS POI standard introduced a more in-depth analysis of source code, although this task is complicated by the lack of an effective tool to automate the process and by the high costs associated with a manual analysis.

Security standards do include requirements in terms of *"enhancing the security of payment terminal operating systems, in particular by deactivating or eliminating software components and unused functionalities and by setting up access restrictions for certain data"*, as previously recommended by the Observatory. However, as well as hosting card payment schemes' payment applications, terminals also host third-party applications developed for merchants, for example to manage loyalty programmes, and these applications are not currently covered by the scope of certification.

2 EMV Level 2 compliance covers in particular the process for selecting the payment card application and also encompasses EMV Level 1, which covers physical and electrical compliance of components.

3 PCI standards are set by the Payment Card Industry Security Standards Council (PCI SSC) founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

The *"performance of regular tests including the operating system and the applications housed on payment terminals to continually assess the overall level of security and the ability to withstand attacks"*, which was previously recommended by the Observatory, is not currently required by card payment scheme operators in their approval processes and in practice this type of testing is done only during the product's initial evaluation.

The Observatory notes however that the rules established by card payment scheme operators require the manufacturer to introduce a security watch process covering all product components, and that this process is assessed during certification. Each new product version must also be covered by specific certification. In practice, these rules therefore make it possible to regularly measure the overall level of security and the ability to withstand attacks.

The Observatory further notes that card payment scheme operators can instruct terminal manufacturers to conduct specific checks on approved models and to take the necessary steps if negative results are detected.

1|3|2 Operation and maintenance of terminals

The Observatory noted that its recommendation concerning implementation by card payment schemes and acquirers of rigorous traceability for acceptance hardware deployed at POS has not been adequately acted on. While acquirers are able to ensure good traceability of the payment terminals that they own, for example in a situation where a terminal is rented out to a merchant, it is harder in practice for them to ensure traceability quality if the terminal is owned by the merchant or a service provider used by the merchant.

At end-2012, an attack was launched against a specific cluster-type terminal model used in integrated electronic payment systems. The attack consisted in substituting a terminal located at a POS by another terminal that had been altered and fitted with a skimming device. This was used to record magnetic stripe data and PINs, which were then transmitted remotely by Bluetooth. Identifying the POS using the terminal model targeted by the attack took more than six months, mainly owing to the lack of technical traceability of acceptance points. The "CB" Bank Card Consortium is working to update electronic payment protocols to make it possible to collect all the information needed to identify outstanding terminals, including those that are connected to concentrators.

The experience gained from this attack demonstrated the effectiveness of systems that pair terminals with the rest of the electronic payment system (especially cash registers). Pairing, which may merely entail recognition by the cash register of the terminal's serial number, is helpful in that it limits the scope for substituting or inserting terminals that have been tampered with. Pairing could extend to full-blown mutual authentication between system elements, in which case certificates would be required.

The attack also underlined the value of raising awareness among merchants and their personnel about the need to keep a constant watch over acceptance hardware.

In terms of its recommendations on regularly updating terminal operating systems and implementing security patches securely and remotely, the Observatory noted that manufacturers of concentrators generally provide solutions that enable clustered terminals to be updated from the concentrators to which they are connected.

Such solutions are not yet available for stand-alone terminals, and local access to the terminal is still required to introduce security patches.

While acquirers are capable of remotely updating EPTs that they own, for example if the terminal is rented to a merchant, updates mainly appear to be for the terminal's operating settings and less often for the operating system.

1|4 The Observatory's recommendations

Given the uptrend in attacks on payment terminals, the Observatory calls on all parties to exercise increased vigilance.

In particular, it recommends that processes used by card payment schemes to approve acceptance devices be strengthened to more effectively manage terminals that are either defective or reaching the end of their life.

The Observatory stresses that efforts to improve hardware traceability, which are expected to lead to changes in electronic payment protocols, must continue and be completed as soon as possible, since they will enable more rigorous management of terminals in use, whether they are owned by the acquirer, the merchant or a technical service provider used by the merchant.

Accordingly, the Observatory urges card payment scheme operators to work with other participants and especially merchants to study the design and implementation of technical solutions that allow acquirers and issuers to refuse payments made using unapproved terminals or terminals whose approval has expired or been withdrawn.

Furthermore, the Observatory reiterates its recommendation on regularly updating terminal operating systems and calls on affected parties to roll out solutions that may be used to update EPTs (software and settings) securely and remotely.

2| Stocktaking of strong cardholder authentication techniques

Over the last few years, the Observatory has noted a substantial difference[4] in its statistics between fraud rates for face-to-face payments and those for CNP sales. For this reason, it has issued a number of recommendations aimed at strengthening cardholder authentication to protect CNP payments, particularly online payments.

Steady growth in CNP fraud prompted the Observatory to issue its first recommendations back in 2008 to strengthen cardholder authentication mechanisms, which until that time had been primarily based on entering a card number and card verification number. Card payment schemes and issuers, which were responsible for providing these solutions to holders, were left free to choose which technical procedures to use for strong (or one-time) authentication.

By early 2014, the goal of ensuring that all cardholders were provided with one-time authentication solutions had been virtually achieved, with approximately 93.7% of cardholders provided with such solutions.[5]

In January 2013, the ECB published a set of recommendations and good practices for the security of internet payments, based on the work of the SecuRe Pay forum. These recommendations, and especially those aimed at protecting enrolment and providing cardholders with strong authentication solutions for CNP payments, support those of the Observatory. All affected participants in Europe are asked to implement these recommendations by 1 February 2015.

The following study takes stock of the strong authentication techniques implemented by French card payment schemes and issuers.

2|1 Characteristics of strong cardholder authentication

The purpose of authentication is to verify the identity given by an entity. Authentication is generally preceded by identification, which enables the entity to be recognised by the system by means of an element provided in advance, such as an identifier.[6] While it is straightforward to define static authentication as entailing the use of a password, strong authentication draws on concepts that require clarification. In its report on the security of internet payments, the ECB defines strong authentication[7] as *"a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:*

- *something only the user knows, e.g. static password, code, personal identification number;*
- *something only the user possesses, e.g. token, smart card, mobile phone;*
- *and something the user is, e.g. biometric characteristic, such as a fingerprint.*

4 Cf. Chapter 2 of this report.
5 3D-Secure statistics, November 2013 to end-April 2014.
6 French ANSSI definition (*http://www.securite-informatique.gouv.fr/gp_rubrique33.html*).
7 Strong customer authentication.

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence)."

Face-to-face use of a smartcard combined with entry of a PIN to validate payment satisfies the definition of strong authentication. The following chapters describe the main strong authentication solutions used in CNP payments, looking first at internet payments generally, followed by payments carried out using a mobile phone, and finally payments made by mail or when placing an order over the phone with an operator.

2|2 Strong cardholder authentication in conventional internet payments

Strong cardholder authentication is an essential link in the wider system for preventing card payment fraud, making it possible to more effectively combat attempted fraudulent payments. This chapter takes stock of the main techniques for strong authentication used in connection with conventional computer-based internet payments. Since issuers are free to choose authentication solutions, they have adopted various approaches for different customer segments.

2|2|1 OTP text message

The most widely used strong authentication solution among issuers on the French market is to send a text message containing a one-time password (OTP) to the cardholder's mobile phone, notably via the 3D-Secure system. While issuers have completed the process of deploying these systems, actually using them may take longer because of the need to verify the mobile phone numbers recorded in their databases.

Although this approach satisfies the need for strong cardholder authentication, it does present security weaknesses: the communication channel used to send text messages is not protected,[8] malware installed on the phone could compromise security, and there is the possibility that under certain circumstances the lawful cardholder's SIM card could be deactivated and a different SIM card associated with the same number activated to carry out fraudulent transactions.

Measures are in place to address these issues. First, authentication by OTP text message takes place within a broader fraud prevention system. In particular, the risk management and transaction scoring tools introduced by card payment schemes, issuers and merchants, and the checks carried out by issuers when they receive authorisation requests, supplement strong cardholder authentication and help to spot fraudulent transactions. Second, the technical environment of mobile phones is evolving all the time with the addition of security-enhancing functionalities, which notably protect mobile operating systems by preventing the use of unauthorised malware. Advances in this field must continue. Third, mobile phone operators have bolstered existing procedures to prevent the unlawful deactivation of SIM cards, but efforts need to be stepped up to make these measures more effective.

In view of this situation, it is important for the Observatory to continue to monitor the security of this strong cardholder authentication technique, whose effectiveness has not to date been questioned.

Paradoxically, the OTP text message approach is ill-suited to payments made by mobile phone, because it removes the protection provided through the use of two separate communication channels, but also because receiving a text message does not work well with the mobile payment process, whether conducted using a browser or a mobile application.[9]

8 Non-encryption of data sent by text message allows unencrypted data to be intercepted.
9 However text messages are extremely useful when it comes to notifying holders in real time of unusual transactions (abroad, high-value, etc.) and enabling them to report cards lost or stolen in the event of fraudulent transactions.

2|2|2 Dynamic virtual card

A dynamic virtual card (DVC) allows the holder to avoid entering the actual card number when making an online payment. To achieve this, a special environment, which can generally be accessed through the holder's online bank, allows the customer to generate a set of specific numbers[10] that are valid for a single transaction and that the holder may enter instead of the data on the actual card. Since access to the dynamic passwords is not provided through a separate communication channel, access to the OTP-generating environment must itself be protected by strong authentication. Accordingly, a DVC is considered to be a strong authentication solution only if access to it is properly protected by strong authentication.

2|2|3 Physical card reader used to generate an OTP

A cardholder can use a stand-alone mini-payment card reader to generate an OTP by inserting the card in the reader and authenticating him or herself by entering a PIN. This approach has the advantage of offering a level of security[11] on par with that of face-to-face payments, with the result that it is one of the most widespread strong authentication solutions deployed by the main card issuers after the text messaging approach. Because of the cost of the terminal and constraints linked to the deployment of hardware, this type of solution is preferred for certain types of cardholders (professionals, cardholders not wishing to use text messages, etc.).

A second type of card reader, this time connected[12] to the holder's personal computer, is also used in some countries. It may be used to approve a payment via a dedicated application installed on the computer. This type of solution was the subject of a widespread but unsuccessful campaign in France.

2|2|4 Display cards

Technical advances in miniaturising certain components have enabled manufacturers to include a display and a keypad on cards to permit interaction with the holder. As with the preceding solution, when a payment has to be authenticated, the holder will be asked to enter a PIN on the card, which will allow him or her to obtain an OTP to be entered on the payment approval screen. This solution, which is already offered by some foreign banks, is currently being piloted in France. It has the advantage of removing the holder's need for additional hardware and enjoys a level of security equivalent to that of an OTP-generating card reader (or token, see below).

10 Card Primary Account Number (PAN), expiry date and verification number.
11 Because of the certification required for card readers.
12 Generally using a USB-type connection.

2|2|5 Token

A token is a device the size of a USB key. It may be used to generate an OTP that is typically synchronised with a remote authentication server and that changes after a certain period of time (for example 60 seconds). The OTP is then entered on the authentication screen during the card payment process. "Mini-calculator" solutions also exist and can be used to add a keypad that enables an additional interaction, whereby a PIN known solely to the holder must be entered to obtain a valid OTP. Alternatively, and depending on the device, during the authentication stage, a remote server may also provide a random number that must be entered to obtain an OTP. Like a physical card reader, these devices are deployed as supplementary solutions by the main issuers, in some cases targeting certain cardholder categories.

2|3 Strong cardholder authentication in mobile payments

The rise of the wireless[13] and mobile[14] internet has promoted the use of new terminals that are suited to mobile environments, such as tablets and smartphones.

Strong authentication solutions used for conventional internet payments are either inappropriate for or ill-suited to this type of situation. Also, the use of an OTP text message may create a security weakness for mobile payments. While the authentication phase in the case of a payment made with a personal computer connected to the internet, uses a second channel, namely that of the mobile phone network, which enhances the overall security, this ceases to be the case if the payment and the authentication both take place on the same device.

New solutions are emerging to address the specific needs of the mobile channel. For example, there has been a sharp increase in digital wallets,[15] which provide greater ease-of-use when using the mobile channel, as sensitive payment data are saved only once, at enrolment, avoiding the need for the holder to enter payment card details on an unsecure terminal.

The security level of these solutions has been the subject of recommendations by the Observatory[16] and more recently by SecuRe Pay.[17] These recommendations cover the use by digital wallet providers of strong cardholder authentication by the payment card issuer when the card's data are enrolled in the digital wallet system. The operator must also carry out a risk analysis leading to the activation of strong authentication for payments that are considered to be at-risk. Digital wallets meeting at least these two recommendations are capable of providing effective protection for payments made using mobile devices.

Other innovative solutions, which are currently being piloted, are being developed to protect payments made using mobile phones. For example, one of these solutions consists in saving personal and payment data in a digital wallet, then initiating payments by using a smartphone to read a QR code[18] displayed on the merchant's standard EPT. The user can see and approve the amount of the payment on his or her smartphone and enters an OTP on the merchant's EPT. This solution, which is based on two identification factors and two separate channels, meets the criteria for strong authentication.

There are also initiatives that seek to build biometric authentication solutions into the latest generation

13 Public or private Wi-Fi.
14 GPRS, 3G, 4G, etc.
15 These solutions were covered by a study in the Observatory's 2011 Annual Report.
16 Cf. 2011 Report, Chapter 3, 2|: "Digital wallets and card payment".
17 *https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf*
18 Quick response code: two dimensional barcode used to store information particularly with a view to initiating payment transactions.

of smartphones. These solutions are based in particular on reading digital fingerprints.[19] Wider introduction of this functionality could play a role going forward in protecting mobile payments, provided the selected authentication solutions are extremely robust from a security perspective and could not be easily circumvented by exploiting security weaknesses in the biometric solutions or their associated peripheral components. The introduction of security evaluation and certification processes for these elements could help to achieve this outcome.

Finally, some mobile phones have specific embedded secure elements that make it possible to keep payment functionalities separate from other mobile applications. These solutions, although not widespread because of their implementation cost, are functional and used in sectors requiring a high level of security for mobile phone-based exchanges.

2|4 Strong authentication in the MO/TO channel

With the rapid rise of online commerce, mail order/telephone order (MO/TO) card payments have decreased markedly. However, these two channels continue to be used in a number of situations (shopping coupons, subscriptions, etc.) and may thus provide a target for fraudsters, creating the risk that some fraud could shift from internet payments, which are now better protected, to these more traditional sales channels.

The MO channel is ill-suited to card payments, which are hard to protect. In the case of TO payments, cardholder authentication through the generation of an OTP is possible and would back up the transaction scoring tools widely used by merchants for online CNP sales.[20] Similarly, established mechanisms for protecting sensitive card payment data are being introduced at merchant level to provide protection against the risk of theft.

The development of digital wallets could also help to secure TO card payments. Since sensitive payment data are already saved in the digital wallet, the payer would merely have to provide his or her identifier (usually a phone number), then approve the payment request in a mobile application or via push text message.[21] This way, the merchant would no longer be circulating sensitive payment data.

3| Conclusion

The fraud rate in the CNP sales sector is around 20 times higher than the rate for face-to-face payments. Accordingly, fraud prevention efforts must be pursued, in particular by strengthening cardholder authentication in line with recommendations made by the Observatory since 2008. With issuers free to choose which solutions to introduce, the Observatory has noted that the market offers a diverse array of solutions, both in terms of functionalities and robustness to security attacks.

Of these different approaches, sending an OTP by text message to a mobile phone or smartphone is currently the most widespread solution in France. While the effectiveness of this solution from a security perspective is not being called in question, the Observatory considers that progress in securing smartphones as a means of conducting one-time authentication must be pursued to guard against malware attacks. Work also needs to be done to strengthen the procedures aimed at preventing

19 Also worth mentioning are solutions currently being examined using voice-based holder authentication for digital wallets.
20 Cf. OSCP 2009 Annual Report, Chapter 3|2 on the security of payments by mail and telephone.
21 Push text message: the user approves payment by responding to an incoming text message rather than by entering an OTP.

fraudsters from deactivating the SIM card of a lawful holder and activating a different SIM associated with the same number to carry out fraudulent transactions. Accordingly, the Observatory will continue to monitor the security of this strong cardholder authentication solution.

Several other solutions exist and strengthen cardholder authentication during online card payments. Dynamic virtual cards can perform this function, for example, provided that access to the device used to generate OTPs for online use is protected by strong authentication. The Observatory also noted the roll-out of solutions based on physical card readers that generate OTPs once a payment card is inserted, display cards with mini-screens that show OTPs, and stand-along authentication tokens that perform a similar function.

The soaring increase in online payments made using internet-connected smartphones raises the question of the solutions that are best suited to this approach. While text message-based approaches are not very user-friendly, the Observatory has noted that the development of digital wallets offers a potential answer to the problem. The security level of these solutions was the subject of recommendations by the Observatory in its 2011 Annual Report and more recently by SecuRe Pay in 2012. These recommendations cover strong cardholder authentication by the payment card issuer when the card's data are enrolled in the digital wallet system and activation of strong authentication for payments that are considered to be at-risk. Digital wallets meeting at least these two recommendations are capable of providing effective protection for payments made over mobile devices.

Finally, the Observatory notes that recent technological developments aimed at building biometric solutions into smartphones could enhance the protection of mobile payment transactions. However, authentication solutions implemented on smartphones must be extremely robust. Accordingly, the introduction of evaluation and certification processes for biometric components may help to promote the large-scale deployment of these solutions for use in payments.

Protection of personal data in fraud prevention systems

While strong cardholder authentication can be ensured in face-to-face card payments through use of an EMV-compliant smartcard, the same is not true for card-not-present (CNP) payments, which may be initiated with a small amount of information (card number, expiry date and card verification number).[1] This leaves them especially vulnerable to fraud.

The rapid increase in CNP payments has thus created new fraud prevention needs, spurring the development of tools aimed at identifying fraudulent behaviour and allowing merchants to conduct strong cardholder authentication through their payment service provider, using solutions such as 3D-Secure, wherever possible and appropriate.

In this environment, personal data have become a critical issue for fraud prevention players, which use them to assess the risk level of a CNP payment, to conduct additional checks where necessary (strong cardholder authentication, for example) or, if they have the authorisation, to reject a transaction if it is considered too risky.

The use of processing operations that employ these data, even to prevent fraud, is governed by the French Data Protection Act, the proper application of which is supervised by the National Data Protection Agency (*Commission nationale de l'informatique et des libertés* – CNIL).

Against the backdrop of rapid developments in CNP fraud prevention technologies, the Observatory decided to examine the challenges posed by the rules applicable to the processing of personal data in the context of fraud prevention.

After recalling the definition and scope of the data in question, this study reviews practices in anti-fraud data processing, current regulatory provisions governing these methods and the changes to come. It should be noted that although the study explores this data privacy issue in relation to card payments, the underlying implications of anti-fraud data processing are broader and encompass all payment means.

1| Protecting personal data: an aspect that fraud prevention systems must take into account

Fraud prevention systems are principally designed to ensure that a payment transaction is duly initiated and approved by the lawful cardholder.

In France, and in Europe more generally, using an EMV-compliant smartcard make it possible to ensure strong cardholder authentication in a face-to-face setting, resulting in a very low level of fraud through this channel (0.013% in 2013).

Since there is no similar mechanism for CNP payments, gathering and using personal data, i.e. data that may be used to identify a natural person,[2] has become a critical issue for fraud prevention players.

Technological advances have enabled these firms to expand the scope and nature of personal data gathered during online transactions in order to verify the consistency of these data and increase the level of certainty about the person initiating the payment transaction.

1 Also known as the CVX2.

2 France's lawmakers have defined the concept of personal data as being *"any information relating to a natural person who is identified or who could be identified directly or indirectly by reference to an identifier or to one or more elements specific to the person. To determine whether a person is identifiable, it is necessary to consider all the identification resources available or potentially available to the person in charge of data processing or any other person"*.

1|1 Fraud prevention players

A card payment involves numerous participants, each of which plays a role in fraud prevention systems according to the nature of the information that they possess and their position in the payment chain.

The main players are the following:

• the payment card issuer naturally has the broadest range of data on the holder's card use. The issuer is also responsible for the security arrangements relating to the payment instrument provided to the holder, in particular as regards strong authentication for internet card payments. However, the issuer has limited information about the nature of the holder's purchase from the merchant;

• the payment order acquirer is responsible for processing card payment transactions on behalf of the acceptor (merchant). It naturally has little information about the holder but may create fraud prevention tools based on all the transactions that it processes as an acquirer (for example, if a card was already the subject of fraud with another merchant for which the acquirer has responsibility, the acquirer can prevent that card from being used with another merchant);[3]

• the acceptor, i.e. the merchant, chiefly has information about the purchase (nature of the good, for example, delivery method, etc.) and may also have information about the customer if he or she is already known to the merchant;

• card payment schemes have the broadest view of payment transactions made by cardholders and/or with merchants affiliated with the payment system. As such, they execute anti-fraud data processing operations for members (issuers and/or acquirers);

• specialised technical service providers, which may be entrusted with anti-fraud data processing operations by any of the participants mentioned above, provide players wishing to outsource this function with expertise and the ability to pool data processing.

Other players that are indirectly linked to the payment chain also contribute to fraud prevention systems.

The judicial and law enforcement authorities are in charge of investigations and legal action in the event of proven fraud and where applicable may need to access and retain the data gathered by the above-mentioned participants by filing judicial requisitions.

Logistics firms, particularly goods transporters, may also have relevant information on central distribution points and the physical address for delivery of a good purchased online, which online merchants may use to improve the quality of information gathered during anti-fraud data processing operations.

Last but not least, the cardholder plays a key role in security by keeping his or her personal identification number (PIN) safe and protecting card data. The holder may also play a significant role in detecting fraudulent transactions, especially if the issuer has set up warning systems (e.g. text alerts) for executed transactions. If these warning systems operate more or less in real time, they allow the issuer to respond quickly in the event of fraud and block further fraud attempts using a compromised card. The Observatory reiterates in this respect that cardholders are obliged to report promptly any unauthorised transaction to the card issuer and to take steps to report the card lost or stolen.

1|2 Technological advances have made it possible for firms to expand the scope and nature of personal data gathered and enhance anti-fraud data processing operations

In order to ensure that the lawful cardholder is carrying out a transaction with his or her card, fraud prevention systems have tended, in the absence of a widespread strong authentication solution, to expand the scope and nature of data – including personal data – gathered during an online card payment to check the consistency of these data and thus increase

3 Participants are responsible for ensuring that the lawful cardholder is correctly informed beforehand in the event that a payment transaction is blocked.

the level of certainty about the person initiating the payment transaction. This development has been facilitated by technological advances.

Alongside the data customarily gathered on the identity and contact details of the person initiating the transaction (full name, postal address, delivery address, email, phone number and so on), fraud prevention tools have gradually added:

- cardholder consumption habits (number and details of orders, length of relationship, frequency and amount of purchases, consumption habits, payment instruments used, etc.);

- location (e.g. through the IP address of the computer used);

- tools used to access the internet (for example by taking a device fingerprint of the terminal used to access the internet, which consists in identifying the terminal's technical specifications and hardware and software components);

- behaviour-related data (analysis of time taken to fill out forms, keypad entry method, etc.).

With the wider scope of processed data, it has become possible to introduce more subtle and targeted processing operations to reconcile information and build sophisticated algorithms to prepare predictive analyses of fraudulent behaviour through transaction scoring tools. The increased number of criteria used in scoring transactions is intended to improve reliability in terms of generating appropriate risk assessments.

Setting aside their effectiveness, these processing operations raise data privacy issues. Participants in the card payment chain have shifted from a disclosure-oriented approach, where customers provide their own data (identity, contact information, etc.), to an approach based on automatic collection of data linked to the customer's IT environment, without always informing customers of this new practice. The technologies that firms use allow them to track customers' activities and habits, which may lead to suspected unlawful behaviour being recorded in blacklists or grey lists.

2| Anti-fraud data processing operations based on the use of personal data are covered by specific regulations that are set to change

2|1 Authorisation arrangements provide numerous data protection guarantees

Under Article 25-I-4° of the Act of 6 January 1978, files containing information destined to prevent fraud or register fraudsters must receive prior authorisation if they deprive registered persons of a right or the benefits of a contract.[4] The same applies to data processing operations that result in fraud charges being laid against the person in question and that could lead to a complete or partial block being placed on a payment card.

To obtain this authorisation in the cases covered by the law, the entity responsible for the file and/or anti-fraud data processing operations must submit an application that should, in particular, make certain guarantees relating to:

1. Purpose of processing: the purpose must be specified and legitimate,[5] ensuring that data are used for the reason or reasons reported by the person responsible for data processing.

2. Nature of data gathered: the person responsible for data processing must provide an exhaustive list of the personal data used in fraud prevention systems that issue warnings on at-risk transactions. The data used should be adequate, appropriate and non-excessive. As regards data linked to payment cards specifically, the CNIL updated its recommendations[6] in 2013 on the requirements for collection, retention and reuse.

4 For example by rejecting an order placed during an online purchase.
5 For example "detection and prevention of bank card fraud".
6 Deliberation 2013-358 of 14 November 2013.

3. Nature of processing operations: every type of data processing operation must be precisely described. Thus, scoring tools should be created using reliable, statistically-based models and must not infringe on data privacy. To ensure proportionality, the various levels of analysis conducted by different fraud prevention participants should complement each other. Furthermore, when customers are asked to provide additional supporting documentation, the person responsible for data processing must make sure that this request is proportionate to the purpose of processing. For example, CNIL recommends keeping a copy of the front of identity cards only and prohibits collecting photocopies of payment cards or bank statements in situations where additional supporting documents are requested.

4. Right to be informed about, consult and remove data: those responsible for processing data must inform affected persons about the data processing operations and their related rights under the provisions of Article 32-II of the Act of 6 January 1978 (amended) as well as about the procedures for exercising these rights by saying which organisations affected persons may contact to exercise these rights (for example if an outside service provider is used).

5. Data retention period: the length of time for which data are retained should be adjusted to reflect the type of processing operation and the purpose of the processing.

6. Physical and logical security of data: this is a major obligation for the person in charge of data processing, who must ensure that the confidentiality and integrity of collected data are preserved. For this, all data must be covered by an appropriate security policy, covering the use of mechanisms to ensure the physical and logical protection of servers and applications housing the collected data, as well as the creation of an audit trail that may be employed to detect and analyse any access to or modification or removal of data in the database of the person in charge of processing.

7. Request for consent: in some cases, it is necessary to apply the provisions of Article 32-II of the Act of 6 January 1978 (amended), which requires the affected person to give their explicit consent in accordance with the procedures set out in Deliberation/Recommendation 2013-378 of 5 December 2013. This applies particularly to the storage of information on the user's equipment or access to previously-stored informations.[7]

Despite the use of fraud prevention tools by participants in the card payment chain, and particularly online merchants, the majority of entities have not submitted prior applications for authorisation as required by the CNIL. For this reason, the CNIL has undertaken work to streamline the disclosure requirements for data processing operations aimed specifically at fraud prevention. This will provide the opportunity to address a number of points highlighted by fraud prevention participants.

2|2 Streamlining disclosure requirements will provide an opportunity to take account of the latest developments in anti-fraud data processing operations

Discussions within the Observatory in connection with this study led to the identification of several obstacles to the protection of personal data in connection with fraud prevention:

- insofar as many acceptors actually use outside service providers to carry out anti-fraud data processing, the question of their responsibility with respect to outsourced processing should be clarified;

- some participants would like to see the pooling of collected data facilitated, particularly the blacklists used to identify proven fraudsters, in order to combat fraud more effectively.

Data pooling could be beneficial to merchants in some sectors, as has already been proven in the field of mobile telephony (Préventel initiative).

Law enforcement agencies are also planning to pool data under an online complaint filing procedure

7 Cookies, which are files stored in internet browsers and which hold information on the use of a website by an internet user, are concerned by this provision, as are any similar mechanisms.

to facilitate the investigation of internet card payment fraud;

• the use of identification data obtained from new methods of accessing the internet (computers but also smartphones, tablets, and so on) by those responsible for anti-fraud data processing remains strictly regulated and restricted. Insofar as the affected person gives their consent, the CNIL did however recently authorise certain entities to carry out processing operations based on such data as part of fraud prevention arrangements;

• although the rules governing the length of time for which personal data may be retained for fraud prevention purposes are clear, some entities have pointed out that the durations may vary sharply depending on the situation, which may be a source of confusion (cf. Box);

• finally, in a setting where controlling the fraud rate has become a major financial and competitive issue for e-merchants, it is appropriate to harmonise the rules for protecting personal data in the context of anti-fraud data processing at the European level. Note in this regard that Europe's data protection authorities have met within an Article 29 Data Protection Working Party (WP29) to work towards uniform application of EU data protection rules. Thus far, however, many provisions continue to be applied differently depending on the country where the data are processed.

To address these issues, the CNIL has undertaken work aimed at adopting a "single" authorisation for payment instrument fraud prevention. This single authorisation will offer a more effective framework for gathering and processing data to ensure that fraud prevention, which is a legitimate goal of professionals, is proportionate to privacy rights. In this regard, the use of strong cardholder authentication solutions such as 3D-Secure when carrying out the payment may help to limit the need for excessive collection of personal data.

A single authorisation could facilitate the performance of advance formalities by those responsible for data processing. It should also be accompanied by clarification on the responsibilities of the parties that process data, particularly if they use an outside service provider to carry out these tasks as part of a fraud prevention system.

Box

CNIL rules on the retention period for personal data used in fraud prevention

A distinction is drawn between the retention period for data analysed and generated as part of issuing alerts and the retention period for data contained in blacklists (instant negative score) or grey lists (not necessarily generating an instant negative score but indicating that additional information is required to successfully complete a transaction).

Alerts issued in the context of fraud prevention are not themselves intended to be kept but may give rise to checks involving the affected persons to confirm or deny fraud. In this case, the retention period is necessarily short and linked to the checks. In some cases, those in charge of data processing would like to keep the data generated by alerts to refine and enhance their scoring models. This is possible if the data are anonymous.

Data included in blacklists and grey lists are linked to confirmed cases of fraud and attempted fraud (excluding payment delinquencies resulting from insufficient funds), notably following an investigation. In this case, the CNIL recommends a retention period not exceeding three years, which corresponds to the limitation period for the offences.

Where court proceedings are initiated, transaction-related data are kept until the end of the proceedings.

Data subject to archival measures are retained in a separate, restricted-access information system for a duration not exceeding the time period for dispute proceedings.

3| Conclusion

In the absence of an equivalent to the EMV standard to protect CNP payments, gathering and using data – in some cases personal data – has become a critical issue for fraud prevention players.

Technological advances have enabled firms to expand the scope and nature of personal data gathered during online transactions in order to verify the consistency of these data and increase the level of certainty that the person initiating the payment transaction is the lawful cardholder.

Fraud prevention participants have shifted from a disclosure-oriented approach, where customers provide their own data (identity, contact information, etc.), to an approach based on automatic collection of data linked to the customer's IT environment, without always informing customers of this new practice.

While anti-fraud data processing operations using personal data address the legitimate goal of preventing unauthorised transactions and round out existing security mechanisms, they remain governed by France's Data Protection Act, whose proper application is supervised by the CNIL.

The CNIL has begun work aimed at streamlining the disclosure requirements for anti-fraud data processing.

This exercise will provide an opportunity to address a number of points highlighted by fraud prevention participants, including the need to clarify the responsibilities of parties using outside service providers, the question of pooling fraud data to improve effectiveness, the possibility where appropriate of using new identification data obtained using new technologies as well as the need to clarify the rules concerning the retention period for personal data used for fraud prevention purposes.

Streamlined authorisation requirements would make it possible, in cases provided for under Article 25 of the Data Protection Act, to regulate data collection and processing to ensure that fraud prevention, which is a legitimate goal of professionals, is proportionate to privacy rights. In this regard, the use of strong cardholder authentication solutions such as 3D-Secure when carrying out the payment may help to limit the need for excessive collection of personal data.

Finally, in a setting where controlling the fraud rate has become a major financial and competitive issue for e-merchants, the protection of personal data needs to be addressed at European level. Accordingly, the European Commission has proposed a draft data protection regulation that would be directly applicable to all EU member countries, with a view to ensuring that Europe introduces uniform rules that are consistent with the Payment Services Directives. The future European regulation is expected to be adopted in the course of 2015 and should make it possible to harmonise the obligations placed on entities that carry out anti-fraud data processing operations based on the use of personal data.

Appendixes

Security tips for cardholders

Your habits make a direct contribution to the security of your card. Please follow these basic security recommendations to protect your transactions.

Be responsible

- Your card is strictly personal: do not lend it to anyone, no matter how close they are to you.
- Check regularly to see that you still have your card.
- If your card comes with a PIN, keep the code secret. Do not give it to anyone. Memorise it. Avoid writing it down and never keep it with your card.
- Make sure that nobody can see you enter your PIN. In particular, shield the keypad with your other hand.
- Read your statements carefully and regularly.

Be aware

When paying a merchant

- 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 withdrawing cash from ATMs

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

When making internet payments

- Protect your card number: do not store it on your computer, never write it in an ordinary e-mail message and verify the security features of the merchant's website (padlock in the lower corner of window, URL starting with "https", etc.).
- Make sure you are dealing with a reputable company. Make sure that you are on the right site and read the general terms of sale carefully.
- Protect your computer by running the security updates offered by software editors (usually free) and by installing antivirus software and a firewall.

When travelling to other countries

- Find out what precautions you need to take and contact the card issuer before leaving to find out about card protection systems that may be implemented.
- Remember to take the international telephone numbers for reporting lost or stolen cards.

A2

Know what to do

If your card is lost or stolen

- Report it immediately by calling the number provided by the card issuer. Make sure to report all of your lost and stolen cards.
- If your card is stolen, you must also file a complaint with the police as soon as possible.

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

If you see any unusual transactions on your statement, and your card is still in your possession

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

Except 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), you must submit a claim to the institution that issued the card as soon as possible and within a time limit set by law, namely 13 months from the debit date of the contested transaction. You will not be liable. The disputed amounts must be immediately refunded at no charge. Note that if the card was misappropriated in a non-European country, the time limit for submitting a claim is 70 days from the debit date of the contested transaction. Your card issuer may extend this limit, but it cannot be more than 120 days.

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

Protection for cardholders in the event of unauthorised payments

The Order that transposed the Directive on Payment Services in the Internal Market, which came into force on 1 November 2009, amended the rules concerning the liability of holders of payment cards.

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

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

Domestic and intra-Community transactions

These include payment transactions made in euros or CFP francs within the territory of the French Republic.[1] They also include transactions carried out with a payment card whose issuer is located in metropolitan France, in the overseas departments, Saint Martin or Saint Barthelemy, on behalf of a beneficiary whose payment service provider is located in another State party to the EEA agreement (EU + Lichtenstein, Norway and Iceland), in euros or in the domestic currency of one of those States.

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

A derogation from these refund rules is allowed for payment transactions carried out using personalised security features, such as the entry of a secret code.

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

A4

Before submitting notification to block the card

Before reporting the card lost or stolen,[2] the payer could be liable for losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment card, if the transaction is carried out using the card's personalised security features. By contrast, the cardholder will not be liable if the personalised security features are not used to conduct the transaction.

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

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

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

After submitting notification to block the card

The payer shall not bear any financial consequences resulting from the use of a card or misappropriation of card data after reporting the loss, theft or misappropriation.

Once again, if the holder acts fraudulently, he or she forfeits all protection and becomes liable for losses associated with use of the card.

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

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

2 The law now uses the term "notification to block the payment instrument".

Transactions outside Europe

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

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

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

The maximum time limit for disputing transactions has been changed to 70 days and may be extended by agreement to 120 days. However, the arrangements concerning immediate refunds for unauthorised transactions have been extended.

3 Including Mayotte since 31 March 2011.
4 That is not part of the EEA agreement (EU + Lichtenstein, Norway and Iceland).

Missions and organisational structure of the Observatory

Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the *Monetary and Financial Code* lay down the missions, composition and operating procedures of the Observatory for Payment Card Security.

Scope

In its wording prior to 1 November 2009,[1] Article L. 132-1 of the *Monetary and Financial Code* defined a payment card as any card issued by a credit institution that enables its holder to withdraw or transfer funds. Because Order 2009-866 of 15 July 2009 on the conditions governing the supply of payment services and creating payment institutions maintained the scope of the Observatory's responsibilities, it was decided to keep the old definition and extend it to payment service providers, which are, under section I of Article L. 521-1 of the *Monetary and Financial Code*, credit institutions, electronic money institutions and payment institutions.

Consequently, the Observatory's remit covers cards issued by payment service providers or other assimilated entities[2] that serve to withdraw or transfer funds. It does not cover the single-purpose cards that may be issued by an undertaking without approval from the French Prudential Supervisory and Resolution Authority (*Autorité de contrôle prudentiel et de résolution* – ACPR). These include cards issued by a single undertaking and accepted as a means of payment for goods or services by the undertaking itself or by merchants that have signed a commercial franchise agreement with it,[3] as well as multi-provider cards, which are accepted, for the acquisition of goods or services, only at the premises of the card issuer or within a limited network of persons or for a limited range of goods and services under a commercial agreement with the issuer.[4]

Several types of payment cards on the French market come within the Observatory's remit. A distinction is generally made between cards whose payment and withdrawal procedures rely on:

- a limited number of issuing and acquiring payment service providers (generally referred to as "three-party" cards);
- a large number of issuing and acquiring payment service providers (generally referred to as "four-party" cards);

These cards offer various functions and may be classified according to the following functional typology:

- debit cards are cards that draw on a payment account[5] and enable their holders to make withdrawals or payments that are debited in accordance with a timeframe set out in the card issuance contract. The debit may be immediate (for withdrawals or payments) or deferred (for payments);

1 The article was deleted by the transposition order for the Payment Services Directive because it was not compatible with the directive, which sets the rules applicable to payment transactions as a function of the payment process to ensure technological neutrality with respect to different payment instruments.

2 Under the terms of section II of Article L. 521-1 of the *Monetary and Financial Code*, assimilated entities include the Banque de France, the French overseas departments note-issuing bank (Institut d'émission des départements d'outre-mer), the Treasury and the Caisse des dépôts et consignations.

3 These cards are exempt from the need for an approval, under point 5° of section I of Article L. 511-7, Article L. 525-6 and section II of Article L. 521-3 of the *Monetary and Financial Code*.

4 These cards are exempt from the need for an approval, under section II of Article L. 511-7, Article L. 525-5 and section I of Article L. 521-3 of the *Monetary and Financial Code*.

5 Under the terms of section I of Article L. 314-1 of the *Monetary and Financial Code*, payment accounts are accounts held in the name of one or more persons and used for the purpose of executing payment transactions. They are sight deposit accounts held on the books of banks and accounts opened on the books of other payment service providers.

• 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 holders to pay the issuer at the end of a determined period (over 40 days in France). The merchant is paid directly by the issuer without delay;

• national cards serve to make payments or withdrawals exclusively with merchants established in France;

• international cards serve to make payments and withdrawals at all national or international acquiring points belonging to the brand or to partner issuers with which the card payment scheme has signed agreements;

• electronic purses are cards that store electronic money units. Under Article L.315-1 of the *Monetary and Financial Code, "electronic money means a monetary value that is stored in electronic form, including magnetic form, representing a claim on the issuer, which is issued against the receipt of funds for the purposes of carrying out the payment transactions defined in Article L. 311-3 and which is accepted by a natural person or legal entity other than the electronic money issuer"*.

The above typology includes contactless payments.

Responsibilities

Pursuant to Articles L. 141-4 and R. 141-1 of the *Monetary and Financial Code*, the Observatory has a threefold responsibility:

• it monitors the implementation of measures adopted by issuers and merchants to strengthen payment card security. It keeps abreast of the principles adopted with regard to security as well as the main developments in this area;

• it compiles statistics on fraud on the basis of the relevant information disclosed by payment card issuers to the Observatory's secretariat. The Observatory issues recommendations aimed at harmonising procedures for establishing fraud statistics for the various types of payment cards;

• it maintains a technology watch in the payment card field, with the aim of proposing ways of combating technological attacks on the security of payment cards. To this end, it collects all the available information that is liable to reinforce payment card security 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 *Monetary and Financial Code*, the Minister of the Economy and Finance may request the Observatory's opinion on various issues, setting a time limit for its response. These opinions may be published by the Minister.

Composition

The composition of the Observatory is set out in Article R. 142-22 of the *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/her representative;
- the Secretary General of the *Autorité de contrôle prudentiel et de résolution* or his/her representative;
- ten representatives of payment card issuers, particularly bank cards, three-party cards and electronic purses;
- five representatives of the Consumer Board of the National Consumers' Council;
- five representatives of merchants, notably from the retail sector, the supermarket sector, CNP sales and e-commerce;
- three 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 *Autorité de contrôle prudentiel et de résolution*, are appointed for a three-year term. Their term can be renewed.

The President is appointed among 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. Christian Noyer, the Governor of the Banque de France, has been the President of the Observatory since 17 November 2003.

Operating procedures

In accordance with Article R. 142-23 *et seq.* of the *Monetary and Financial Code*, the Observatory meets at least twice a year at the invitation of its President. The meetings are held in camera. Measures proposed within the Observatory are adopted by absolute majority. Each member has one vote; the President has the casting vote in the event of a tie. In 2003, the Observatory adopted rules of procedure that delineate its working conditions.

The secretariat of the Observatory, which is ensured by the Banque de France, is responsible for organising and monitoring meetings, centralising the information required for the establishment of payment card fraud statistics, 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 cards. The secretariat also drafts the Observatory's annual report that is submitted 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 working groups by absolute majority. The working groups report on their work at each meeting of the Observatory. The groups may hear all persons that are liable to 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 card technology watch. In 2010, the Observatory decided to set up a third working group to look at the question of 3D-Secure deployment.

Given the sensitivity of the data exchanged, the members of the Observatory and its secretariat, which are bound by professional secrecy under Article R. 142-25 of the *Monetary and Financial Code*, must 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.

Members of the Observatory

Pursuant to Article R. 142-22 of the *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 Prudential Supervisory and Resolution Authority (*Autorité de contrôle prudentiel et de résolution*), are appointed for a three-year term by order of the Minister of the Economy, Industrial Renewal and Digital Technology. The most recent appointment orders were issued on 6 September 2013 and 11 December 2013.

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Philippe GOUJON
Deputy
Michèle ANDRÉ
Senator

Representatives of the Secretary General of the *Autorité de contrôle prudentiel et de résolution*

Emmanuel CARRERE
Philippe RICHARD
General Secretariat

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

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

Nominated on proposition by the Minister of the Economy, Industrial Renewal and Digital Technology:

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

- The Head of the Treasury or his/her representative:
  Magali CESANA
  Fabrice WENGER

- The Director General for Competitiveness, Industry and Services or his/her representative:
  Mireille CAMPANA

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

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  Nathalie KHOKHOLKOFF
  Charles MOYNOT
  Régis PIERRE

Nominated on proposition by the Minister of the Interior:

- The Head of the Central Office for the Fight against Crimes Linked to Information and Communication Technologies or his/her representative:
  Valérie MALDONADO
  Philippe DEVRED

Nominated on proposition by the Minister of Defence:

- The Director General of the *Gendarmerie nationale* or his/her representative:
  Éric FREYSSINET

Representatives of payment card issuers

Frédéric COLLARDEAU
Head of Payments
La Banque Postale
Gilbert ARIRA
Director
"CB" Bank Card Consortium
Jean-François DUMAS
Vice-President
American Express France
Willy DUBOST
Director, Systems and Payment Instruments
Fédération bancaire française
Caroline SELLIER
Director, Risk Management and Fraud Prevention
Natixis Paiements
François LANGLOIS
Director, Institutional Relations
BNP Paribas Personal Finance
Frédéric MAZURIER
Administrative and Financial Director
Carrefour Banque
Gérard NEBOUY
CEO
Visa Europe France
Régis FOLBAUM
Chairman and CEO
MasterCard France
Narinda YOU
Director
Interbank Strategy and Coordination
Crédit Agricole SA

Representatives of the Consumer Board of the National Consumers' Council

Régis CREPY
Confédération nationale
Associations familiales catholiques (CNAFC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)
Patrick MERCIER
President
Association de défense d'éducation et d'information du consommateur (ADEIC)
Frédéric POLACSEK
Conseil national des associations familiales laïques (CNAFAL)
Maxime CHIPOY
UFC-Que Choisir

Representatives of merchants' professional organisations

Philippe JOGUET
Director, Sustainable Development, CSR, Financial Issues
Fédération des entreprises du commerce et de la distribution (FCD)
Marc LOLIVIER
General Delegate
Fédération du e-commerce et de la vente à distance (Fevad)
Jean-Jacques MELI
Chambre de commerce et d'industrie du Val d'Oise
Jean-Marc MOSCONI
General Delegate
Mercatel
Philippe SOLIGNAC
Vice-President
Chambre de commerce et d'industrie de Paris/ACFCI

Persons chosen for their expertise

Eric BRIER
Chief Security Officer
Ingenico
David NACCACHE
Professor
École normale supérieure
Sophie NERBONNE
Deputy Head of Legal and International Affairs and Assessments
Commission nationale de l'informatique et des libertés (CNIL)

Statistics

The following statistics were compiled from the data that the Observatory for Payment Card Security received from:

- the 130 members of the "CB" Bank Card Consortium, through the consortium, MasterCard and Visa Europe France;
- ten three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Crédit Agricole Consumer Finance (Finaref and Sofinco), Cofidis, Cofinoga, Diners Club, Franfinance, JCB and UnionPay;
- issuers of the electronic purse Moneo.

Total number of cards in circulation in 2013: 85.5 million
- 68.4 million four-party cards ("CB", MasterCard, Visa and Moneo);
- 17.1 million three-party cards.

Number of cards reported lost or stolen[1] in 2013: around 861,000

Domestic transactions involve a French issuer and a French accepting merchant.

Until 2009, there were two types of international transactions:
- French issuer/foreign acceptor;
- foreign issuer/French acceptor.

In 2010, the Observatory began distinguishing international transactions within SEPA from those conducted elsewhere in the world. As a result, there are now four types of international transactions:
- French issuer/non-SEPA foreign acceptor;
- non-SEPA foreign issuer/French acceptor;
- French issuer/SEPA foreign acceptor;
- SEPA foreign issuer/French acceptor.

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

Table 1

The payment card market in France in 2013 – Issuance

(volume in millions; value in EUR billions)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	**Value**	**Volume**	**Value**	**Volume**	**Value**
Four-party cards						
Face-to-face payments and UPT	7,688.46	332.48	137.26	8.30	43.25	3.67
Card-not-present payments excluding internet payments	17.66	2.46	9.49	0.72	7.13	0.52
Card-not-present internet payments	709.69	53.40	128.66	5.18	31.38	1.98
Withdrawals	1,496.32	117.51	28.25	3.14	19.97	2.84
Total	**9,912.14**	**505.84**	**303.66**	**17.34**	**101.71**	**9.01**
Three-party cards						
Face-to-face payments and UPT	117.46	12.84	6.72	0.84	6.27	1.04
Card-not-present payments excluding internet payments	1.82	0.15	na	na	na	na
Card-not-present internet payments	9.53	1.29	3.05	0.35	0.99	0.16
Withdrawals	3.41	0.31	na	na	na	na
Total	**132.22**	**14.58**	**9.77**	**1.20**	**7.26**	**1.20**
Grand total	**10,044.35**	**520.42**	**313.43**	**18.54**	**108.97**	**10.20**

Source: Observatory for Payment Card Security.

Table 2

The payment card market in France in 2013 – Acquisition

(volume in millions; value in EUR billions)

	French issuer, French acquirer		SEPA foreign issuer, French acquirer		Non-SEPA foreign issuer, French acquirer	
	Volume	**Value**	**Volume**	**Value**	**Volume**	**Value**
Four-party cards						
Face-to-face payments and UPT	7,688.46	332.48	170.65	11.79	65.17	7.80
Card-not-present payments excluding internet payments	17.66	2.46	4.49	1.24	2.09	0.99
Card-not-present internet payments	709.69	53.40	29.67	3.72	10.51	1.90
Withdrawals	1,496.32	117.51	21.68	3.61	7.97	1.74
Total	**9,912.14**	**505.84**	**226.49**	**20.37**	**85.73**	**12.43**
Three-party cards						
Face-to-face payments and UPT	117.46	12.84	4.60	1.00	6.74	3.22
Card-not-present payments excluding internet payments	1.82	0.15	na	na	na	na
Card-not-present internet payments	9.53	1.29	0.67	0.11	0.41	0.10
Withdrawals	3.41	0.31	na	na	0.27	0.11
Total	**132.22**	**14.58**	**5.26**	**1.11**	**7.43**	**3.44**
Grand total	**10,044.35**	**520.42**	**231.76**	**21.48**	**93.16**	**15.86**

Source: Observatory for Payment Card Security.

Table 3

Breakdown of four-party card fraud by type of transaction, type of fraud and geographical zone in 2013 – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	562.0	43,986.7	63.0	7,863.6	87.7	16,963.3
Lost or stolen cards	546.3	42,988.2	42.9	4,217.8	17.9	3,748.3
Intercepted cards	8.2	410.9	0.5	32.0	0.1	13.3
Forged or counterfeit cards	2.9	163.0	7.5	1,484.5	56.4	10,356.3
Misappropriated numbers	4.3	411.3	10.4	1,853.3	11.8	2,567.7
Other	0.3	13.3	1.7	275.9	1.5	277.6
Card-not-present payments excluding internet payments	355.9	28,947.0	117.7	11,268.1	49.6	6,397.0
Lost or stolen cards	0.0	0.3	7.6	779.3	3.9	555.5
Intercepted cards	0.0	0.0	0.1	5.6	0.1	3.2
Forged or counterfeit cards	0.0	0.1	37.0	2,791.1	9.9	1,706.1
Misappropriated numbers	355.9	28,946.6	72.8	7,662.1	33.4	4,034.3
Other	0.0	0.0	0.3	30.0	2.4	97.9
Card-not-present internet payments	972.2	122,969.2	857.2	45,931.6	122.5	15,530.6
Lost or stolen cards	0.0	5.4	63.2	3,996.0	9.2	1,443.7
Intercepted cards	0.0	0.2	0.3	9.7	0.0	2.7
Forged or counterfeit cards	0.0	3.3	94.2	5,906.9	19.9	2,532.8
Misappropriated numbers	972.2	122,958.9	698.3	35,941.8	93.1	11,523.0
Other	0.0	1.5	1.2	77.2	0.2	28.5
Withdrawals	130.5	38,237.8	5.3	1,129.3	186.9	29,887.4
Lost or stolen cards	129.8	38,031.9	3.6	835.8	5.2	832.0
Intercepted cards	0.6	195.5	0.0	5.6	0.1	20.4
Forged or counterfeit cards	0.0	1.5	1.4	242.6	172.1	27,468.5
Misappropriated numbers	0.1	8.9	0.1	9.5	1.5	223.4
Other	0.0	0.0	0.2	35.9	7.9	1,343.1
Total	**2,020.6**	**234,140.8**	**1,043.3**	**66,192.7**	**446.7**	**68,778.3**

Source: Observatory for Payment Card Security.

Table 4

Breakdown of four-party card fraud by type of transaction, type of fraud and geographical zone in 2013 – Acquisition

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		SEPA foreign issuer, French acquirer		Non-SEPA foreign issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	562.0	43,986.7	193.9	26,974.3	303.9	57,896.4
Lost or stolen cards	546.3	42,988.2	66.5	2,568.5	41.7	8,381.1
Intercepted cards	8.2	410.9	2.0	592.2	0.6	95.6
Forged or counterfeit cards	2.9	163.0	16.0	1,404.9	101.9	17,801.0
Misappropriated numbers	4.3	411.3	107.8	22,066.0	158.0	31,167.8
Other	0.3	13.3	1.7	342.6	1.6	450.9
Card-not-present payments excluding internet payments	355.9	28,947.0	na	na	na	na
Lost or stolen cards	0.0	0.3	na	na	na	na
Intercepted cards	0.0	0.0	na	na	na	na
Forged or counterfeit cards	0.0	0.1	na	na	na	na
Misappropriated numbers	355.9	28,946.6	na	na	na	na
Other	0.0	0.0	na	na	na	na
Card-not-present internet payments	972.2	122,969.2	na	na	na	na
Lost or stolen cards	0.0	5.4	na	na	na	na
Intercepted cards	0.0	0.2	na	na	na	na
Forged or counterfeit cards	0.0	3.3	na	na	na	na
Misappropriated numbers	972.2	122,958.9	na	na	na	na
Other	0.0	1.5	na	na	na	na
Withdrawals	130.5	38,237.8	11.5	907.8	3.3	945.5
Lost or stolen cards	129.8	38,031.9	10.9	809.0	1.1	338.6
Intercepted cards	0.6	195.5	0.1	16.4	0.0	6.6
Forged or counterfeit cards	0.0	1.5	0.4	60.4	2.0	569.0
Misappropriated numbers	0.1	8.9	0.1	18.2	0.1	30.4
Other	0.0	0.0	0.0	3.8	0.0	0.8
Total	**2,020.6**	**234,140.8**	**205.4**	**27,882.1**	**307.1**	**58,841.9**

Source: Observatory for Payment Card Security.

Table 5

Breakdown of three-party card fraud by type of transaction, type of fraud and geographical zone in 2013 – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	4.23	1,771.38	0.66	303.12	3.77	777.65
Lost or stolen cards	0.92	319.18	0.09	36.98	0.55	182.14
Intercepted cards	0.94	286.93	0.12	52.58	0.02	18.07
Forged or counterfeit cards	0.73	183.38	0.41	207.25	3.10	559.52
Misappropriated numbers	0.19	62.59	0.04	5.01	0.10	16.97
Other	1.45	919.30	0.00	1.30	0.01	0.95
Card-not-present payments excluding internet payments	0.26	265.62	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.03	14.20	na	na	na	na
Other	0.24	251.42	na	na	na	na
Card-not-present internet payments	5.28	2,008.95	7.04	1,394.45	2.57	639.21
Lost or stolen cards	0.50	116.90	0.09	2.01	0.06	6.01
Intercepted cards	0.03	14.76	0.07	3.04	0.01	1.27
Forged or counterfeit cards	0.14	18.31	0.15	7.67	0.11	20.66
Misappropriated numbers	4.18	1,576.17	6.70	1,360.63	2.35	602.56
Other	0.42	282.80	0.04	21.10	0.03	8.72
Withdrawals	1.75	372.31	na	na	na	na
Lost or stolen cards	1.27	211.41	na	na	na	na
Intercepted cards	0.08	27.35	na	na	na	na
Forged or counterfeit cards	0.30	83.39	na	na	na	na
Misappropriated numbers	0.10	48.15	na	na	na	na
Other	0.01	2.01	na	na	na	na
Total	**11.52**	**4,418.26**	**7.70**	**1,697.56**	**6.34**	**1,416.86**

Source: Observatory for Payment Card Security.

Table 6

Breakdown of three-party card fraud by type of transaction, type of fraud and geographical zone in 2013 – Acquisition

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	4.23	1,771.38	0.33	200.66	5.66	3,278.05
Lost or stolen cards	0.92	319.18	0.03	18.35	0.54	318.32
Intercepted cards	0.94	286.93	0.02	9.98	0.03	12.23
Forged or counterfeit cards	0.73	183.38	0.17	87.80	4.63	2,675.63
Misappropriated numbers	0.19	62.59	0.06	15.01	0.23	125.01
Other	1.45	919.30	0.04	69.53	0.22	146.86
Card-not-present payments excluding internet payments	0.26	265.62	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.03	14.20	na	na	na	na
Other	0.24	251.42	na	na	na	na
Card-not-present internet payments	5.28	2,008.95	2.82	741.61	2.82	741.61
Lost or stolen cards	0.50	116.90	0.16	66.70	0.16	66.70
Intercepted cards	0.03	14.76	0.01	9.15	0.01	9.15
Forged or counterfeit cards	0.14	18.31	0.98	280.87	0.98	280.87
Misappropriated numbers	4.18	1,576.17	1.65	378.76	1.65	378.76
Other	0.42	282.80	0.02	6.13	0.02	6.13
Withdrawals	1.75	372.31	na	na	na	na
Lost or stolen cards	1.27	211.41	na	na	na	na
Intercepted cards	0.08	27.35	na	na	na	na
Forged or counterfeit cards	0.30	83.39	na	na	na	na
Misappropriated numbers	0.10	48.15	na	na	na	na
Other	0.01	2.01	na	na	Na	na
Total	**11.52**	**4,418.26**	**2.78**	**1,208.95**	**11.58**	**5,302.60**

Source: Observatory for Payment Card Security.

Definition and typology of payment card fraud

Definition of fraud

For the purposes of drawing up statistics, the Observatory considers that the following acts constitute fraud: all acts that contribute to the preparations for illegitimate use and/or illegitimate use of payment cards or data stored on them:

- that cause harm to the account-holding bank, be it the bank of the cardholder or of the acceptor (e.g. merchant or general government agency, on its own account or within a payment scheme),[1] the cardholder, merchant, issuer, insurer, trusted third parties or any parties involved in the chain of design, manufacture, transport, or distribution of physical or logical data that could incur civil, commercial or criminal liability;

- irrespective of:
  – the methods used to obtain, without lawful reason, cards or data stored on them (theft, taking possession of cards, physical or logical data, personalisation data and/or misappropriation of secret codes, and/or security codes, magnetic stripe and chip hacking),

  – the procedures for using cards or the data stored on them (payments or withdrawals, face-to-face or card-not-present, via physical use of the card or the card number, via UPTs, etc.),

  – the geographical area of issuance or use of the card and the data held on it:
    - French issuer and card used in France,
    - foreign issuer within SEPA and card used in France,
    - foreign issuer outside SEPA and card used in France,
    - French issuer and card used abroad within SEPA,
    - French issuer and card used abroad outside SEPA,

  – the type of payment card,[2] including electronic purses;

- whether or not the fraudster is a third party, the account-holding bank, the cardholder him/herself (for example, using the card after it has been declared lost or stolen, wrongful termination of transactions), the acceptor, the issuer, an insurer, a trusted third party, etc.

1 In the case of the internet, the merchant may be different from the service provider or a trusted third party (payments, donations made by internet users wishing to support a website, cause, etc.).
2 As defined by Article L. 132-1 of the *Monetary and Financial Code* as worded prior to 1 November 2009.

Fraud typology

The Observatory has in addition defined a fraud typology that makes distinctions in the following categories.

Origin of fraud:

• lost or stolen cards: the fraudster uses a payment card following card theft or loss;

• intercepted cards: cards intercepted when sent by issuers to lawful cardholders. While this type of origin is similar to theft or loss, it is nonetheless different because it is not easy for a cardholder to ascertain that a fraudster is in possession of a card that belongs to him/her; it also entails risks specific to procedures for sending cards;

• forged or counterfeit cards: an authentic payment card may be falsified by modifying magnetic stripe data, embossing or programming. Creating a counterfeit card means creating an object that appears to be an authentic payment card and/or is capable of deceiving UPTs or a person. For payments made via UPTs, counterfeit cards incorporate the data required to deceive the system. In face-to-face transactions, counterfeit cards present certain security features found on authentic cards (including visual appearance), incorporate data stored on authentic cards, and are intended to deceive acceptors;

• misappropriated numbers: a cardholder's card number is taken without his/her knowledge or created through card number generation (see fraud techniques) and used in card-not-present transactions;

• unallocated card numbers: use of a true PAN[3] that has not been attributed to a cardholder, generally in card-not-present transactions;

• splitting payments: splitting up payments so as not to exceed the authorisation limit defined by the issuer.

Fraud techniques:

• skimming: technique that consists in copying the magnetic stripe of a payment card using an illegal card reader known as a skimmer embedded in merchants' payment terminals or ATMs. The PIN may also be captured visually using a camera or by tampering with the keypad of a payment terminal. Captured data are then re-encoded onto the magnetic stripe of a counterfeit card;

• phishing: technique used by criminals to obtain personal data, chiefly through unsolicited emails that take users to fraudulent websites that look like trusted ones;

• opening of a fraudulent account: opening of an account using false personal data;

3 Personal Account Number.

- identity theft: fraudulent acts linked to payment cards and involving the use of another person's identity;

- wrongful repudiation: a cardholder, acting in bad faith, disputes a valid payment order that he/she initiated;

- hacking automated machines: techniques that consist in placing card duplication devices in UPTs or ATMs;

- hacking automated data systems, servers or networks: fraudulent intrusion into these systems;

- card number generation: using issuers' own rules to create payment card numbers that are then used in fraudulent transactions.

Types of payment:

- face-to-face payment, carried out at the point of sale or UPT;
- card-not-present payment carried out online, by mail, by fax/telephone, or any other means;
- withdrawal (withdrawal from an ATM or any other type of withdrawal).

Distribution of losses between:

- the merchant's bank, the acquirer of the transaction;
- the cardholder's bank, the issuer of the card;
- the merchant;
- the cardholder;
- insurers, if any;
- any other participant.

The geographical area of issue or use of the card or of the data encoded on the card:

- the issuer and acquirer are both established in France. In this case, the transaction is qualified as national or domestic. However, for card-not-present payments, the fraudster may operate from abroad;
- the issuer is established in France and the acquirer is abroad within SEPA;
- the issuer is established in France and the acquirer is abroad outside SEPA;
- the issuer is established abroad within SEPA and the acquirer is in France;
- the issuer is established abroad outside SEPA and the acquirer is in France.

Merchant sector of activity for CNP payments:

- food: groceries, supermarkets, superstores;
- account loading, person to person sales: sites enabling online sales between private individuals;
- insurance;
- general and semi-general trade: textiles/apparel, department stores, mail-order sales, private sales;
- household goods, furnishings, DIY;
- online gaming;
- technical and cultural products: IT hardware and software, photographic equipment, books, CDs/DVDs;
- health and beauty;
- personal services: hotels, rental services, box office, charities;
- professional services: office equipment, courier service;
- telephony and communication: telecommunication/mobile telephony hardware and services;
- travel, transportation: rail, air, sea;
- miscellaneous.

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

Managing Editor
Denis Beau,
Director General Operations
Banque de France

Editor-in-Chief
Frédéric Hervo,
Director of Payment Systems and Market Infrastructures
Banque de France

Editorial Secretariat
Marcia Toma, Josiane Usseglio-Nanot

Production
Banque de France
Press and Communication Directorate

Technical production
Nicolas Besson, Pierre Bordenave, Angélique Brunelle, Alexandrine Dimouchy, Christian Heurtaux, François Lécuyer, Aurélien Lefèvre, Carine Otto, Isabelle Pasquier

Orders
Observatory for Payment Card Security
011-2323
Telephone: +1 42 92 96 13
Fax: +1 42 92 31 74

Imprint
Banque de France

ISSN 1768-2991

Website
www.observatoire-cartes.fr

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

Upon request, printed copies can be obtained free of charge, while stocks last (see address opposite).

The Observatory for Payment Card Security reserves the right to suspend distribution of the report and to limit the number of copies per person.