# 2014 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 2014
# of the Observatory for payment card security

*addressed to*

**The Minister of the Economy,**
**Industry 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* Observatoire de la sécurité des cartes de paiement *(Observatory for Payment Card Security – hereinafter the Observatory), referred to in section I of Article L141-4 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 abovementioned 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 12th* Annual Report of the Observatory for Payment Card Security, *covering the 2014 financial year, contains four parts, summarised as follows.*

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

*The continued decline in the fraud rate for internet card payments reflects efforts by issuers and e-merchants to make these transactions more secure.*

*Over 90% of cardholders now have cards that offer strong authentication solutions. Take-up of strong authentication by e-merchants now stands at close to 60%, substantially higher than in 2013 (43%), chiefly owing to adoption of 3D-Secure by smaller e-merchants and the ability to activate authentication on the basis of risk analyses.*

*The failure rate for authenticated transactions remains on a par with the failure rate for non-authenticated transactions, showing that there are no obstacles to the adoption of this type of protective solution by e-merchants.*

*Accordingly, the Observatory reminds all affected parties that the widespread introduction of strong authentication solutions is a priority for the Eurosystem and also for the European Banking Authority (EBA), whose guidelines on the security of internet payments will come into force on 1 August 2015.*

## Part 2: fraud statistics for 2014

*The fraud rate for payments and withdrawals made using cards issued in France was stable in 2014 for the second year running at 0.069%. Including transactions involving cards issued in other countries, the overall fraud rate also remained steady at 0.080% for the third year in a row.*

*However, the steady overall rate masked contrasting trends:*

- *For the first time since 2004, total fraud in domestic transactions fell, shrinking to EUR 235 million from EUR 239 million in 2013, even though the value of transactions continued to rise. As a result, the fraud rate for domestic transactions declined from 0.046% in 2013 to 0.043%, with the fraud rate for face-to-face payments falling to 0.010% from 0.013% in 2013.*

  *The fraud rate for card-not-present (CNP) payments fell for the third year running, easing to 0.248% compared with 0.269% in 2013. However, amid sustained growth in e-commerce, the amount of CNP payment fraud continued to rise. CNP payments still account for the lion's share of fraud by value (66.5%) but for just 11.6% of the total value of payments.*

  *Some sectors, notably telephony and communication, feature fraud rates for online transactions that are markedly higher than those recorded for e-merchants as a whole, raising the need for increased vigilance by these players.*

*The fraud rate for withdrawals continued to rise, climbing to 0.034% from 0.033% in 2013, as ATM attacks and thefts of cards with PINs remained the methods of choice for organised fraud rings.*

*Meanwhile, the initial statistical data on contactless payments reveal that the fraud rate for the last nine months of 2014 was low (0.015%), sitting between the rates recorded for face-to-face payments and ATM withdrawals. This type of fraud almost always stems from card theft or loss, supporting the Observatory's assessment that the risk of fraud linked to contactless technology is limited.*

- *Fraud in international transactions continued to increase, rising from EUR 231.3 million in 2013 to EUR 266 million in 2014. Because the value of transactions increased sharply, the fraud rate for international transactions actually fell from 0.480% in 2013 to 0.456%, but it was still more than ten times higher than the rate for domestic transactions. Accordingly, international transactions accounted for 41% of the total amount of fraud involving cards issued in France, but for just 6% of the total value of transactions.*

  *In particular, fraud rates for CNP payments using French cards both within and outside the Single Euro Payments Area (SEPA) remained at high levels (0.910% and 0.960% respectively), reflecting the fact that improved protection for CNP transactions on French websites has prompted criminals to shift their focus to international targets. The entry into force in summer 2015 of guidelines issued by the EBA on the introduction of strong customer authentication solutions should enable CNP payment fraud to be prevented more effectively within SEPA.*

## Part 3: technology watch on the use of biometrics as an authentication factor

*Some biometric authentication methods are already used routinely by a growing section of the general public and could be used to enhance the security of face-to-face and CNP payments and withdrawals made with cards. For this reason, the Observatory decided to review these techniques and their implementation requirements.*

*The use of biometric techniques in France is strictly regulated by the Data Privacy Act. Accordingly, the Observatory notes that an authorisation application must be filed with the French Data Privacy Agency (CNIL) before such techniques may be employed with payment solutions.*

*The Observatory notes that the trials being conducted in France are primarily aimed at testing the user-friendliness of biometric solutions. Prior to large-scale deployment, the Observatory stresses the need to analyse the risks created in situations where biometric authentication is used, in order to ensure that solutions provide a level of protection at least equivalent to that offered by existing techniques, i.e. PIN and smartcard for face-to-face payments, one-time password for CNP payments.*

*Furthermore, given the shortage of available information to assess the security level of biometric solutions in comparison to existing technologies, e.g. smartcards and mobile phone SIM cards,*

*the Observatory calls on participants to establish security standards that can be used to evaluate proposed solutions by assessing all of their components and parameters, including the equipment used to sense and process biometric information, algorithms and use cases.*

*The Observatory also urges participants to be on their guard while trialling biometric solutions, since the compromise of biometric information used in pilots could threaten the introduction of larger-scale solutions in the future.*

*In view of the inherent limitations of biometrics and the immaturity of security evaluations for these solutions, the Observatory continues to recommend maintaining an alternative authentication solution that can replace the biometric method.*

## Part 4: summary of the conference "Towards retail payments 2.0: The new security challenges" organised on 22 October 2014

*On 22 October 2014, the Banque de France and the European Central Bank teamed up to organise an international conference in Paris on the new security challenges for payment instruments. The day-long event provided an opportunity for European institutions, national authorities and market participants to dialogue on these topics. The discussions identified three main areas that will shape future work on the security of payment instruments.*

*First, cooperation between both European authorities through fora such as SecuRe Pay[1] and these authorities and payments market stakeholders, including banks, companies, solution providers and consumers, is viewed as an effective response to the need for consistent development of security requirements on the European market.*

*Second, at a time when innovation is driving swift changes in consumer practices, European authorities need to constantly factor market developments into what they do. In this regard, work done within SecuRe Pay and by the European Banking Authority on the security of internet payments illustrates this determination to promote safe and efficient payment services in the most innovative segments.*

*Third, in a rapidly-evolving sector, the authorities need to strike the right balance between innovation and security, ensuring that regulatory requirements are not a barrier to the development of new services. Discussions conducted as part of the revision of the Payment Services Directive, notably on regulating third party payment providers and their security requirements, reflect a resolve to open up the payments market to innovation while controlling the risks for participants and consumers.*

1 SecuRe Pay is a European forum that is co-chaired by the ECB and the EBA. It enables central banks and national bank supervisors to gather and talk about matters relating to the security of cashless payment instruments.

# Stock-taking of measures to protect internet card payments

The Observatory regularly monitors fraud in internet card 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 to phase in 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 of the Observatory and the Banque de France, as well as those carried out at European level to promote safer internet payments (2|).

## 1| Progress in enhancing the security of internet card payments

Faced with an upsurge in attempted fraud and attacks geared to compromise payment instruments or data, participants have to adapt continually to shifting fraud threats and the measures taken in response. Among the various measures available, the Observatory continues to view strong cardholder authentication as a priority.

In this setting, the Observatory gathers half-yearly statistics from the main banks to monitor the roll-out of authentication solutions.

This statistical monitoring exercise, which covers 58.8 million payment cards and EUR 39.6 billion in payments (including EUR 12.4 billion in payments protected by 3D-Secure),[1] offers a way to measure quantitative and qualitative progress in the implementation of strong authentication solutions.

The ninth data gathering exercise, which covered the period from 1 November 2014 to 30 April 2015, highlighted three key points.

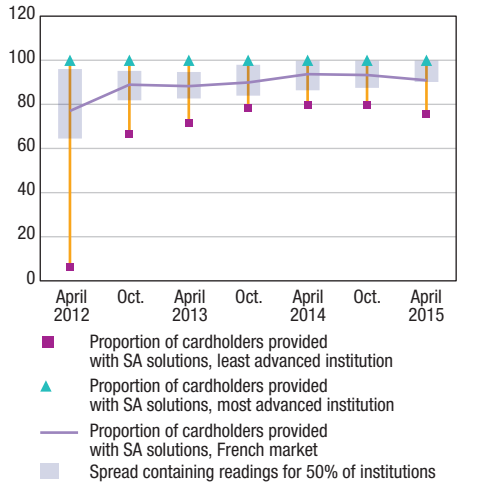
### 1|1 Virtually all cardholders have now been provided with at least one strong authentication solution

The average proportion of cardholders provided with at least one strong authentication solution has sharply increased in the last three years, rising from 77% to over 90%. The slight average decline observed in the most recent statistics (90.9% in April 2015, compared with 93.3% in October 2014) is due to migration of the clients of a major marketplace issuer to a new strong authentication method.

**Chart 1**

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

*( %)*




*Source: Observatory for Payment Card Security.*

1 Interbank protocol for the protection of online card payments enabling cardholder authentication.

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 authentication solution is to send an OTP by text message.[2]

## 1|2 The failure rate[3] for transactions subject to strong authentication is similar to the failure rate for non-secured transactions

The Observatory has observed an improvement in the failure rate for authenticated payments over the data collection periods, with the rate falling from 18.0% in 2011 to 14.6% 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 widespread adoption of 3D-Secure by large e-merchants.

As a result, the failure rate for authenticated transactions actually fell slightly below the rate for non-authenticated transactions, on which the Observatory has collected data since 2013 and which stands at 14.9%. **The Observatory notes this as evidence that implementation of strong cardholder authentication wherever possible and appropriate is not a hindrance to the development of e-commerce.**

## 1|3 Use of 3D-Secure authentication continues to rise, supported by increased take-up among e-merchants

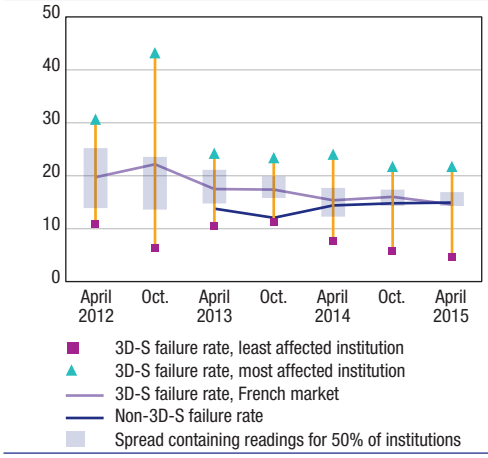
The share of authenticated transactions went up in value terms from 29.7% to 31.3% over the course of one year. This increase contributed to the decrease in the fraud rate for CNP payments in 2014.

Furthermore, the proportion of merchants supporting strong authentication solutions surged from 43% to 58%. This increase is chiefly due to the adoption of 3D-Secure by smaller e-merchants and the ability to activate 3D-Secure authentication on the basis of risk analyses.

**Chart 2**

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

*(%)*

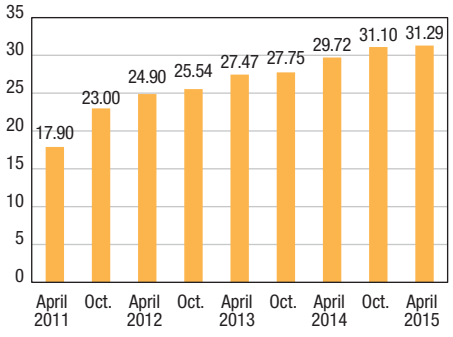



*Source: Observatory for Payment Card Security.*

**Chart 3**

**Proportion of online payments protected by 3D-Secure (value terms)**

*(%)*




*Source: Observatory for Payment Card Security.*

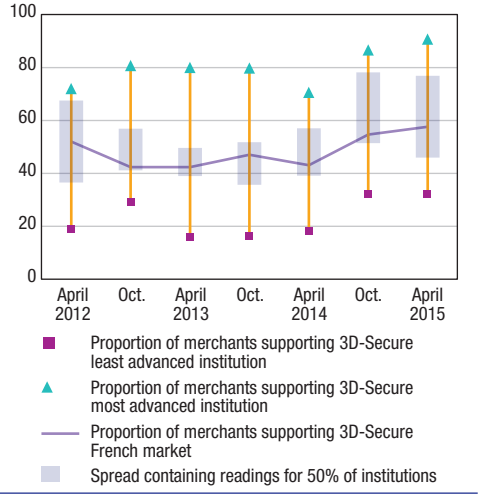
2 A one-time password is sent by text message for each transaction and used to authenticate the card holder.

3 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 4**

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

*(%)*




*Source: Observatory for Payment Card Security.*

# 2| Initiatives by national and European bodies aimed at enhancing the security of internet payments

## 2|1 Initiatives conducted by the Banque de France and the Observatory

The Banque de France pursued its efforts to raise awareness among e-merchants and their payment service providers about fraud prevention, building on steps taken in 2013 at the Observatory's request. The Banque de France also introduced a procedure for payment chain participants to report production incidents occurring in connection with cardholder authentication. This information will be used to identify more effectively weaknesses in deployed solutions that potentially reduce the conversion rate[4] of authenticated payments.

The Observatory noted that in 2014 the majority of large e-merchants contacted had introduced action plans to curb fraud rates, particularly through strong cardholder authentication mechanisms. This should aid in the domestic implementation of European regulatory changes aimed at enhancing the security of internet payments.

## 2|2 Initiatives by European authorities

In December 2014, the European Banking Authority (EBA) published guidelines on the security of internet payments. Drawing largely on earlier recommendations issued by the SecuRe Pay Forum in 2013, the guidelines notably seek to encourage widespread introduction of strong customer authentication by recommending:

- that card issuers support strong authentication of cardholders;

- and that payment service providers require their online merchants to promote solutions that enable issuers to perform strong authentication of cardholders during internet transactions. Alternative authentication measures may be considered for pre-identified types of low-risk transactions, e.g. based on a transaction risk analysis.

The EBA guidelines entered into force on 1 August 2015. They have been incorporated into the Eurosystem's payment instrument oversight frameworks.

Systematic use of strong authentication for internet payments will also be covered in the revised version of the Payment Services Directive (PSD2), which is scheduled to be published in the second half of 2015 and which will have to be transposed into domestic law.[5]

## 2|3 National Conference on Payments recognises the role of strong authentication in developing straightforward, secure means of payment

The National Conference on Payments, which was organised by the Minister for Finance and Public Accounts, Michel Sapin, and the Minister for the Economy, Industry and Digital Technology,

4 The conversion rate is used by online merchants to measure the number of purchases made relative to the number of visits to the website.
5 See Chapter 4 for more details on the PSD2 regulatory mechanism.

Emmanuel Macron, was held on 2 June 2015. The purpose of the event was to outline a national strategy to modernise payment instruments and meet users' needs in terms of speed, security and accessibility, and also to promote the use of innovative payment instruments and foster a competitive national payments industry.

The widespread roll-out of strong customer authentication solutions for CNP payments was clearly identified as part of the process of developing straightforward, secure means of payment to respond to strong growth in online commerce and the substantial proportion of total card payment fraud attributable to CNP payments.

Proposals put forward in the lead-up to the conference recommended encouraging initiatives that would support more widespread take-up of strong authentication, by stepping up communication and education measures targeting merchants and users. It was also proposed to support "second generation" strong authentication solutions, including biometric techniques and methods that offer the benefit of not requiring e-merchants to have special equipment.

The introduction of these new solutions would be intended among other things to address concerns voiced by e-merchants, particularly with regard to the sharp growth in payments by mobile phone and the lack of suitable solutions for this type of terminal. The new solutions that establish themselves in the coming years will undoubtedly be those that marry ease of use and security with viable business models.

## 3| Conclusion

The Observatory urges all payment chain participants to keep up efforts to enhance the security of internet payments. Given the substantial increase in the proportion of e-commerce websites that support strong authentication (to almost 60% in April 2015), the Observatory acknowledges that widespread introduction of these solutions is well underway. These efforts should remain a priority, as they will make it possible to comply with Eurosystem and EBA guidelines on the security of internet payments, which are set to come into force on 1 August 2015.

# Fraud statistics for 2014

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 2014 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. To promote consistency with the European fraud statistics and rates provided by the ECB,[1] data pertaining exclusively to cards issued in France are presented separately. By construction, these statistics do not include fraud occurring in France and involving cards issued elsewhere, when the Observatory is able to measure such fraud. For the first time this year, the Observatory is also publishing partial fraud data on contactless payment cards. Appendix 5 to this report presents a series of detailed fraud indicators.

**Box 1**

## Fraud statistics: respondents

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

*The 2014 statistics calculated by the Observatory thus cover:*

- *EUR 558.7 billion in transactions in France and in other countries made with 71.0 million four-party cards issued in France (including 1.98 million electronic purses and 30.6 million contactless cards);*
- *EUR 17.2 billion in transactions primarily in France with 14.6 million three-party cards issued in France;*
- *EUR 49.0 billion in transactions in France 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 Cf. *Third Report On Card Fraud*, February 2014, available in English on the ECB website: *https://www.ecb.europa.eu/pub/pub/paym/html/index.en.html*

## 1| Overview

In 2014, the total amount of fraud involving payments and withdrawals made using French payment cards in France and abroad came to EUR 395.6 million, a 5.0% increase on 2013. Meanwhile, the total value of transactions increased 4.9% relative to 2013 to reach EUR 575.9 billion.

As a result, the **fraud rate for French payment cards was steady at 0.069%** after rising for three years in a row.

The number of French cards for which at least one fraudulent transaction was recorded in 2014 climbed by 5.2% compared with 2013 to 905,600.

When transactions conducted in France using cards issued in other countries are included as well, the total amount of fraud increased by 6.5% compared with 2013 to EUR 500.6 million in 2014, while the total value of transactions climbed 6.5% to EUR 624.9 billion.

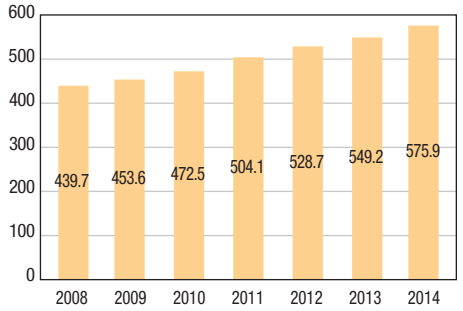
As a result, the overall fraud rate for transactions handled by French schemes, which includes payments and withdrawals in France and abroad made using French cards, along with payments and withdrawals in France made using foreign cards, was steady at 0.080% for the second year running, after increasing for five years in a row.

The average value of a fraudulent transaction fell to EUR 112 from EUR 116 in 2013.

**Chart 1**

**Value of transactions, French cards**

*(EUR billions)*

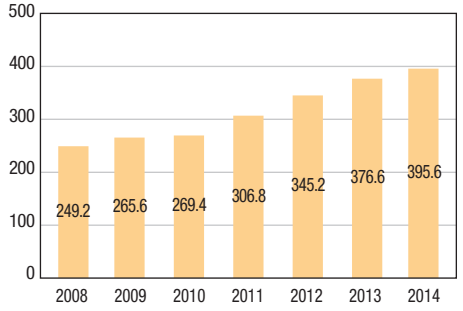



*Source: Observatory for Payment Card Security.*

**Chart 2**

**Amount of fraud, French cards**

*(EUR millions)*

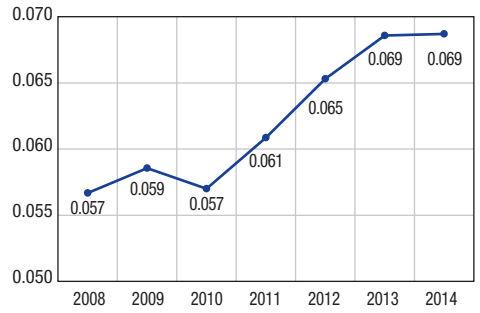



*Source: Observatory for Payment Card Security.*

**Chart 3**

**Fraud rate, French cards**

*(%)*

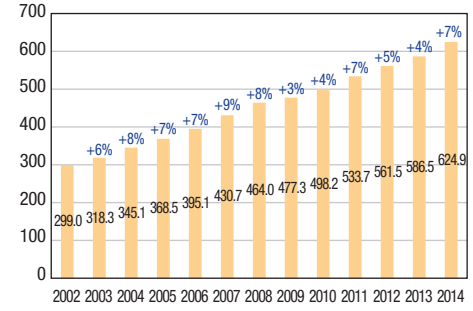



*Source: Observatory for Payment Card Security.*

**Chart 4**

**Transactions handled by French schemes**

*(EUR billions)*

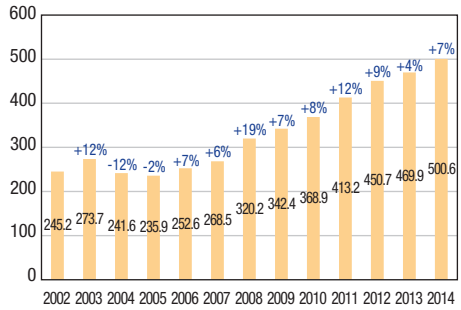



*Source: Observatory for Payment Card Security.*

**Chart 5**

**Amount of fraud in transactions handled by French schemes**

*(EUR millions)*

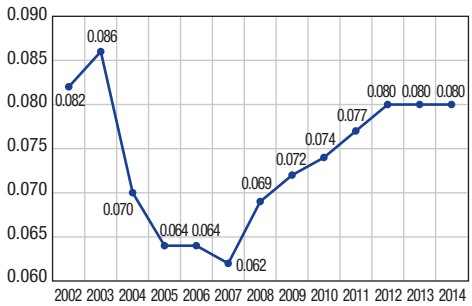



*Source: Observatory for Payment Card Security.*

**Chart 6**

**Fraud rate for transactions handled by French schemes (French and foreign cards)**

*(%)*




*Source: Observatory for Payment Card Security.*

## 2| Breakdown of fraud by card type

The fraud rate for four-party cards was unchanged at 0.080% in 2014. It has now been stable for two years, after rising for five years in a row. The fraud rate for three-party cards was 0.062% in 2014 compared with 0.065% in 2013, and declined for the third year running after previously increasing for four consecutive years.

The average value of a fraudulent transaction for four-party cards was EUR 112, compared with EUR 122 in 2013. For three-party cards, the average value of a fraudulent transaction was EUR 297, compared with EUR 352 in 2013.

**Table 1**

**Breakdown of fraud by card type**

*(% rate, amounts in EUR millions)*

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Four-party cards | 0.074 | 0.077 | 0.080 | 0.080 | **0.080** |
| | (351.5) | (394.9) | (434.4) | (455.8) | **(486.4)** |
| Three-party cards | 0.080 | 0.083 | 0.076 | 0.065 | **0.062** |
| | (17.4) | (18.3) | (16.3) | (14.0) | **(14.2)** |
| Total | 0.074 | 0.077 | 0.080 | 0.080 | **0.080** |
| | (368.9) | (413.2) | (450.7) | (469.9) | **(500.6)** |

*Source: Observatory for Payment Card Security.*

## 3| Geographical breakdown of fraud

**The amount of fraud in domestic transactions fell for the first time since the Observatory was set up.** It stood at EUR 234.6 million, giving a fraud rate of 0.043%, compared with EUR 238.6 million and a fraud rate of 0.046% in 2013.

Conversely, the amount of fraud in international transactions climbed by 15.0% compared with 2013 to reach EUR 266.0 million, considerably exceeding fraud in domestic transactions, whereas the two amounts have been close in the last three years. Although the fraud rate for international transactions fell sharply from 0.350% in 2013 to 0.316% in 2014, it remained more than seven times higher than the rate for domestic transactions.

**International transactions thus accounted for 53.1% of the total amount of fraud**, even though they made up just **13.5% of the total value of transactions**.

Within international transactions, fraud continues to be more limited for transactions inside SEPA than for transactions in non-SEPA countries:

- in the case of French cards, the fraud rate for transactions conducted outside SEPA (0.636%) was around twice as high as the rate for transactions conducted inside SEPA (0.374%);

- in the case of cards issued in countries other than France, the fraud rate for transactions carried out in France using foreign cards issued outside SEPA (0.336%) was two and a half times higher than the rate for cards issued within SEPA (0.134%).

Table 2

**Geographical breakdown of fraud**

*(% rate, amounts in EUR millions)*

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| **Domestic transactions** | **0.036** | **0.044** | **0.045** | **0.046** | **0.043** |
| | **(163.8)** | **(211.5)** | **(226.4)** | **(238.6)** | **(234.6)** |
| **International transactions** | **0.423** | **0.367** | **0.380** | **0.350** | **0.316** |
| | **(205.0)** | **(201.7)** | **(224.3)** | **(231.3)** | **(266.0)** |
| – o/w French card and non-SEPA acceptor | 0.728 | 0.638 | 0.759 | 0.688 | 0.636 |
| | (54.9) | (51.0) | (62.5) | (70.2) | (70.0) |
| – o/w French card and SEPA acceptor | 0.331 | 0.255 | 0.316 | 0.366 | 0.374 |
| | (50.6) | (44.3) | (56.3) | (67.9) | (91.0) |
| – o/w foreign non-SEPA card and French acceptor | 0.831 | 0.892 | 0.639 | 0.404 | 0.336 |
| | (64.5) | (81.3) | (78.2) | (64.1) | (65.6) |
| – o/w foreign SEPA card and French acceptor | 0.195 | 0.122 | 0.132 | 0.135 | 0.134 |
| | (35.0) | (25.1) | (27.3) | (29.1) | (39.3) |
| **Total** | **0.074** | **0.077** | **0.080** | **0.080** | **0.080** |
| | **(368.9)** | **(413.2)** | **(450.7)** | **(469.9)** | **(500.6)** |

*Source: Observatory for Payment Card Security.*

These results reward the efforts made over recent years in Europe, and to a lesser degree and more belatedly elsewhere in the world, to migrate cards and payment terminals to the EMV standard. In the case of France, they also reflect improved detection of attempted fraud originating outside SEPA and involving counterfeit magnetic stripes.

In this regard, it is worth highlighting measures announced by Visa, MasterCard, American Express and Discover (Diners Club International) to encourage international adoption of the EMV standard. With many countries introducing a shift in liability from the card issuer to the merchant in the event of fraud at points of sale that have not migrated to EMV, issuers will have a big incentive to swiftly adopt the standard for new cards while merchants will be encouraged to migrate their terminals. It is expected that, in the United States, around 500 million cards will migrate to the EMV standard over the course of 2015, or approximately half of the total.

## 4| Breakdown of fraud by transaction type

The Observatory's classification of card payment transactions distinguishes three types of transaction:

- face-to-face payments and unattended payment terminal (UPT) payments made at a point of sale (POS) or at fuel pumps, ticket, parking and other machines. This category includes contactless payments;

- CNP payments made on the internet, by post, telephone or fax;

- 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 0.010%**. These types of payments account for 66% of the value of domestic transactions but just 16% of the total amount of fraud;

- the **fraud rate for withdrawals edged up to 0.034%**. This mainly reflected the continued high number of attacks on automated teller machines (ATMs – over 1,000 in 2014) and POS (560 in 2014, or three times more than in 2013), which have become prime targets for organised fraud rings, and the continued high number of thefts of cards involving the capture of the PINs.

With these trends, which have been in place since 2011, still ongoing, the Observatory again reminds cardholders to be on their guard and

**Table 3**

**Breakdown of domestic fraud by transaction type**

*(% rate, amounts in EUR millions)*

| | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|
| Payments | 0.041 | 0.049 | 0.049 | 0.050 | 0.046 |
| | (137.3) | (177.8) | (190.0) | (199.9) | (193.0) |
| – o/w face-to-face and UPT | 0.012 | 0.015 | 0.015 | 0.013 | 0.010 |
| | (36.2) | (48.1) | (51.2) | (45.8) | (37.8) |
| – o/w CNP | 0.262 | 0.321 | 0.299 | 0.269 | 0.248 |
| | (101.1) | (129.6) | (138.8) | (154.2) | (155.9) |
| *– o/w by post/phone* | *0.231* | *0.259* | *0.338* | *1.122* | *0.147* |
| | *(27.3)* | *(25.4)* | *(29.4)* | *(29.2)* | *(2.8 a))* |
| *– o/w internet* | *0.276* | *0.341* | *0.290* | *0.229* | *0.251* |
| | *(73.9)* | *(104.2)* | *(109.4)* | *(125.0)* | *(153.0 a))* |
| Withdrawals | 0.024 | 0.029 | 0.031 | 0.033 | 0.034 |
| | (26.5) | (33.7) | (36.4) | (38.6) | (41.4) |
| **Total** | **0.036** | **0.044** | **0.045** | **0.046** | **0.043** |
| | **(163.8)** | **(211.5)** | **(226.4)** | **(238.6)** | **(234.6)** |

*a) The substantial decline relative to 2013 in the amount of fraud in CNP payments made by post or phone and the corresponding increase in the amount for internet payments are largely attributable to a change in the statistical methodology used by the "CB" Bank Card Consortium. The change involves the way in which fraud is distributed between internet and post/phone payments and does not affect the total amount of fraud or the overall fraud rate for CNP payments. A study by the consortium revealed that it was preferable to use internet payments to record fraud not classified by e-merchants, rather than post/phone payments, which used to be the default category. Similar measures had previously helped to improve data quality in 2013 (see the Observatory's 2013 Annual Report). The Observatory encourages all stakeholders to pursue efforts to improve the quality of the data reported to it.*

*Source: Observatory for Payment Card Security.*

reiterates the best practices to follow when making payments to a merchant or when making withdrawals (see Appendix 1).

- the **fraud rate for CNP payments declined** for the third year running, **falling to 0.248%**.

However, this was still 20 times higher than the rate for face-to-face payments.

As a result, **CNP payments accounted for just 11.6% of the value of domestic transactions but for 66.5% of the total amount of fraud**.

Given the level of fraud in CNP payments, the Observatory is repeating recommendations aimed at encouraging e-merchants, particularly those sustaining the greatest fraud, to deploy solutions such as 3D-Secure that enable strong authentication of cardholders for the most at-risk payments. The entry into force in summer 2015 of EBA guidelines on the security of internet payments will lend additional support to these recommendations (cf. Chapter 1 of this report).

In the case of international transactions (cf. Table 4), fraud in CNP payments to foreign e-merchants made using French cards surged in 2014 to EUR 104.5 million from EUR 81.2 million in 2013. One explanation for this may be that criminals have shifted their focus to target less well-protected foreign websites as online commerce sites in France have phased in solutions to protect internet payments.

Fraud rates for CNP payments were high both outside SEPA (0.960%) and inside SEPA (0.910%). The deployment of strong authentication solutions, spurred on by SecuRe Pay recommendations and EBA guidelines (see Chapter 1), should however help to turn this trend around in SEPA.

There was a further decline in fraud in face-to-face payments and withdrawals using French cards within SEPA, where EMV has now been extensively adopted. Notably, the fraud rate for withdrawals in SEPA (0.033%) is around 25 times lower than the rate for withdrawals outside SEPA (0.890%), as magnetic stripes continue to be widely used in certain countries.

## Table 4a

### Breakdown of international fraud by transaction type – French cards

*(% rate, amounts in EUR millions)*

| French card – Foreign non-SEPA acceptor | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|
| Payments | 0.561 | 0.687 | 0.547 | 0.532 |
| | (30.5) | (37.8) | (40.3) | (41.7) |
| – o/w face-to-face and UPT | 0.369 | 0.456 | 0.377 | 0.350 |
| | (16.0) | (19.8) | (17.7) | (19.2) |
| – o/w CNP | 1.320 | 1.551 | 0.848 | 0.960 |
| | (14.5) | (18.0) | (22.6) | (22.5) |
| *– o/w by post/phone* | *1.011* | *1.150* | *1.234* | *4.955* |
| | *(3.1)* | *(4.0)* | *(6.4)* | *(7.5)* |
| *– o/w internet* | *1.440* | *1.720* | *0.755* | *0.682* |
| | *(11.4)* | *(14.1)* | *(16.2)* | *(14.9)* |
| Withdrawals | 0.800 | 0.904 | 1.054 | 0.890 |
| | (20.5) | (24.7) | (29.9) | (28.3) |
| **Total** | **0.638** | **0.759** | **0.688** | **0.636** |
| | **(51.0)** | **(62.5)** | **(70.2)** | **(70.0)** |
| **French card – Foreign SEPA acceptor** | | | | |
| Payments | 0.300 | 0.372 | 0.434 | 0.434 |
| | (43.1) | (55.3) | (66.8) | (89.8) |
| – o/w face-to-face and UPT | 0.140 | 0.131 | 0.089 | 0.067 |
| | (12.6) | (11.7) | (8.2) | (7.8) |
| – o/w CNP | 0.571 | 0.735 | 0.937 | 0.910 |
| | (30.5) | (43.6) | (58.6) | (82.0) |
| *– o/w by post/phone* | *0.643* | *0.532* | *1.566* | *1.317* |
| | *(5.6)* | *(6.5)* | *(11.3)* | *(13.9)* |
| *– o/w internet* | *0.557* | *0.788* | *0.856* | *0.856* |
| | *(24.9)* | *(37.1)* | *(47.3)* | *(68.1)* |
| Withdrawals | 0.040 | 0.036 | 0.036 | 0.033 |
| | (1.2) | (1.1) | (1.1) | (1.2) |
| **Total** | **0.255** | **0.316** | **0.366** | **0.374** |
| | **(44.3)** | **(56.3)** | **(67.9)** | **(91.0)** |

*Source: Observatory for Payment Card Security.*

## Table 4b

### Breakdown of international fraud by transaction type – Foreign cards

*(% rate, amounts in EUR millions)*

| Foreign non-SEPA card – French acceptor | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|
| Payments | 1.056 | 0.735 | 0.451 | 0.380 |
| | (80.7) | (77.7) | (63.2) | (65.0) |
| – o/w face-to-face and UPT | – | 0.353 | 0.230 | 0.162 |
| | (–) | (30.3) | (25.3) | (21.9) |
| – o/w CNP | – | 2.378 | 1.268 | 1.213 |
| | (–) | (47.4) | (37.9) | (43.1) |
| *– o/w by post/phone* | – | *0.737* | *0.930* | *1.018* |
| | *(–)* | *(8.8)* | *(9.2)* | *(7.7)* |
| *– o/w internet* | – | *4.833* | *1.436* | *1.265* |
| | *(–)* | *(38.6)* | *(28.7)* | *(35.4)* |
| Withdrawals | 0.042 | 0.033 | 0.051 | 0.026 |
| | (0.6) | (0.6) | (0.9) | (0.6) |
| **Total** | **0.892** | **0.639** | **0.404** | **0.336** |
| | **(81.3)** | **(78.2)** | **(64.1)** | **(65.6)** |
| **Foreign SEPA card – French acceptor** | | | | |
| Payments | 0.155 | 0.158 | 0.158 | 0.156 |
| | (24.3) | (26.6) | (28.2) | (38.5) |
| – o/w face-to-face and UPT | – | 0.046 | 0.039 | 0.026 |
| | (–) | (5.7) | (4.9) | (5.1) |
| – o/w CNP | – | 0.466 | 0.458 | 0.476 |
| | (–) | (20.9) | (23.2) | (33.1) |
| *– o/w by post/phone* | – | *0.216* | *0.308* | *0.397* |
| | *(–)* | *(3.8)* | *(3.8)* | *(4.8)* |
| *– o/w internet* | – | *0.626* | *0.506* | *0.492* |
| | *(–)* | *(17.1)* | *(19.4)* | *(28.6)* |
| Withdrawals | 0.017 | 0.017 | 0.025 | 0.018 |
| | (0.8) | (0.7) | (0.9) | (0.9) |
| **Total** | **0.122** | **0.132** | **0.135** | **0.134** |
| | **(25.1)** | **(27.3)** | **(29.1)** | **(39.3)** |

*Source: Observatory for Payment Card Security.*

**Box 2**

### Payment fraud involving contactless cards

*For the first time this year, the Observatory gathered data to measure the fraud rate for contactless payments. Over 2014 as a whole, 72.2 million contactless payments were recorded, worth a total EUR 780.9 million, making an average of EUR 11 per transaction. Comprehensive data on fraud, meanwhile, have been collected since 1 April 2014. Over the last nine months of 2014, 9,600 fraudulent payments were recorded, worth a total EUR 108,000. The fraud rate for contactless transactions can thus be estimated at 0.015% during this period, putting it between the overall rate for face-to-face payments (0.010%) and the rate for withdrawals (0.034%).*

*Fraud in contactless payments is almost always due to theft or loss of the card. Contactless technology itself does not seem to have offered vulnerabilities for fraudsters to exploit (capturing card data by eavesdropping on a transaction, or remotely activating cards in public places, for example), which corroborates the risk analysis performed by the Observatory and published in its 2012 Annual Report. Furthermore, because card issuers have introduced ceilings for individual transactions (usually EUR 20 or EUR 25) or for total consecutive transactions that can be done without entering the PIN (typically EUR 100), the possible losses if a card is lost or stolen are limited.*

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

*As take-up increases, with more than 30 million cards with contactless payment capabilities in circulation at the end of December 2014, the Observatory calls on issuers to be vigilant and reminds them of their commitment regarding the ability to deactivate the contactless function. For these undertakings to be met, users must be provided with protective covers for their cards,[3] or it should be possible to switch off the contactless function remotely,[4] or cardholders must be able to ask to replace a contactless card with a non-contactless card.*

*As the overseer of cashless means of payment, the Banque de France supervises the implementation of these measures.*

1 *See Appendix 2.*
2 *See Appendix 1: a card payment in contactless mode is performed without using the card's personalised security features (no PIN entered), which means that even before reporting the card lost or stolen, the cardholder is not responsible for losses linked to unauthorised payments.*
3 *Protective covers block NFC radio waves, preventing the card from being activated unintentionally.*
4 *Here, the contactless function is deactivated by executing an EMV script on the card, which is done when the card is entered in an ATM or electronic payment terminal.*

## 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;
- 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.

**Box 3**

## Domestic fraud in 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 |
|---|---|---|
| Personal and professional services | 31.8 | 20.4 |
| Travel/transportation | 30.8 | 19.7 |
| General and semi-general trade | 29.5 | 18.9 |
| Telephony and communication | 26.7 | 17.1 |
| Household goods, furnishings, DIY | 12.7 | 8.2 |
| Technical and cultural products | 8.0 | 5.1 |
| Miscellaneous | 6.0 | 3.8 |
| Online gaming | 3.2 | 2.0 |
| Food | 2.6 | 1.7 |
| Account loading, person to person sales | 2.5 | 1.6 |
| Health and beauty | 1.8 | 1.1 |
| Insurance | 0.4 | 0.3 |
| **Total** | **155.9** | **100.0** |

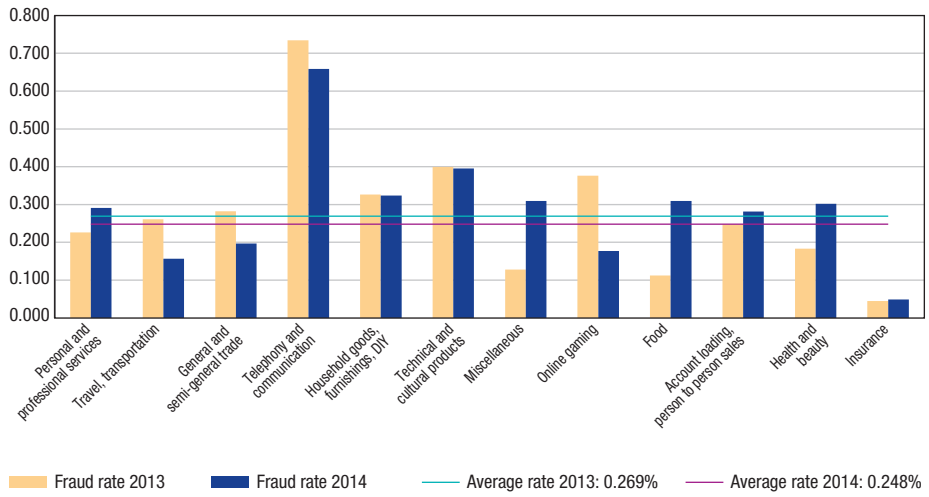
*The personal and professional services, travel/transportation, general and semi-general trade, and telephony and communication sectors were the most exposed to CNP fraud, accounting for 76% of the total amount. A comparison of average fraud rates for each sector sheds additional light, revealing that some sectors, including technical and cultural products, have considerable exposure despite accounting for a small portion of the total fraud amount.*

*Fraud rates are below the average in virtually all sectors with the notable exception of telephony and communication, which has persistently reported a higher-than-average fraud rate. The Observatory calls on firms in this sector in particular to step up fraud prevention measures.*

### Chart

**Domestic fraud rate in CNP payments, by sector of activity**

*(%)*

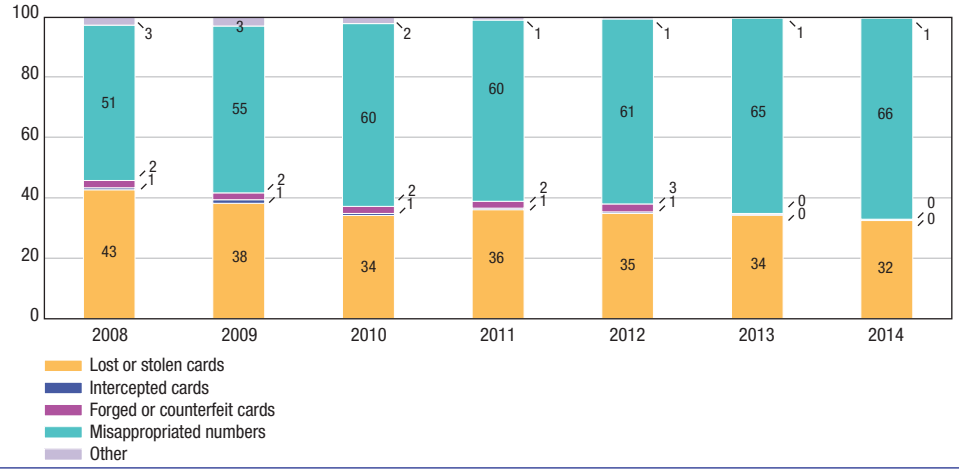



1 *Cf. Appendix 6 for sector descriptions.*

## Chart 7

### Breakdown by fraud type (domestic transactions, value)

*(%)*




*Source: Observatory for Payment Card Security.*

Chart 7 shows national fraud trends for all payment cards. The breakdown covers payments only (not withdrawals).

Fraud involving the use of misappropriated card numbers for CNP payments is the most common type of fraud, accounting for 66.4% of the total amount, a larger proportion than in 2013 (64.6%).

Fraud involving lost or stolen cards continued to account for around one-third of fraud in domestic payment transactions (32.5%) although its share, which stood at 34.2% in 2013, has been shrinking for three years.

Counterfeit cards accounted for just 0.1% of fraudulent domestic payments, a share that has been falling sharply in recent years (it was 2.6% in 2011). The decrease is mainly attributable to the adoption of smartcard technologies by a growing number of three-party card schemes and to enhanced security for existing EMV smartcards.[2]

## Table 5

### Breakdown of domestic fraud by fraud type and by type of card in 2014

*(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 | 76.3 | 32.5 | 75.6 | 32.8 | 0.7 | 17.3 |
| Intercepted cards | 0.9 | 0.4 | 0.5 | 0.2 | 0.4 | 9.6 |
| Forged or counterfeit cards | 0.2 | 0.1 | 0.1 | 0.1 | 0.1 | 1.5 |
| Misappropriated numbers | 155.9 | 66.4 | 154.3 | 66.9 | 1.6 | 40.0 |
| Other | 1.4 | 0.6 | 0.1 | 0.1 | 1.3 | 31.6 |
| Total | 234.6 | 100.0 | 230.6 | 100.0 | 4.0 | 100.0 |

*Source: Observatory for Payment Card Security.*

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

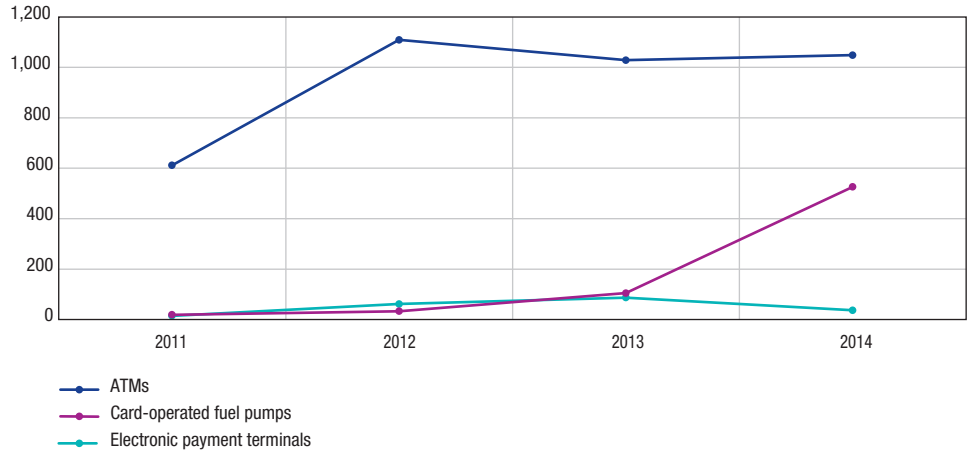
**Box 4**

## Indicators provided by law enforcement agencies

*In 2014, law enforcement agencies recorded another substantial decrease in arrests connected with bank card fraud, reporting 45 arrests, compared with 103 in 2013, 122 in 2012, and around 200 a year between 2011 and 2009. The decline reflects stiffer sentencing by the courts, which caused counterfeiting of foreign bank cards to fall sharply from end-2011 onwards.*

*ATM attacks were steady at 1,048 in 2014, compared with approximately 1,000 a year since 2012 and around 500 a year between 2011 and 2006, 200 in 2005 and just 80 in 2004. There were also 560 attacks on POS, compared with 188 in 2013, including 525 on card-operated fuel pumps and 35 on merchant payment terminals. These figures, which remain high for ATMs and are up sharply for fuel pumps, are evidence that crime rings are constantly seeking to gather card data, which they can use either to create counterfeit magnetic stripe cards for use in foreign payments and withdrawals, chiefly in countries where EMV technology is not widespread, or to misappropriate card numbers in CNP payments, particularly on websites that have not yet implemented strong cardholder authentication solutions.*

**Chart**
**Attacks on ATMs and terminals**



# Use of biometric techniques in payment card transactions

## 1| Background

Payment card transactions are largely protected by safeguarding the channel used to initiate payments, which is achieved through payer and payee authentication. While payee authentication relies on tried and tested solutions such as in-store terminals and digital certification for internet payments, payer authentication in card payment transactions, particularly when the card is not present but also in face-to-face settings, remains a major challenge. Accordingly, in January 2013 the European Forum on the Security of Retail Payments (SecuRe Pay) published a set of guidelines and best practices on the security of internet payments. These guidelines are consistent with positions adopted by the Observatory, especially as regards introducing strong cardholder authentication for the riskiest internet payments and for sensitive transactions generally (for example, when registering a card in an electronic wallet).

The SecuRe Pay guidelines define strong authentication[1] as *"a set of procedures based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:*

- *something only the user possesses, e.g. token, smartcard, mobile phone;*
- *something only the user knows, e.g. password, code, personal identification number;*
- *something the user is, e.g. a biometric characteristic.*

*In addition, the three elements 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)".*

Some biometric techniques that are already used routinely by more and more people could help to enhance the security of CNP and face-to-face payments and withdrawals. This study will seek to take stock of the use of these techniques in card payment transactions and withdrawals.

## 2| Biometrics: definition and application to payment cards

### 2|1 Definition

The French Data Privacy Agency (CNIL), whose chief task is to protect personal data, which include biometric data, defines biometrics as *"computer techniques that may be employed to automatically recognise an individual based on physical, biological, or behavioural characteristics. Biometric data are personal data because they may be used to identify an individual. Most of them, such as DNA or fingerprints, are particular in being both unique and permanent. They thus resemble what could be termed a 'universal unique identifier', and may be used to trace individuals".*[2]

In France, biometric recognition solutions must have prior authorisation from the CNIL. Specifically, to set up and operate such a system, an authorisation application or a compliance statement (depending on the processing objective and the type of biometric sample) needs to be filed with the CNIL. The latter option is not currently available for biometric techniques applied to payment instruments, however, as this use case is not covered by the CNIL's reference frameworks.

1 Also called strong customer authentication.
2 Cf. *http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/la-biometrie-sur-les-lieux-de-travail/* (in French).

**Box**

## The CNIL's view on biometric authentication

*Until now, the CNIL has authorised the use of biometrics as an authentication factor to access payment instruments or carry out remote transactions only on a trial basis. The purpose of the temporary authorisations granted in this context is to gauge customer interest in these solutions and assess the reliability of biometric technology when coupled with a payment instrument on the internet.*

*These trials expose problems, which are then used to identify avenues for improvement. They are restricted to the length of time needed to obtain conclusive results, and the CNIL requires detailed results to be submitted to it once tests are complete. Trials may be conducted only on a voluntary basis – under no circumstances may users be forced to use a biometric system.*

*The CNIL is working to develop guidelines for biometric solutions based on the trial results and the legislative landscape, which is changing both at home, with a bill under review that would restrict the use of biometric techniques, and at the European level, with the proposed data protection directive.*

*Although a reference framework has yet to be created for "retail" biometrics, i.e. excluding professional applications, a number of constant features can be picked out. The CNIL's positioning notably reflects its determination to ensure that biometrics is not made compulsory in day-to-day use and that people keep control over their biometric data.*

*Accordingly, the CNIL does not want biometrics to be the only way to access a service. Rather, it should be offered as an alternative to another method. Users must have the option of selecting another technique that is just as easy to use and can be accessed under the same terms as the biometric solution; opting for a different technology must not mean, for example, that additional restrictions are added, such as extra time or cost.*

*Furthermore, individuals unquestionably have less control over their biometric information if their biometric templates[1] are stored on remote servers rather than on media under their sole control. The compromise of an individually held medium would have far less serious consequences than that of a database holding multiple templates. For this reason, the CNIL would prefer biometric information to be stored on an individual medium under the sole control of the person in question.*

*In addition, the CNIL wants users to receive enhanced disclosures about the biometric solution used, including its optional nature and the existence of an alternative solution, and about data storage procedures. People should be able to change their choice whenever they want and have their biometric templates deleted if need be.*

*Many different parties could be involved in the biometric authentication processing chain, whether as suppliers or managers of template storage media or as providers of biometric authentication solutions. As a result, special attention is needed to clarify the distribution of responsibilities and to build in data protection rules from the service design stage onwards.*

*1 Set of biometric data used as a reference during authentication.*

The CNIL distinguishes three types of solution based on the physical or biological trait used:

• traceable biometrics include finger and palm prints. These are referred to as traceable because people involuntarily leave them behind on everything that they touch. The risk with such techniques is that these traces could potentially be captured and replicated without the knowledge of the person in question, e.g. by creating a false finger;

• traceless biometrics, which include hand geometry and finger vein pattern;

• intermediate biometrics, such as voice, iris or facial shape.

While this categorisation is still relevant, the latest capture methods and the voluntary and involuntary online proliferation of personal information, including high resolution photos and video recordings, can be used to reconstitute the biometric samples used in these solutions. This is blurring the boundaries between categories, as all approaches gradually become traceable.

When defining a biometric solution, it is necessary to distinguish between two types of use:

• identification: the biometric sample is compared against all biometric references to determine a person's identity;

• authentication: the identity of the rightful holder is already known and the biometric sample is compared only against the person's own biometric reference to check his or her identity.

In the area of payment card transactions, the holder is identified through presentation of the payment card or card data. The biometric solution is thus used to authenticate the holder.

## 2|2 Application to payment cards

A growing number of smartphone and laptop manufacturers are building in biometric recognition solutions, most of which are based on fingerprints (see the Observatory's 2013 Annual Report). Large-scale marketing of these new models has resulted in greater public familiarity with biometric techniques, creating an opportunity to deploy and use these technologies in the area of payments.

### 2|2|1 Using biometrics in card payments

In **CNP payments**, just over 30% of card payments are covered by strong cardholder authentication based on one-time passwords. In the case of new initiation methods such as mobile payments and electronic wallets, cardholder authentication typically relies on passwords. Although a password is more complex than a PIN and can be regularly updated, it is still reusable and is generally entered on standard computer or phone keypads that do not offer the same safeguards as the approved keypads on UPTs or payment terminals. Biometric techniques could provide an additional solution to enhance cardholder authentication.

Chip and PIN solutions offer a high level of security in **face-to-face payments**. The Observatory puts the fraud rate for this type of transaction at around 0.015% in recent years, or approximately 20 times less than the rate for CNP sales.

But PINs can still be reused: a fraudster who finds out a PIN during a withdrawal or payment either by compromising an ATM, terminal or UPT or simply by observing the number as it is entered, could reuse this information to commit fraud after stealing or counterfeiting the card. The keypads of ATMs, terminals and UPTs have to comply with authorisation rules that are intended to limit the threat of compromise. It is harder to stop a criminal from visually intercepting a PIN when it is entered, either by watching or by setting up a mini-camera. Cardholder vigilance is the best way to prevent this type of threat.

Biometric techniques could provide an additional solution that would lessen the risk in the event that the PIN is compromised, or offer an alternative in certain situations, so reducing PIN usage and hence the risk of compromise.

### 2|2|2 Limits of biometric solutions

Biometrics offers unquestionable practical benefits by simplifying and shortening the payment initiation procedure, or aiding people who struggle

to remember their PIN. Even so, the use of biometrics raises several specific issues:

• once a biometric sample is compromised, it is always compromised: if a biometric sample, such as a fingerprint, is compromised, a new one cannot usually be generated for the same physical feature. This contrasts with a physical medium, such as a smartcard or token, or a PIN, which can easily be renewed. Although there is the option of using a different finger, hand or eye, for example, the number of possibilities remains finite;

• there may be limits to the scope of biometric solutions. Some people may be temporarily unable to use their biometric characteristics because of wear, soiling or, injury, say. Others may never be able to use them, if, for example, their physical characteristics are incompatible with the solution or if they suffer from a disability;

• there are challenges involved in setting the tolerance level of biometric solutions, which will influence the error rate. Two rates are chiefly measured in biometrics: the false rejection rate (FRR) and the false acceptance rate (FAR), which reflect, respectively, the strictness and laxness of the solution with respect to the biometric sample that is captured and compared against the biometric reference. Accordingly, cuts, burns or even sweat can cause a fingerprint to be rejected, just as background noise can affect a voice analysis. These rates may vary to a greater or lesser extent depending on the physical trait being analysed, the quality of the biometric sensor and the algorithm used. The difficulty stems from the fact that while a tolerance level can be set, these two rates generally move in opposite directions. There are no public data on FRRs and FARs for the solutions currently on the market, which makes it hard to draw a comparison with a PIN-based approach. PINs have an FRR of close to zero (the correct number is never rejected and the keypads of payment terminals and ATMs are built to reduce the risk of mistyping), while the FAR is 3 in 10,000.[3]

In addition to the technical issues mentioned above, members of the public may feel reluctant to use biometric solutions for ethical reasons or because they do not trust the overall system, which could also slow the development of biometrics. Regarding the first concern, the use of biometric solutions is regulated by the CNIL, which ensures that the proposed solution has solid ethical grounds. As regards the second, the perceived robustness of biometric solutions in the eyes of the general public could be affected by current events, for example if new fraud techniques are discovered that do not put the reliability of the solutions into question but that get widespread media coverage (demonstrated under test conditions, for example). The success of a payment instrument lies as much in perceived as in actual security.

### 2|2|3 Existing standards

The current trials rely on proprietary solutions or pre-existing standards that generally come from the area of access control. Standards issued by the International Organization for Standardization (ISO)[4] notably cover the following aspects:

• detailed description of finger minutiae location, direction and type;

• conditions for taking photographs for face image data;

• biometrics application programming interfaces;

• common biometric exchange formats framework;

• compliance testing methodology and clarification of defects;

• biometric performance testing and reporting;

• testing of multimodal biometric implementations.

3 Assuming a four-digit PIN and three attempts allowed before the card is blocked.
4 Notably ISO/IEC 19784, 19785, 19794 and 19795.

However, these standards are mainly designed to ensure interoperability between the components, such as sensors and algorithms, that make up biometric solutions.

The first security evaluations, which began in 2008, used the Common Criteria to assess biometric solutions and sensors. However, just three products have so far obtained certification,[5] which, moreover is at an insufficient level for card payments.[6] A group of biometrics players formed the Biometrics Alliance Initiative (BAI) to establish a testing, certification and authorisation process that will ensure a level of security commensurate with international needs and standards, particularly in the banking field, along with associated testing procedures. The Biometrics Evaluation and Testing (BEAT) project, which is backed by the European Commission, is intended to establish an operational evaluation standard for biometric technologies.

EMV Co, which comprises the main card payment schemes (Visa, MasterCard, American Express, Discover, JCB and Union Pay), is exploring the use of biometric techniques as an alternative to PIN entry[7] within its Card and Terminal Working Group.

In France, the "CB" Bank Card Consortium is planning to incorporate biometrics in its authentication framework (available some time in 2015) and to establish possible use cases based on the intrinsic level of resistance to attacks measured during security evaluations.

Furthermore, several stakeholders from the payments sector came together in 2013 to form the Natural Security Alliance, which works to promote the use of biometrics and develop standards in the area.

# 3| Stock-taking of biometric solutions used in card payment transactions

## 3|1 Preliminary stages before implementation of a biometric solution

Before a biometric solution can be used to access a service, several stages common to all types of biometrics must be followed.

### 3|1|1 User enrolment

Every user has to follow a procedure whereby a biometric reference is captured and subsequently used to recognise the user. In the case of a fingerprint-based solution, for example, this stage would consist in taking an initial set of fingerprints, which could include multiple prints[8] to promote high quality.

This stage may be performed in a secure and controlled environment such as a bank branch, in a non-specialised environment, or in a personal device such as the user's smartphone.

### 3|1|2 Storage of users' biometric reference data

Biometric reference data are stored so that the system can compare them against the sample that is presented.

Storage may be done at a central location that holds the biometric reference data of all service users or it may be done locally on a device specific to each user, such as the chip of a payment card, a mobile phone or a secure token.

5 Cf. *http://www.ssi.gouv.fr/administration/glossaire/c/* (in French).
6 The protection profile implemented offers the EAL 2 security level (basic resistance to attacks) whereas EAL 4+ (high resistance to attacks) is required for card payment schemes.
7 Note that Visa, MasterCard and Discover are also members of the Fast IDentity Online (FIDO) Alliance, an industrial consortium set up in February 2013 that is developing specifications to simplify and strengthen authentication in online transactions and develop a viable alternative to passwords.
8 Several fingers may be used and several prints taken for each finger.

**Box**

## Example of a fingerprint recognition solution applied to card payments

### User enrolment and registration of biometric references

| | Case 1 – Registration on local device held by user, such as a smartphone | Case 2 – Registration on remote server based in a commercial branch |
|---|---|---|
| 1) Entry into relationship | User installs dedicated app or connects to dedicated web service  | User visits branch  |
| 2) User identification | User enters service-related information (user and card information) | User provides information/supporting documentation (contract, ID) |
| 3) Biometric reference taken |  |  |
| 4) Reference registered | Locally  | On remote server  |

Secure local storage of biometric reference data is generally preferred because it reduces the risk of massive compromise of reference data in the event of an intrusion in the central storage facility. However, some kinds of biometric techniques, such as voice biometrics, may require computing power that current portable devices such as smartphones cannot yet provide, making central processing necessary.

#### 3|1|3 Service access based on biometric solution used

Service access entails a preliminary identification step, which is similar to that used with a "traditional" payment solution, i.e. insertion of the card in a terminal, presentation at an NFC point, entry of identifier or card number, etc. The biometric sample is then read and may either replace the usual authentication method, such as PIN/password entry or 3D-Secure authentication, or supplement it. In the last stage, the sample is compared against the biometric reference data, which requires the payment solution to access a storage medium either through a local connection or online, depending on the storage method used.

### 3|2 Potential contribution of biometric authentication relative to existing solutions

A biometric solution may be introduced to enhance an existing authentication system either by supplementing it, i.e. adding an extra check to the holder authentication process (for example by

**User authentication in face-to-face payment**
(example without PIN entry)


adding fingerprint recognition to password/PIN entry), or by providing an alternative method, i.e. replacing the existing authentication solution (for example, entry of the biometric instead of a PIN).

When **used as a supplement**, biometric authentication can increase the overall level of security of an existing solution by making it harder to initiate fraudulent payments. For example, biometrics can help to improve the security of low-value contactless payments for which a PIN does not have to be entered, without materially affecting the speed of the payment initiation process. The level of security offered in this case will inevitably be higher than that of the initial system. However, the risk that biometric samples could be compromised, which is inherent to any biometric solution, creates an additional risk that must be taken into consideration. Biometric authentication could also be used to supplement PIN entry to make payments more secure, for example in the case of large-value transactions that a risk analysis has identified as most at-risk.

When **biometrics is used as an alternative**, the replacement of an existing authentication factor with biometric recognition could also improve the security of card payments by lowering the risk of compromise of the replaced solution. For example, using biometric authentication instead of card PIN entry could reduce the risk of PIN compromise in some cases (card-operated fuel pumps, for example). Here, the security level offered is primarily based

on that of the biometric solution and does not benefit from the protective mechanisms provided by the replaced solution (PIN, 3D-Secure, etc.).

## 3|3 Application to CNP payments

The most advanced trials of biometric solutions in CNP payments are based on voice or fingerprint recognition. These trials employ users' phones to add a holder authentication phase to make remote transactions safer.

TalkToPay in France and VoicePay in the UK, for example, offer a strong authentication service that is based on enrolment of a landline or mobile phone in the system and customer voice recognition. When making a remote payment, the user is called and must authenticate him or herself. This type of solution, which is solely based on voice telephony, has the advantage of working with all types of fixed-line and mobile phones.

Fingerprint-based solutions seek to harness the print reading features that some smartphone manufacturers have now built into their models, primarily to safeguard device access, but also to enable use by additional services. The PayPal app available on Samsung Galaxy S5 models, for example, allows users to make payments from an electronic money account by authenticating themselves with their fingerprints. Similarly, the Apple Pay solution offered in the USA on the latest Apple iPhones enables users to agree to online card purchases. In these cases, reading the fingerprint generally replaces entry of a password.

## 3|4 Application to face-to-face payments

Because face-to-face payments already enjoy a high level of security, biometric techniques are sought after because they are quick and convenient. They enable large companies to enrol their customers and have them make payments through a simple biometric reading, which subsequently activates payment using a card or another pre-registered means of payment. In this case, biometrics acts as an alternative to customary PIN-based authentication methods, offering a way to get through the checkout process more quickly and easily. For this type of application, electronic payment terminals fitted with the technology must be provided, and merchants need to be trained in using the equipment.

Trials in this area have chiefly been based on fingerprint recognition:

- some harness functionalities built into the latest generation of smartphones, which are fitted with fingerprint sensors. Here, the payment terminal interacts with the smartphone, in which the payment card's reference information has already been pre-enrolled. The connection to the terminal can be established through a local wireless network (NFC or Bluetooth for example). Under this approach, validation is carried out using the smartphone through recognition of the customer's fingerprint, potentially in conjunction with other authentication solutions such as PIN/password entry. This is what Apple Pay, among others, currently offers. With this type of solution, the same process could potentially be used to enhance the security of low-value contactless payments (compared with a standard NFC card, since the biometric reading adds an additional level of security) and replace PIN entry for larger-value payments up to the limits set by the issuer based on a risk analysis;

- one uses a card featuring an integrated fingerprint sensor: in October 2014 MasterCard announced the launch of MasterCard Zwipe, a contactless NFC card with a fingerprint sensor whose use replaces PIN entry. This EMV-compliant payment card also has a chip and can require PIN entry. It has not yet been released in France;

- another involves merchant equipment fitted with a fingerprint or finger vein sensor: in France, Natural Security Alliance has teamed up with several major retailers to run a trial since October 2012 that uses authentication based on reading this type of biometric information as a replacement for PIN entry. The payment terminal is fitted with a module that senses the fingerprint or the finger veins of the customer and compares this information against what is stored on the card.

Techniques based on other physical or biological characteristics, such as facial recognition, may also be tested in the near future. In January 2015, Toshiba,

a manufacturer, unveiled its Toshiba Touchless Commerce automated checkout concept, which features a camera to enable facial recognition of pre-enrolled customers; however, this solution has not yet been piloted.

### 3|5 Application to withdrawals

Withdrawals benefit from generally better supervised environments, especially if ATMs are located inside branches.

Several manufacturers already offer ATMs fitted with biometric sensors, which typically provide a substitute for PIN entry. However, there are no registered trials of this type of system going on in France. Two types of biometric solution share the market:

- finger or palm vein recognition, which is a commonly used authentication method with Japanese ATMs. This type of approach has also been introduced on a widespread basis in Brazil and Turkey;

- iris recognition has also been trialled on ATMs in several US states.

For this type of application, ATMs fitted with the technology must be provided, and holders and branch personnel need to be trained in using the equipment.

## 4| Conclusion

The use of biometric techniques in payment card transactions is governed in France by the Data Privacy Act. Before payment solutions using biometrics can be offered, an authorisation application must be filed with the CNIL, which sets the guidelines applicable in this area.

The Observatory has noted that the trials currently being conducted in France seek primarily to test the user-friendliness of proposed biometric solutions and to gauge the level of public interest. Prior to large-scale deployment, the Observatory stresses the need to analyse the risks created in situations where biometric authentication is used, in order to ensure that solutions provide payment transactions with a level of protection that is at least on par with current practice in the area (i.e. PIN and smartcard for face-to-face payments, one-time password for CNP payments).

In this regard, the Observatory notes that the level of security offered by current biometric solutions is hard to measure because there are no evaluation standards equivalent to those that exist for proven technologies, such as smartcards and mobile phone SIM cards. Accordingly, the Observatory emphasises the need to quickly set standards that can be used to assess the security level of these new solutions based on evaluations that encompass all the components employed by the solutions, including hardware, algorithms and planned use cases.

Firms should take care not to engage in widespread deployment of biometric authentication solutions with an overly low security level that could result in the biometric characteristics of a large number of users becoming compromised. This could threaten the introduction of future solutions that offer better security but rely on the same potentially compromised biometric characteristics.

In view of the inherent limitations of biometrics and the immaturity of security evaluations for these solutions, the Observatory continues to recommend maintaining an alternative authentication solution that can replace the biometric solution if it is no longer able to offer the requisite service and security levels.

# Towards retail payments 2.0: the new security challenges

## Summary of the conference organised on 22 October 2014 by the Banque de France and the European Central Bank

On 22 October 2014, the Banque de France teamed up with the European Central Bank (ECB) to organise an international conference in Paris on new security challenges for payment instruments.

The day-long event provided an opportunity to present institutional changes within Europe in the area of payment security, talk about possible ways to enhance mobile and internet payments, and explore the security consequences of using third party payment providers.

### 1| The emergence of new security challenges

In his opening address, Banque de France Governor Christian Noyer pointed out that while new payment methods need to be developed to cater to new consumer behaviours, they also raise security risks that must be kept in check.

Referring notably to experience garnered by the Observatory in the area of card payments, the Governor emphasised the factors that will ensure the success of new payment methods:

- new payment solutions will be more widely used if consumers see them as safe. Consequently, innovative payment services providers (PSPs) have an inherent interest in investing in fraud prevention;

- payment chain participants need to work together to achieve sustainable results. Bodies such as the Observatory can play a major part in preventing fraud over the long run;

- as fraud rings become increasingly international, it is vital to improve coordination by national and European authorities in charge of maintaining the security of means of payment. The decisive contribution of SecuRe Pay over the last three years shows how significant progress can be made when all authorities work together.

Benoît Cœuré, a member of the Executive Board of the ECB, presented the history of the SecuRe Pay forum and the reasons for its creation. Set up in early 2011 in response to rising fraud in CNP payments, the forum, which was initially led by the ECB, brings together prudential supervisors and overseers (central banks) of PSPs from EU member countries. Co-chaired since October 2014 by the ECB and the European Banking Authority (EBA), SecuRe Pay seeks to promote dialogue between national and European authorities with a view to determining common security requirements for payment instruments. The forum has published three sets of recommendations so far.[1] These technology-neutral recommendations and guidelines require PSPs to conduct comprehensive assessments of risks linked to internet payments and to strengthen their security by adopting strong user authentication solutions. Special attention is also devoted to protecting sensitive payment data and raising user awareness to prevent fraud more effectively.

1 The recommendations for the security of mobile payments and those on payment account access services are being used in the current revision of the Payment Services Directive; the recommendations on the security of internet payments were taken up by the Eurosystem for its oversight frameworks and by the EBA as guidelines that were published in December 2014 and become effective on 1 August 2015.

**Box**

## Conference programme, 22 October 2014

Opening address
*Christian Noyer (Governor, Banque de France)*

Opening remarks
*Benoît Coeuré (Member of the Executive Board, European Central Bank)*

### Topic I: Cooperation by European authorities on the security of retail payment instruments

Panel discussion
*Moderator: Pierre Petit (Co-Chair, SecuRe Pay forum)*
*Mario Nava (Director for Financial Institutions, European Commission)*
*Adam Farkas (Executive Director, European Banking Authority)*

### Topic II: Security expectations for payment instruments

Panel discussion on mobile payments
*Moderator: Hanna Franiak (Advisor in Payment Systems Department, Narodowy Bank Polski)*
*Pierre Chassigneux (Chief Risk and Audit Officer, Groupement des Cartes Bancaires)*
*Rob Marrewijk (Terminal Security Program Manager, Brightsight)*
*Santiago Minguito Santos (Director of Information Security, Banco Sabadell)*
*Edwin Aoki (Technology Fellow and Chief Architect, PayPal)*

Opening remarks
*Adam Farkas (Executive Director, European Banking Authority)*

Panel discussion on internet payments
*Moderator: Dirk Haubrich (Head of Consumer Protection Unit, European Banking Authority)*
*Dirk Schrade (Deputy Head of Payment and Settlement Systems Department, Deutsche Bundesbank)*
*Ingrid Lauterbach (Head of Client Security, Cyber-Security Group, Deutsche Bank)*
*Paul Alfing (Chair, E-Payments Committee)*
*Monique Goyens (Director General, The European Consumer Organisation)*

### Topic III: Regulating third party service providers

Opening remarks
*Mario Nava (Director for Financial Institutions, European Commission)*

Panel discussion on third party payment providers
*Moderator: Denis Beau (Director General Operations, Banque de France)*
*Pierre Petit (Co-Chair, SecuRe Pay forum)*
*Irmfried Schwimann (Director of Financial Services, European Commission)*
*Massimo Doria (Head of Payment Instruments and Services Division, Banca d'Italia)*
*Jean Clamon (Managing Director, BNP Paribas)*
*Georg Schardt (Deputy CEO, SOFORT AG)*

Closing remarks
*Denis Beau (Director General Operations, Banque de France)*

## 2| Cooperation by European authorities to ensure the security of payment instruments

The first session provided an opportunity to review the responsibilities of the European institutions and their cooperation in executing the tasks appointed to them.

The mandate given to the Eurosystem and the ECB with respect to payment instruments stems from provisions in the founding treaties and the statute of the European System of Central Banks on promoting the smooth operation of payment systems. The ECB and the Eurosystem pursue two objectives in this regard: maintaining user confidence in the currency and preventing further fragmentation of the European payments market. To achieve these goals, the ECB and the Eurosystem's national central banks act as catalysts to market initiatives that contribute to the greater integration of European payment services. They also directly oversee the security of payment instruments of common interest to all euro area countries. To this end, the Eurosystem has published oversight frameworks for payment cards (January 2008), and for direct debits and credit transfers (October 2008). Assessment guides are available for each of these three oversight frameworks.

The European Commission seeks to uphold the interests of European citizens, particularly by establishing the legal framework needed for the emergence of a safe, effective and competitive European payments market.

Since the European supervisory authorities were established, the European Commission has increasingly adopted a two-tier approach to preparing legislative proposals, by writing the overarching principles directly into the legislation while leaving the new European regulatory authorities to determine common standards and practices necessary for the consistent application of these principles.

This approach is being adopted for the revision of the Payment Services Directive (PSD2). The EBA, in close collaboration with the ECB, has been entrusted with establishing technical standards for certain provisions of the directive, such as those that deal with the requirements for operational and security risks, including strong authentication for users of payment instruments and transactions.

The EBA has two types of regulatory instrument at its disposal:

- regulatory technical standards (RTS), which apply directly in Member States once approved by the European Commission;

- guidelines and recommendations, which have to be transposed nationally by Member States' supervisory authorities, with the EBA monitoring their proper application.

As part of the PSD2 revision, work on preparing RTS, guidelines and recommendations will be taken forward within SecuRe Pay, which is now co-chaired by the ECB and the EBA.

## 3| Security expectations for new payment instruments

### 3|1 Security of payments by mobile phone

The session on payments by mobile phone sought to provide an insight into developments and security challenges linked to this emerging payment approach.

The wide distribution of mobile phones – some two billion smartphones are thought to be in use around the world, i.e. almost on par with the number of EMV-compliant payment cards – has seen these devices emerge as key payment instruments. The session stressed the diverse range of uses, as mobile phones can employ a broad array of mechanisms to make payments, including NFC contactless payments using card data stored on a SIM card or on a secure element, host card emulation,[2] QR[3] codes, phone

2 Software architecture enabling a connected object, such as a smartphone or watch, with an NFC chip to be recognised as a payment card.
3 Quick Response.

number-based methods, electronic wallets and virtual payment cards.

The growing availability and diversity of these new methods make it necessary to review the conventional classification of payments. Mobile payments sometimes blur the boundaries between face-to-face and CNP payments, since, for example, some in-store transactions by mobile phone may be approved via an internet connection.

This presents new security challenges. Given that the fraud rate for CNP payments is far higher than that of face-to-face payments, bringing these two payment environments together must not lead to lower overall security requirements and higher fraud rates, particularly in the face-to-face setting. Those working in the field need to provide mobile payments with the same level of security as that currently enjoyed by face-to-face payments using EMV-compliant smartcards.

In this area, the first security challenge is to identify the threats. These can be grouped into three categories:

- threats to phone operating systems, which could for example be infected by malware;
- threats to the communication channels used in mobile phone payments (attacks on Wi-Fi, NFC or Bluetooth wireless transmissions);
- threats of physical attacks on phone components.

Given this situation, at least four avenues of discussion could be useful in enhancing the security of payments by mobile phone.

First, providers of operating systems need to be involved in work on the security of mobile phone payments, to promote better protection for device operating systems.

Next, efforts should be made to promote more research into safeguarding the physical architecture of mobile phones.

Third, amid growing use of cloud computing, the question of protecting remotely stored data needs to be revisited with a view to enhancing security.

Fourth, the accent needs to be placed on new authentication methods, such as biometrics,[4] and on techniques such as tokenisation[5] that protect payment data circulating on networks.

## 3|2 Security of internet payments

This session was used to present the content and implementing procedures of EBA guidelines on the security of internet payments. The EBA published its final guidelines on 19 December 2014 and they come into force on 1 August 2015.

The guidelines take up, with a few minor adjustments, the recommendations issued by SecuRe Pay on the same subject on 31 January 2013. Like SecuRe Pay's recommendations, the guidelines address different aspects of the security of internet payments:

- the overall oversight and security environment (governance, risk assessment and mitigation, incident monitoring and reporting, traceability);
- specific oversight and security measures for internet payments (authentication, transaction monitoring, protection of sensitive data, setting of payment limits and disclosure to customers of transaction information);
- customer awareness and procedures for communication between the customer and PSP.

It was recalled that these guidelines were partly adopted in response to the surge in the fraud rate for CNP payments that has accompanied the soaring rise of online commerce of recent years. In 2012, European data showed that this type of fraud accounted for 60% of total fraud in card payments and had been steadily rising since 2008. Strong customer authentication in internet payments should help to counter this trend.

4 See the study in this report by the Observatory as part of its technology watch.
5 In the electronic payments sector, tokenisation is the process of substituting bank data (card number, etc.) by one-time data that create a secure token. This makes it possible to reduce the transmission of sensitive data on communication channels.

While participants in the panel discussion agreed on the need to strengthen the security of internet payments to maintain consumer trust in the security of the payment instruments made available to them, some also stressed the need to maintain the user-friendliness of these instruments and to ensure that the new security solutions are not a source of added complexity for users.

## 3|3 Security challenges linked to the emergence of third party payment providers

The proposed PSD2 revision provides for the creation of two new payment services, which are designed to enable a third party operator to access payment accounts held by PSPs to: (i) initiate payments, e.g. pay an online merchant by credit transfer, or (ii) consolidate information, e.g. show the balance of the accounts held by one person with multiple institutions on a single web page.

A small number of firms in Europe, notably in Germany and the Netherlands, currently perform these activities, particularly initiation services, without being subject to any legal framework. As the regulations stand, these activities pose a fraud risk insofar as they require users to share login information and access codes for their online bank accounts with a third party.

From a security perspective, these new participants have to be regulated to ensure that users' bank data are kept safe. Accordingly, the new directive is expected to make changes so that a legal framework can be established for these firms. It will also introduce provisions covering the security of exchanged and stored data, and the security of communications between account-servicing PSPs, third party payment providers and consumers.

# Appendices

# 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 the 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.

## 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.

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

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 R141-1, R141-2 and R142-22 to R142-27 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 L132-1 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 L521-1 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 *Autorité de contrôle prudentiel et de résolution* (ACPR – Prudential Supervisory and Resolution Authority). 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 L521-1 of the *Monetary and Financial Code*, assimilated entities include the Banque de France, the *Institut d'émission des départements d'outre-mer* (French overseas departments note-issuing bank), 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 L511-7, Article L525-6 and section II of Article L521-3 of the *Monetary and Financial Code*.

4 These cards are exempt from the need for an approval, under section II of Article L511-7, Article L525-5 and section I of Article L521-3 of the *Monetary and Financial Code*.

5 Under the terms of section I of Article L314-1 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 acceptance 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 L315-1 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 L311-3 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 L141-4 and R141-1 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 R141-2 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 R142-22 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 ACPR 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 ACPR, 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 R142-23 *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 provided by the Banque de France, is responsible for organising and following up on 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 R142-25 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 R142-22 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 ACPR, are appointed for a three-year term by order of the Minister of the Economy, Industrial Renewal and Digital Technology. The most recent appointment order was issued on 19 December 2014.

### 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 ACPR

**Olivier PRATO**
General Secretariat

### Representatives of general government

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

- The Director General of the National Agency for the Security of Information Systems or his/her representative:
  **José ARAUJO**
  **Vincent STRUBEL**

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

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

- The Head of the Treasury or his/her representative:
  **Isabelle BUI**

- The Director General for Enterprises or his/her representative:
  **Loïc DUFLOT**

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

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  **Vincent FILHOL**

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**
  **Sylvain BRUN**

Nominated on proposition by the Minister of Defence:

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

### Representatives of payment card issuers

**Frédéric COLLARDEAU**
Head of Payments
La Banque Postale
**Gilbert ARIRA**
Director
"CB" Bank Card Consortium
**Jean DIACONO**
Director
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

**Éric 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 French cards in circulation in 2014:** 85.6 million
- 71.0 million four-party cards ("CB", MasterCard, Visa and Moneo);
- 14.6 million three-party cards.

**Number of cards reported lost or stolen[1] in 2014:** around 905,600

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

In international transactions, a distinction has been drawn since 2010 between transactions within SEPA and those involving an issuer or an accepting merchant elsewhere in the world. As a result, there are now four types of international transactions: French issuer/foreign SEPA acceptor, French issuer/foreign non-SEPA acceptor, foreign SEPA issuer/French acceptor, foreign non-SEPA 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 2014 – Issuance

*(volume in millions; value in EUR billions)*

| | French issuer, French acceptor | | French issuer, Foreign SEPA acceptor | | French issuer, Foreign non-SEPA acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Four-party cards | | | | | | |
| Face-to-face payments and UPT | 8,148.87 | 344.31 | 163.38 | 10.70 | 46.99 | 4.38 |
| CNP payments excluding internet | 14.29 | 1.85 | 17.11 | 1.06 | 2.04 | 0.15 |
| CNP internet payments | 781.70 | 58.58 | 155.17 | 7.50 | 30.76 | 1.99 |
| Withdrawals | 1,512.18 | 121.39 | 29.85 | 3.61 | 20.96 | 3.18 |
| **Total** | **10,457.05** | **526.14** | **365.51** | **22.87** | **100.75** | **9.70** |
| Three-party cards | | | | | | |
| Face-to-face payments and UPT | 103.57 | 11.73 | 7.52 | 0.97 | 6.24 | 1.11 |
| CNP payments excluding internet | 1.13 | 0.07 | – | – | – | – |
| CNP internet payments | 17.58 | 2.40 | 3.70 | 0.46 | 1.28 | 0.20 |
| Withdrawals | 3.28 | 0.30 | – | – | – | – |
| **Total** | **125.56** | **14.49** | **11.22** | **1.43** | **7.51** | **1.31** |
| **Grand total** | **10,582.61** | **540.63** | **376.73** | **24.30** | **108.27** | **11.01** |

*Source: Observatory for Payment Card Security.*

## Table 2

### The payment card market in France in 2014 – Acceptance

*(volume in millions; value in EUR billions)*

| | French issuer, French acceptor | | Foreign SEPA issuer, French acceptor | | Foreign non-SEPA issuer, French acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Four-party cards | | | | | | |
| Face-to-face payments and UPT | 8,148.87 | 344.31 | 217.66 | 16.51 | 68.51 | 9.50 |
| CNP payments excluding internet | 14.29 | 1.85 | 5.61 | 1.20 | 1.62 | 0.76 |
| CNP internet payments | 781.70 | 58.58 | 43.87 | 5.64 | 13.20 | 2.61 |
| Withdrawals | 1,512.18 | 121.39 | 26.68 | 4.86 | 8.87 | 2.19 |
| **Total** | **10,457.05** | **526.14** | **293.82** | **28.20** | **92.20** | **15.06** |
| Three-party cards | | | | | | |
| Face-to-face payments and UPT | 103.57 | 11.73 | 4.31 | 1.10 | 7.03 | 4.03 |
| CNP payments excluding internet | 1.13 | 0.07 | – | – | – | – |
| CNP internet payments | 17.58 | 2.40 | 0.88 | 0.16 | 0.53 | 0.19 |
| Withdrawals | 3.28 | 0.30 | – | – | 0.44 | 0.23 |
| **Total** | **125.56** | **14.49** | **5.19** | **1.26** | **8.00** | **4.45** |
| **Grand total** | **10,582.61** | **540.63** | **299.02** | **29.46** | **100.20** | **19.51** |

*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 2014 – Issuance

*(volume in thousands; value in EUR thousands)*

| | French issuer, French acceptor | | French issuer, Foreign SEPA acceptor | | French issuer, Foreign non-SEPA acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Face-to-face payments and UPT | 469.7 | 35,077.6 | 63.7 | 7,182.8 | 106.5 | 17,879.5 |
| Lost or stolen cards | 457.5 | 34,590.8 | 47.3 | 4,135.1 | 17.6 | 3,840.4 |
| Intercepted cards | 5.7 | 309.8 | 0.3 | 32.2 | 0.1 | 7.3 |
| Forged or counterfeit cards | 5.3 | 99.9 | 7.1 | 1,287.8 | 75.2 | 11,674.9 |
| Misappropriated numbers | 0.2 | 33.1 | 7.2 | 1,371.5 | 11.3 | 2,008.1 |
| Other | 0.9 | 44.1 | 1.7 | 356.2 | 2.4 | 348.7 |
| CNP payments excluding internet | 18.2 | 2,579.9 | 141.3 | 13,896.5 | 37.5 | 7,535.7 |
| Lost or stolen cards | 0.1 | 8.3 | 16.5 | 1,841.1 | 6.3 | 1,285.8 |
| Intercepted cards | 0.0 | 0.0 | 0.1 | 5.1 | 0.0 | 1.1 |
| Forged or counterfeit cards | 0.0 | 1.3 | 3.1 | 519.4 | 2.0 | 599.5 |
| Misappropriated numbers | 18.0 | 2,569.6 | 121.2 | 11,498.8 | 29.0 | 5,632.4 |
| Other | 0.0 | 0.7 | 0.4 | 32.1 | 0.2 | 17.0 |
| CNP internet payments | 1,355.4 | 151,716.4 | 1,276.3 | 67,142.8 | 136.4 | 14,515.6 |
| Lost or stolen cards | 0.3 | 21.6 | 123.9 | 7,288.6 | 14.8 | 1,712.5 |
| Intercepted cards | 0.0 | 0.0 | 0.4 | 11.6 | 0.1 | 4.1 |
| Forged or counterfeit cards | 0.1 | 11.2 | 34.1 | 2,077.1 | 5.2 | 521.1 |
| Misappropriated numbers | 1,355.0 | 151,677.2 | 1,115.8 | 57,624.5 | 115.8 | 12,230.6 |
| Other | 0.0 | 6.4 | 2.1 | 141.0 | 0.5 | 47.4 |
| Withdrawals | 139.5 | 41,252.8 | 5.4 | 1,174.0 | 179.7 | 28,315.0 |
| Lost or stolen cards | 137.9 | 40,931.6 | 3.7 | 853.3 | 9.7 | 1,564.6 |
| Intercepted cards | 0.6 | 205.8 | 0.0 | 5.2 | 0.0 | 5.6 |
| Forged or counterfeit cards | 0.1 | 15.3 | 1.5 | 273.9 | 164.4 | 25,883.5 |
| Misappropriated numbers | 0.0 | 4.0 | 0.0 | 9.9 | 1.4 | 191.2 |
| Other | 0.8 | 96.0 | 0.2 | 31.7 | 4.2 | 670.0 |
| **Total** | **1,982.8** | **230,626.7** | **1,486.7** | **89,396.1** | **460.1** | **68,245.8** |

*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 2014 – Acceptance

*(volume in thousands; value in EUR thousands)*

| | French issuer, French acceptor | | Foreign SEPA issuer, French acceptor | | Foreign non-SEPA issuer, French acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Face-to-face payments and UPT | 469.7 | 35,077.6 | 62.9 | 5,048.0 | 98.6 | 18,801.4 |
| Lost or stolen cards | 457.5 | 34,590.8 | 39.6 | 2,439.4 | 15.6 | 3,598.1 |
| Intercepted cards | 5.7 | 309.8 | 1.4 | 73.1 | 0.3 | 78.8 |
| Forged or counterfeit cards | 5.3 | 99.9 | 10.1 | 643.7 | 71.5 | 12,118.7 |
| Misappropriated numbers | 0.2 | 33.1 | 10.5 | 1,694.1 | 10.6 | 2,808.7 |
| Other | 0.9 | 44.1 | 1.3 | 197.7 | 0.6 | 197.2 |
| CNP payments excluding internet | 18.2 | 2,579.9 | 18.0 | 4,743.7 | 19.0 | 7,694.0 |
| Lost or stolen cards | 0.1 | 8.3 | 1.9 | 157.8 | 0.9 | 465.3 |
| Intercepted cards | 0.0 | 0.0 | 0.0 | 2.4 | 0.0 | 9.2 |
| Forged or counterfeit cards | 0.0 | 1.3 | 1.5 | 414.4 | 1.5 | 698.5 |
| Misappropriated numbers | 18.0 | 2,569.6 | 14.4 | 4,138.7 | 16.5 | 6,472.4 |
| Other | 0.0 | 0.7 | 0.2 | 30.3 | 0.1 | 48.6 |
| CNP internet payments | 1,355.4 | 151,716.4 | 125.0 | 27,548.1 | 154.0 | 34,743.3 |
| Lost or stolen cards | 0.3 | 21.6 | 3.9 | 555.8 | 7.9 | 1,962.7 |
| Intercepted cards | 0.0 | 0.0 | 0.2 | 13.5 | 0.2 | 35.3 |
| Forged or counterfeit cards | 0.1 | 11.2 | 3.0 | 558.0 | 12.8 | 2,470.2 |
| Misappropriated numbers | 1,355.0 | 151,677.2 | 115.9 | 26,026.6 | 132.0 | 28,055.2 |
| Other | 0.0 | 6.4 | 2.1 | 394.2 | 1.0 | 219.9 |
| Withdrawals | 139.5 | 41,252.8 | 3.8 | 880.5 | 2.2 | 631.4 |
| Lost or stolen cards | 137.9 | 40,931.6 | 3.3 | 784.3 | 1.0 | 305.8 |
| Intercepted cards | 0.6 | 205.8 | 0.0 | 3.8 | 0.0 | 0.4 |
| Forged or counterfeit cards | 0.1 | 15.3 | 0.2 | 48.3 | 1.2 | 310.9 |
| Misappropriated numbers | 0.0 | 4.0 | 0.2 | 31.7 | 0.1 | 12.5 |
| Other | 0.8 | 96.0 | 0.1 | 12.3 | 0.0 | 1.8 |
| **Total** | **1,982.8** | **230,626.7** | **209.6** | **38,220.3** | **273.8** | **59,870.2** |

*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 2014 – Issuance

*(volume in thousands; value in EUR thousands)*

| | French issuer, French acceptor | | French issuer, Foreign SEPA acceptor | | French issuer, Foreign non-SEPA acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Face-to-face payments and UPT | 3.09 | 2,040.95 | 0.93 | 585.80 | 5.82 | 1,323.39 |
| Lost or stolen cards | 1.18 | 404.45 | 0.11 | 79.53 | 0.43 | 94.77 |
| Intercepted cards | 0.65 | 356.56 | 0.15 | 71.59 | 0.07 | 34.41 |
| Forged or counterfeit cards | 0.27 | 51.73 | 0.36 | 286.49 | 4.32 | 789.18 |
| Misappropriated numbers | 0.34 | 173.71 | 0.32 | 148.20 | 1.00 | 405.03 |
| Other | 0.65 | 1,054.51 | 0.0 | 0.0 | 0.0 | 0.0 |
| CNP payments excluding internet | 0.24 | 250.74 | – | – | – | – |
| Lost or stolen cards | 0.00 | 0.00 | – | – | – | – |
| Intercepted cards | 0.00 | 0.00 | – | – | – | – |
| Forged or counterfeit cards | 0.00 | 0.00 | – | – | – | – |
| Misappropriated numbers | 0.17 | 171.01 | – | – | – | – |
| Other | 0.07 | 79.72 | – | – | – | – |
| CNP internet payments | 5.48 | 1,498.31 | 12.92 | 1,005.94 | 2.48 | 429.36 |
| Lost or stolen cards | 0.31 | 91.81 | 0.43 | 8.87 | 0.05 | 1.50 |
| Intercepted cards | 0.03 | 3.94 | 0.01 | 0.74 | 0.01 | 0.39 |
| Forged or counterfeit cards | 0.08 | 8.31 | 0.13 | 15.04 | 0.31 | 22.60 |
| Misappropriated numbers | 4.94 | 1,262.87 | 12.35 | 981.29 | 2.13 | 404.87 |
| Other | 0.13 | 131.37 | – | – | – | – |
| Withdrawals | 1.67 | 226.02 | – | – | – | – |
| Lost or stolen cards | 1.57 | 199.59 | – | – | – | – |
| Intercepted cards | 0.09 | 24.50 | – | – | – | – |
| Forged or counterfeit cards | 0.00 | 0.00 | – | – | – | – |
| Misappropriated numbers | 0.00 | 0.00 | – | – | – | – |
| Other | 0.01 | 1.93 | – | – | – | – |
| **Total** | **10.48** | **4,016.01** | **13.85** | **1,591.75** | **8.30** | **1,752.76** |

*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 2014 – Acceptance

*(volume in thousands; value in EUR thousands)*

| | French issuer, French acceptor | | Foreign SEPA issuer, French acceptor | | Foreign non-SEPA issuer, French acceptor | |
|---|---|---|---|---|---|---|
| | Volume | Value | Volume | Value | Volume | Value |
| Face-to-face payments and UPT | 3.09 | 2,040.95 | 0.20 | 76.10 | 4.64 | 3,059.16 |
| Lost or stolen cards | 1.18 | 404.45 | 0.03 | 17.10 | 0.59 | 368.53 |
| Intercepted cards | 0.65 | 356.56 | 0.00 | 1.18 | 0.00 | 4.25 |
| Forged or counterfeit cards | 0.27 | 51.73 | 0.06 | 26.91 | 3.70 | 2,435.01 |
| Misappropriated numbers | 0.34 | 173.71 | 0.10 | 30.92 | 0.35 | 250.81 |
| Other | 0.65 | 1,054.51 | 0.00 | 0.00 | 0.00 | 0.55 |
| CNP payments excluding internet | 0.24 | 250.74 | 0.01 | 9.19 | 0.01 | 6.50 |
| Lost or stolen cards | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Intercepted cards | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Forged or counterfeit cards | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Misappropriated numbers | 0.17 | 171.01 | 0.00 | 0.00 | 0.00 | 0.00 |
| Other | 0.07 | 79.72 | 0.01 | 9.19 | 0.01 | 6.50 |
| CNP internet payments | 5.48 | 1,498.31 | 2.43 | 1,030.54 | 7.93 | 2,692.55 |
| Lost or stolen cards | 0.31 | 91.81 | 0.01 | 2.87 | 0.14 | 34.12 |
| Intercepted cards | 0.03 | 3.94 | 0.00 | 2.99 | 0.10 | 5.09 |
| Forged or counterfeit cards | 0.08 | 8.31 | 0.18 | 77.20 | 0.73 | 215.56 |
| Misappropriated numbers | 4.94 | 1,262.87 | 2.22 | 936.93 | 6.97 | 2,437.79 |
| Other | 0.13 | 131.37 | 0.01 | 10.56 | 0.00 | 0.00 |
| Withdrawals | 1.67 | 226.02 | – | – | 0.00 | 0.90 |
| Lost or stolen cards | 1.57 | 199.59 | – | – | 0.00 | 0.00 |
| Intercepted cards | 0.09 | 24.50 | – | – | 0.00 | 0.00 |
| Forged or counterfeit cards | 0.00 | 0.00 | – | – | 0.00 | 0.84 |
| Misappropriated numbers | 0.00 | 0.00 | – | – | 0.00 | 0.00 |
| Other | 0.01 | 1.93 | – | – | 0.00 | 0.06 |
| **Total** | **10.48** | **4,016.01** | **2.63** | **1,115.82** | **12.59** | **5,759.12** |

*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, acceptor, 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 acceptor 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 L132-1 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 may be 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.

### 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;

• 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.

3 Personal Account Number.

## Types of payment:

- face-to-face payment, carried out at a 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).

## 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 and professional services: hotels, rental services, box office, charities, 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

**Production**
Banque de France
Press and Communication Directorate

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

**Orders**
Observatory for Payment Card Security
011-2323
Téléphone : +1 42 92 96 13
Télécopie : +1 42 92 31 74

**Imprint**
Banque de France



**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.