2011 | 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 : 11-2324

Annual report 2011
of the Observatory for payment card security

submitted to

The Minister of the Economy, Finance and External Trade
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

Contents

*The Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement – *hereinafter the Observatory), referred to in section I of Article L. 141-4 of the French* Monetary and Financial Code*, was created by virtue of 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).*[1]

Pursuant to the sixth indent of the above-mentioned article, the present document reports on the activities of the Observatory. It is addressed to the Minister of the Economy, Finance and External Trade and transmitted to Parliament. This year's report consists of:

- *a stocktaking of measures to protect online card payments (Part 1);*
- *the 2011 fraud statistics (Part 2);*
- *a summary of the Observatory's technology watch activities (Part 3), covering two areas: the use of mobile phones as payment terminals and the use of digital wallets to initiate card payment orders;*
- *a study on international cooperation in the fight against fraud (Part 4);*
- *a new annex that reminds cardholders to be on their guard and reiterates the best practices to follow when making payments to a merchant, online or when making withdrawals.*

1 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.

The 2011 Annual Report of the Observatory for Payment Card Security contains four sections, summarised as follows.

Part 1: measures to protect online card payments

The opinion survey conducted for the second year running by the Observatory and statistical data provided by banks and their technical providers show that real progress was made in 2011 in terms of protecting online card payments.

Even so, only 23% of online payment transactions are currently protected by one-time authentication, even though these solutions have demonstrated their effectiveness among some e-merchants and are welcomed by consumers. Accordingly, the progressive general introduction of one-time authentication, and hence of 3D-Secure, by e-merchants, with activation based on risk analyses, remains a priority for the Observatory, particularly for the most heavily used websites.

These recommendations are consistent with the findings of the Pauget-Constans Report on the future of payment instruments in France and the report by SecuRe Pay, Europe's new forum on the security of payment instruments, which recommend the general introduction across Europe of one-time authentication and strong cardholder authentication in internet payments as a function of transaction risk.

Part 2: 2011 fraud statistics

The fraud rate was up slightly for the fourth year in a row, standing at 0.077% in 2011, corresponding to total fraud of EUR 413.2 million. By comparison, in 2010 the rate was 0.074% and total fraud amounted to EUR 368.9 million.

Since non-domestic fraud was down slightly, the increase in domestic fraud reflected two key trends:

- *fraud in card-not-present (CNP) payments increased, with the fraud rate rising to 0.321%. The fraud rate for online payments climbed to 0.341%. The rate for payments by mail or phone increased more moderately. Overall, CNP payments accounted for just 8.4% of the value of domestic transactions but for 61% of fraud in value terms. Given the unfavourable trend in fraud recorded through this payment channel, the Observatory is calling on e-merchants, especially major firms, to act on its recommendations to deploy solutions such as 3D-Secure that enable one-time cardholder authentication for the most at-risk payments;*

• *the fraud rate for face-to-face payments climbed to 0.015% from 0.012% in 2010. The fraud rate for withdrawals also rose again, reaching 0.029%. The increase in fraud for these transactions, which nevertheless remains at low levels, follows several years of decline. It is partly attributable to an increase in thefts of cards with PINs. Given these trends, the Observatory reminds cardholders to be on their guard and reiterates the best practices to follow when making payments to a merchant, online or when making withdrawals (see Appendix 1).*

Also, and for the second year in a row, the Observatory calculated separate fraud rates for international transactions within Europe (Single European Payments Area – SEPA) and outside Europe, i.e. outside SEPA. Fraud rates outside Europe are about two and a half times higher than the rate within Europe for cards issued in France, and fraud affecting foreign cards issued outside Europe is seven times higher than that for cards issued in Europe. These statistics demonstrate the beneficial effects of the major efforts carried out within Europe in recent years to combat fraud, notably through the widespread use of EMV-compliant chip cards at points of sale and ATMs.

Part 3: technology watch on the security of mobile phones used as payment terminals and new online payment solutions (digital wallets)

Mobile phones used as payment terminals. The payment terminals market has witnessed many developments in recent months, with the emergence of solutions using advanced mobile devices, in particular smartphones. Since smartphones are by definition multi-application, multi-task devices without secure elements, they are fairly incompatible with the usual requirements for conventional payment terminals, which are designed specifically for the function. As the situation currently stands, therefore, if mobile payment terminals are to be used in the acceptance chain, then measures must be adopted to guarantee a level of security on a par with that provided with conventional payment terminals.

Digital wallets and card payments. Strong growth in e-commerce has led to the emergence of "alternative" payment solutions, such as digital wallets. Digital wallets contribute to the increased diversity of payment solutions by providing consumers with resources that are tailored to their uses. However, these developments must not come at the cost of payment card security, which could undermine confidence in existing means of payment and prompt fraud to shift to less well-protected solutions. For these reasons, the Observatory recommends that all participants implement measures to protect sensitive data (including data linked to payment cards), that digital wallet providers use systems to enable one-time authentication of the holder by the issuer when the card is saved in the wallet, that digital wallet providers conduct risk analyses resulting in one-time authentication for payments that are viewed as risky, and that clear rules be set as regards the management of payment instruments and transactions, including the definition and distribution of responsibilities between users, merchants and providers of these solutions.

Part 4: international cooperation in the fight against fraud

The Observatory conducted a stocktaking of participants in the anti-fraud effort in France and international cooperation arrangements. The review shows that participants have organised themselves in their respective areas, achieving tangible results, and that cooperation structures exist at domestic, European and international level. However, there is room for improvement. Notably, steps are needed to ensure the operational exchange of fraud data, which help in the detection of points of compromise, to finalise a common approach to the certification of acceptance terminals, notably as regards governance aspects, and to ensure that bank regulators harmonise security requirements at international level.

A stocktaking of measures to protect online card payments

The Observatory regularly monitors fraud in card-not-present (CNP) payments, which amounted to EUR 129.6 million in 2011 (giving a fraud rate of 0.321%), as well as the counter-fraud measures put in place by payment chain participants. One of the Observatory's key recommendations is that participants should gradually generalise one-time cardholder authentication for online payments wherever possible and appropriate.

The first section of this chapter reports on progress in implementing the Observatory's recommendation. The second section considers how banks and merchants have implemented one-time authentication, as well as the related costs. The third and final section is devoted to SecuRe Pay, Europe's new forum on the security of payment instruments, which is driving the implementation of one-time authentication at European level.

1| A stocktaking of measures to protect online card payments

1|1 Progress in deploying 3D-Secure

To monitor the deployment of one-time authentication solutions by issuers and identify difficulties or areas for improvement, the Observatory began in 2011 collecting weekly statistics from banks and their technical providers to measure quantitative and qualitative developments in the implementation of one-time authentication. The data gathered by the Observatory show a marked improvement in the deployment rate of such solutions by issuers and merchants in 2011.

1|1|1 84% of cardholders have now been provided with functional authentication systems

Virtually all cardholders have now been provided with at least one one-time authentication solution, in line with recommendations made by the Observatory. By far the most common solution is authentication by text message.[1]

In the space of a year, activation rates[2] for these solutions among cardholders increased from 67% to 84% of the total population of online shoppers. Rates continue to vary from issuer to issuer, reflecting the relative complexity of the activation processes put in place. Participants thus still need to provide support to help users switch to the new solutions (see 1|2|3).

1|1|2 The failure rate for secure transactions remains steady at around 20%

The failure rate for secure transactions is around 20%. Although this rate may seem high at first glance, it neither takes account of failures followed by a successful attempt nor attempted fraud. The situation varies widely from issuer to issuer, and the Banque de France deals on a bilateral basis with the least satisfactory cases. The Observatory will continue to closely monitor this rate to ensure that it gradually declines.

1 Some banks have introduced solutions based on tokens, card readers or emails combined with one-time codes given by matrix cards. See the 2009 Annual Report, chapter 4, p.51-52, for a more complete description of these authentication solutions.

2 In the case of a text message-based approach, for example, to activate the solution, the cardholder has to give his or her bank the number of the mobile phone to which one-time codes should be sent.

1|1|3 The share of transactions authenticated by 3D-Secure has increased sharply thanks to the migration of a major e-merchant

While the proportion of merchants enabling strong authentication of online shoppers was stable at about 50%, the share of transactions authenticated by 3D-Secure rose in value terms from 17.9% to 23% over one year.

Voyages-SNCF.com, a major player in online commerce, played a large part in this increase by adopting 3D-Secure in July 2011. Initially, the firm targeted transactions with an especially high risk level before gradually extending the scope of the new security measures. These figures, which go up to autumn 2011, are likely to increase further in 2012 since Voyages-SNCF.com stepped up its deployment of 3D-Secure from Q3 2011.

1|2 How French online shoppers perceive one-time authentication solutions

In 2011, the Observatory updated the results of the survey conducted as part of its 2010 Annual Report to assess how cardholders perceive one-time authentication solutions.[3] Having to enter a one-time code received by text message was the most widely used solution, which corroborates the data collected from issuers. There was greater awareness of the various solutions, and the share of people who used at least one solution increased markedly, consistent with the steady deployment of 3D-Secure, thanks notably to the contribution of Voyages-SNCF.com.

1|2|1 77% of online shoppers consider online card payments to be safe

Payment by card is perceived as a safe way to pay for online purchases, although the share of users who felt nervous rose sharply compared with the previous year, from 23% to 33%. The feeling of nervousness declines with the frequency of purchases and the use of at least one one-time authentication solution.

These results reflect the need among respondents to be reassured when making online purchases and justify actions by the Observatory to promote the implementation of strong cardholder authentication solutions.

1|2|2 Growing awareness of strong authentication systems to protect online card purchases

More than eight in ten online shoppers (83%) say that they have heard of authentication solutions to protect online card purchases (compared with 79% in 2011). Awareness of these solutions appears to be well established and on the increase among online shoppers.

Although the share of online shoppers who said that they had received information from their bank increased from 39% to 44%, this low percentage explains respondents' expectations in terms of communication (see 1|2|3). However, where information was provided by the relevant actors, respondents felt that it was clear, a sentiment that has grown since last year (up from 84% to 89%).

1|2|3 Ease of use is key

On the whole, respondents find the solutions easy to use...

Only 8% of users said that they found at least one one-time authentication solution difficult to use, much the same percentage as last year. Mini card readers and matrix cards were again viewed as the least user-friendly solutions.

... but users still need support when using the solutions for the first time or subsequently

Solutions involving codes sent by text message are seen as the most user-friendly as banks have, on the whole, provided clear communications on these solutions.

3 The survey was conducted by LH2. The methodological approach was the same as for the survey conducted as part of the 2010 Annual Report (see p. 35).

Compared with the previous survey, respondents had greater difficulties both understanding how solutions worked (from 26% to 40%) and accessing the said solutions (from 27% to 32%). However, fewer than 10% of users were actually unable to use the solutions, and they tended to experience fewer problems in subsequent attempts.

These results show that users still need support from all participants to make the transition to the new solutions. When asked which groups could usefully provide information about the new solutions, the vast majority of respondents mentioned banks (80%), ahead of e-merchants (49%).

1|2|4 Solutions that enhance security and place websites at an advantage

The trade-off between inconvenience and benefit still largely favours security

Around 90% of respondents felt that these solutions significantly improve the security of online bank card payments. Only one person out of five was unhappy about the extra time required to use the new solutions.

Overall, 84% of users said that they felt safer when making online card purchases with the new solutions, compared with 76% in 2011.

Users do not view these solutions as a handicap for websites, but rather as an argument in their favour

While the share of users who said that they would either maintain or increase their level of online shopping following the implementation of these solutions was steady in 2011, at 97%, the proportion of respondents who said that the new solutions were likely to encourage them to do more online shopping doubled to 35% of users.

The importance of security when choosing where to shop online also increased sharply: 23% said that they would shop solely on websites offering such solutions (17% in 2011) while 57% said that they would prefer to use such sites (compared with 54% in 2011).

These results confirm the interest of cardholders in solutions that provide them with enhanced security when shopping online and in communications that enable them to use these solutions immediately. Such communications should mainly be provided by banks and merchants, which are also responsible for deploying these solutions, relying on the infrastructures proposed by card payment schemes. The following section considers the implementation of one-time authentication and looks at the organisational, technical and financial impact on participants.

2| Costs of implementing one-time authentication

To build on the survey on the costs of EMV deployment contained in its 2010 Annual Report, the Observatory decided to assess the impact for issuers and merchants[4] of deploying one-time authentication solutions to protect online card payments.

2|1 A large-scale project for banks, harder to measure among merchants

2|1|1 Banks have taken different paths to implementing one-time authentication

All respondent banks emphasized the importance of human resources assigned to these projects,

4 The following participated in the survey: BPCE, Crédit Agricole SA, Crédit Mutuel-CIC, Société Générale, La Banque Postale, LCL, GIE Cartes Bancaires, MasterCard, Voyages-SNCF and Air France. Of these, the card payment schemes questioned said that they were not concerned.

both during the various implementation phases (preliminary studies, development, drafting and monitoring of procedures, overall project management, internal training), and after the deployment, with the creation of special counter-fraud and user support units.

The costs linked to the introduction of one-time authentication were however largely attributable (80%-90%) to the technical solutions involved:

• new Access Control Servers (ACS) to authenticate cardholders were required. Banks followed a range of strategies in this regard, with some developing servers internally, while others outsourced the solution completely. The cost structures resulting from this phase of the project thus varied considerably across respondent institutions: whereas investment expenditures were high in the first case, they were low in the second, but offset by higher operating costs at a later stage;

• providing cardholders with the technical solutions to enable one-time authentication was another major expense item. Some of these solutions, such as tokens, generate substantial manufacturing costs (usually borne in large part by issuers). Others, such as the text messaging approach, may entail sizeable recurring costs (see 2|2|1).

All respondents agreed on the importance of assigning resources to communicating with:

• cardholders, through all available channels (sending out brochures, online and in-branch communications);

• merchants, to clarify the nature and scope of the liability shift arising from the implementation of such solutions.

Communication efforts are expected across-the-board and must be maintained.

2|1|2 Merchants include these projects within broader costs

Merchants taking part in the survey found it harder to isolate the expenses specific to the project, since spending on customer support and communication, which make up a large share of the expenses, are usually included in the overall costs of call centres and more general marketing activities.

As in the case of banks, more technical expenses (deployment of 3D-Secure type solutions) depend closely on whether merchants decide to outsource electronic payment solutions. Some merchants have developed their own payment platforms (leading to higher development costs when integrating 3D-Secure), while others base their solutions on platforms managed by outside providers, which leads to higher costs at a later stage.

2|2 Tangible financial and organisational effects

2|2|1 A genuine impact on fraud, together with an additional cost that warrants a risk-based approach

The different cost structures of the various institutions make it hard to aggregate the results, as seen above. However, respondent institutions agree that there is an additional cost per transaction for one-time cardholder authentication compared with weak authentication or non-authentication.

Weak authentication solutions involve an additional cost of between EUR 0.025 and EUR 0.05 per transaction compared with a non-authenticated transaction. Strong cardholder authentication, meanwhile, costs between EUR 0.105 and EUR 0.11 more than weak authentication per transaction. Note that these findings vary among institutions depending on the authentication method used.

This additional cost justifies taking the risk-based approach recommended by the Observatory, whereby institutions employ strong cardholder authentication based on the estimated risk of the transaction.

Strong authentication has a significant impact on fraud rates no matter what method is used. Although banks find it hard to isolate the effects of strong authentication from other counter-fraud measures (such as transaction scoring), they do find that fraud in CNP transactions is cut by 70% to 90% depending on the issuer. These figures are corroborated by merchants. Furthermore, steps to ensure the reliability of internal lists of phone numbers or emails, which form an integral part of the customer enrolment process, improve the effectiveness of warning processes triggered in the event of suspected or actual fraud, and enable participants to respond more swiftly.

Banks emphasise that these projects also have a positive impact on image, by boosting customer confidence and creating a feeling of greater security.

2|2|2 One-time authentication projects open up prospects for merchants without impacting business volumes

Merchants that took part in the survey (i.e. Voyages-SNCF and Air France) stressed that implementation of 3D-Secure did not impact their revenues overall.

In fact, they found that the project opened up new financial and commercial prospects for them:

• commissions to acquirer banks went down;

• the enhanced security of transactions allowed merchants to expand the range of products available online to include more expensive or completely paperless products, which are traditionally more vulnerable to fraud.

2|3 Strong authentication will take other forms in the years ahead

2|3|1 Banks will propose new solutions

Two major questions lead now banks to engage on reflection:

• all payment chain participants expect to see growth in electronic commerce using mobile phones connected to the internet. In this setting, security solutions based on sending one-time codes to phones are deemed to be less effective and user-friendly. Discussions are thus underway aimed at addressing these specific constraints;

• face-to-face and CNP environments are converging. For example, customers can now initiate face-to-face transactions by using mobile phones or by connecting to online selling environments. Banks are therefore planning to standardise the security solutions for different selling channels by offering merchants and cardholders technical solutions that are tailored to these new methods for initiating transactions.

Against this backdrop, the latest technological innovations are providing new means of authentication, such as bank cards with new built-in functionalities, including the ability to generate one-time codes on an integrated screen.

2|3|2 Merchants will make these solutions available on a wide range of channels

The same trend can be observed among merchants, who are monitoring the development of new payment methods, such as digital wallets. They too believe it is vital to standardise security levels for all payment instruments offered on websites.

The survey feedback points to a positive cost/benefit trade-off for merchants with no impact on revenues. The additional cost currently generated by one-time authentication and borne by issuers justifies taking the risk-based approach recommended by the Observatory. The Observatory once again urges major e-merchants to migrate to 3D-Secure. This recommendation is taken up in the recent Pauget-Constans Report on the future of payment instruments in France[5] as well as in the report prepared by the SecuRe Pay Forum on the security of online payments,[6] which is described below.

3| SecuRe Pay, working to harmonise security levels within Europe

3|1 A forum that brings together all participants with responsibility for overseeing the security of payment instruments

The SecuRe Pay Forum, which was set up in 2011, seeks to aid overseers and supervisors of payment services providers to gain a shared awareness and understanding of issues in the area of retail payments security.

SecuRe Pay thus includes the bank supervisors and central banks of EU member countries. Each year, it establishes a work programme and establishes working groups that consult with market participants on the topics addressed.

The working groups set up in 2011 worked on the protection of online banking services and the security of online card payments, with a view to combating fraud, in line with the priorities of the Observatory. These activities will lead to the publication of an initial report in 2012,[7] whose final recommendations will be applied by banks, payment services providers as well as merchants indirectly through their acquirer banks.

3|2 Recommendations consistent with those issued by the Observatory

The forum recommends the general use of one-time authentication to protect online card payments, with application of a risk-based approach to ensure that the primary focus is to protect the transactions that are most exposed to fraud, wherever this is possible and appropriate.

The recommendations cover alternative payment solutions based on card payments, such as digital wallets, and provide for the adoption of supplementary security measures for the enrolment process, data security, risk analysis updates, etc.

4| Conclusion: steady increase in levels of online security, thanks to efforts by all participants

The opinion survey conducted for the second year running by the Observatory and the statistical data provided by banks and their technical providers show that real progress was made in protecting online card payment transactions in 2011. Increased awareness of the security solutions demonstrates how these solutions have matured in the space of a year.

5 Report published in March 2012, p. 17: "Ensure maximum security for online payments through general use of the 3D-Secure solution". The goals of the Pauget-Constans Report are (1) to perform a stocktaking of payment instruments used in France and (2) to identify developments or innovations required to better address the needs of consumers and improve security while cutting the costs of these solutions. The report recommends developing secure online payments and face-to-face card payments, reducing the role of cheques and developing new payment services. It encourages general government to participate actively in taking these efforts forward.
http://www.banque-france.fr/ccsf/fr/publications/telechar/autres/rapport_avenir_moyens_paiement.pdf

6 Report published in April 2012, p. 11: "Internet payment services should be initiated by strong customer authentication".

7 A public consultation on the draft report was held from April to June 2012.

The benefits linked to the introduction of strong authentication resources and 3D-Secure appear to be real and felt by banks and merchants alike (with a substantial decrease in fraud rates for secure transactions) and consumers, who continue to welcome these solutions. Deployment costs appear to be significant for stakeholders, although they remain hard to estimate.

The Observatory recommends that banks and merchants keep up their efforts to combat the increase in the fraud rate for CNP transactions, which remains high (see chapter 2, p.24):

• since banks have more or less completed the deployment of strong authentication solutions, the challenge now facing them is to put together appropriate communication plans to show cardholders and merchants how to use the solutions and explain the related benefits. Some banks also need to do work to improve the success rate for secure transactions;

• the general introduction of one-time authentication and hence of 3D-Secure among merchants, with activation based on risk analyses, remains a priority for the Observatory. In this context, the adoption of 3D-Secure by several major e-merchants should play a determining role in improving the reliability of lists held by issuers and ensuring broader use of this protocol by large e-merchants;

• these recommendations are consistent with the findings of the Pauget-Constans Report on the future of payment instruments in France and the SecuRe Pay report on the security of internet payments in Europe, which recommend, respectively, the general introduction of one-time authentication and strong cardholder authentication in internet payments as a function of transaction risk.

Fraud statistics for 2011

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 2011 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 appropriated card numbers. In addition, Appendix 5 to this report presents a series of detailed fraud indicators.

Box 1

Fraud statistics: respondents

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

The statistics calculated by the Observatory thus cover:

- *EUR 485.2 billion in transactions in France and in other countries made with 64.7 million four-party cards issued in France (including 1.92 million electronic purses and 3.26 million contactless cards);*
- *EUR 18.8 billion in transactions primarily in France with 21.0 million three-party cards issued in France;*
- *EUR 29.6 billion in transactions in France with foreign three-party and four-party cards.*

Data were gathered from:

- *nine three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref and Sofinco), Cofidis, Cofinoga, Diners Club and Franfinance;*
- *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.*

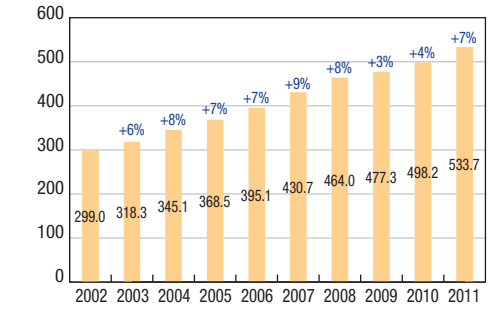
1| Overview

The total value of card payments amounted to EUR 533.7 billion in 2011, up 7% compared with 2010. The annual growth rate returned to levels close to those of 2004-2008, after two years of more moderate growth in 2009 (3%) and 2010 (4%).

Chart 1

Value of transactions

(EUR billions)



Source: Observatory for Payment Card Security.

The total amount of fraud increased sharply, rising by 12% compared with 2010 to reach EUR 413.2 million in 2011. Since non-domestic fraud was down slightly, the increase in fraud reflected two domestic trends:

- another substantial increase in fraud in CNP payments, notably among online payments. Overall, CNP payments accounted for 8.4% of the value of domestic transactions but for 61% of fraud in value terms;

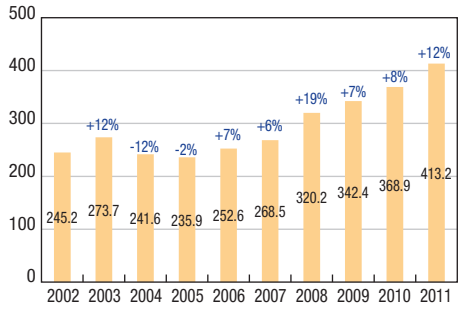
- for the first time in several years, fraud in face-to-face payments increased. Withdrawal fraud was also up, following on from the growth noted last year. Even so, the fraud rate for this type of transaction is still some 20 times lower than the rate for CNP transactions.

Owing to these trends, the overall fraud rate for card payments and withdrawals recorded by French schemes in 2011 stood at 0.077%, a slight increase for the fourth year running.

Chart 2

Amount of fraud

(EUR millions)



Source: Observatory for Payment Card Security.

The rate of issuer fraud, which covers all fraudulent payments and withdrawals made in France and in other countries with cards issued in France, was 0.061% in 2011, up from 0.057% in 2010. Issuer fraud totalled EUR 306.8 million, compared with EUR 269.3 million in 2010.

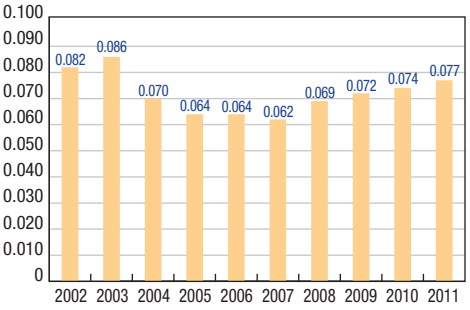
The rate of acquirer fraud, which covers all fraudulent payments and withdrawals made in France with all French and foreign cards, rose more sharply, to 0.063%, corresponding to fraud of EUR 317.8 million, from 0.055% and EUR 263 million in 2010.

The average value of a fraudulent transaction was also up, from EUR 122 in 2010 to EUR 130.

Chart 3

Fraud rate, all card and transaction types

(%)



Source: Observatory for Payment Card Security.

2| Breakdown of fraud by card type

Table 1

Breakdown of fraud by card type

(% rate, amounts in EUR millions)

	2007	2008	2009	2010	2011
Four-party cards	0.063 (253.6)	0.070 (304.3)	0.072 (324.3)	0.074 (351.5)	**0.077 (394.9)**
Three-party cards	0.052 (15.0)	0.054 (16.0)	0.068 (18.2)	0.080 (17.4)	**0.083 (18.3)**
Total	0.062 (268.5)	0.069 (320.2)	0.072 (342.4)	0.074 (368.9)	**0.077 (413.2)**

Source: Observatory for Payment Card Security.

Overall fraud rates were up by the same amount for both types of cards.

Issuer and acquirer fraud rates for four-party cards stood at 0.061% and 0.062% respectively, compared with 0.057% and 0.055% respectively in 2010. The average value of a fraudulent transaction was EUR 127, compared with EUR 119 in 2010.

Issuer and acquirer fraud rates for three-party cards were 0.059% and 0.071% respectively, compared with 0.063% and 0.068% respectively in 2010. The average value of a fraudulent transaction was EUR 321 in 2010, compared with EUR 353 in 2010.

3| Geographical breakdown of fraud

The geographical breakdown of fraud in 2011 reveals a sharp increase in fraud in domestic transactions, which rose by 29.1% compared with 2010 to EUR 211.5 million. As a result, for the first time since the Observatory was established in 2002, the amount of fraud in domestic transactions overtook that of fraud in international transactions, which declined by 1.6% on 2010 to EUR 201.7 million.

Even so, because of the transaction values involved, the fraud rate for international transactions, at 0.367%, was still around eight times higher than the rate for domestic transactions (0.044%).

International transactions thus account for 49% of the total value of fraud, even though they make up just over 10% of the total value of card payments.

Fraud in foreign transactions using cards issued in France fell by 9.7% from EUR 105.5 million in 2010 to EUR 95.3 million. The fraud rate for transactions outside SEPA with cards issued in France was more than two and a half times higher than the rate for transactions conducted within SEPA with the same types of cards (0.638% vs. 0.255%).

Table 2

Geographical breakdown of fraud

(% rate, amounts in EUR millions)

	2007	2008	2009	2010	2011
Domestic transactions	**0.029 (114.5)**	**0.031 (130.9)**	**0.033 (144.0)**	**0.036 (163.8)**	**0.044 (211.5)**
International transactions	**0.368 (154.0)**	**0.427 (189.4)**	**0.449 (198.4)**	**0.423 (205.0)**	**0.367 (201.7)**
- o/w French issuer and foreign acquirer [a]	0.476 (85.3)	0.594 (118.3)	0.594 (121.6)	0.728 (54.9)	0.638 (51.0)
- o/w French issuer and SEPA acquirer	–	–	–	0.331 (50.6)	0.255 (44.3)
- o/w foreign issuer [b] and French acquirer	0.288 (68.7)	0.291 (71.0)	0.324 (76.8)	0.831 (64.5)	0.892 (81.3)
- o/w SEPA issuer and French acquirer	–	–	–	0.195 (35.0)	0.122 (25.1)
Total	**0.062 (268.5)**	**0.069 (320.2)**	**0.072 (342.4)**	**0.074 (368.9)**	**0.077 (413.2)**

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

Fraud in domestic transactions using foreign cards however increased by 6.9% from EUR 99.5 million in 2010 to EUR 106.4 million in 2011. That being said, fraud in transactions in France with foreign cards issued in SEPA fell substantially (by 28%, from EUR 35 million in 2010 to EUR 25.1 million in 2011), while fraud in domestic transactions with foreign cards issued outside SEPA jumped 26% from EUR 64.5 million to EUR 81.3 million in 2011.

The fraud rate for transactions in France using foreign cards issued outside SEPA is thus more than seven times higher than the rate for transactions carried out using foreign cards issued in SEPA (0.892% vs. 0.122%), justifying the efforts made over recent years in Europe to migrate cards and payment terminals to the EMV standard (cf. chapter 3.3 – Progress on the migration to EMV).

4| Breakdown of fraud by transaction type

The Observatory's classification of card payment transactions distinguishes face-to-face payments and unattended payment terminal (UPT) payments, which are made at the point of sale or at fuel pumps, ticket machines, etc., from card-not-present (CNP) payments made online, by post, telephone, fax, etc., and withdrawals. For the sake of clarity, the following section distinguishes national data from cross-border data.

In the case of domestic transactions, the figures show that:

- the fraud rate for face-to-face and UPT payments increased to 0.015%, after declining steadily since 2004. Face-to-face and UPT payments accounted for over 67% of domestic transactions but just 23% of fraud in value terms.

The fraud rate for withdrawals also increased markedly to 0.029%.

The increasing fraud among these transactions may reflect more challenging economic conditions than in previous years and an increase in thefts of cards with PINs from more vulnerable sections of the population. The number of cards reported lost or stolen, for which at least one fraudulent transaction was recorded, increased sharply, by 16%, from 640,500 in 2010 to 745,000 in 2011. There was also a 18% leap in attacks on automated teller machines (ATMs), which now appear to be a preferred target of organised crime rings, a fact supported by the increase in the number of such cases handled by law enforcement agencies (see Box 2 on indicators provided by law enforcement agencies). Given this trend, the Observatory is reiterating its guidance to cardholders on best practices for protecting themselves when making payments to a merchant, online or when making withdrawals (see Appendix 1).

Table 3

Breakdown of domestic fraud by transaction type

(% rate, amounts in EUR millions)

	2007	2008	2009	2010	2011
Payments	0.032 (95.6)	0.036 (111.7)	0.038 (123.2)	0.041 (137.3)	0.049 (177.8)
- o/w face-to-face and UPT	0.017 (45.4)	0.015 (44.5)	0.014 (41.0)	0.012 (36.2)	0.015 (48.1)
- o/w card-not-present	0.236 (50.1)	0.252 (67.2)	0.263 (82.2)	0.262 (101.1)	0.321 (129.6)
- o/w by post/phone	*0.201* *(23.8)*	*0.280* *(28.5)*	*0.263* *(30.3)*	*0.231* *(27.3)*	*0.259* *(25.4)*
- o/w online	*0.281* *(26.4)*	*0.235* *(38.8)*	*0.263* *(51.9)*	*0.276* *(73.9)*	*0.341* *(104.2)*
Withdrawals	0.020 (19.0)	0.018 (19.1)	0.019 (20.8)	0.024 (26.5)	0.029 (33.7)
Total	**0.029** **(114.5)**	**0.031** **(130.9)**	**0.033** **(144.0)**	**0.036** **(163.8)**	**0.044** **(211.5)**

Source: Observatory for Payment Card Security.

• the fraud rate for CNP payments increased by 22% to 0.321%, more than 20 times higher than the fraud rate for face-to-face payments. The fraud rate for online payments, in particular, continued to rise, climbing to 0.341%. The rate for payments by mail or phone increased more moderately. Amid sustained growth in electronic commerce, CNP payments accounted for just 8.4% of the value of domestic transactions but for 61% of fraud in value terms (the same as in 2010).

In view of the level of fraud recorded through this payment channel, the Observatory is repeating its recommendations that e-merchants, particularly the largest ones, deploy solutions such as 3D-Secure that enable one-time authentication of cardholders for the most at-risk payments (cf. chapter 1 of this report).

In the case of international transactions, the Observatory has a detailed breakdown of fraud by transaction type only for transactions by French cards in other countries.

Fraud in face-to-face and UPT payments fell from EUR 35.0 million in 2010 to EUR 28.6 million in 2011. The fraud rate for face-to-face payments made using French cards outside SEPA (0.369%) was two and a half times higher than the rate for face-to-face payments in SEPA (0.140%), where virtually all points of sale have migrated to EMV. However, this ratio was halved between 2010 and 2011 owing to efforts by card issuers to combat magnetic stripe counterfeiting fraud.

The fraud rate for payments made with foreign cards issued outside SEPA increased to 1.056% in 2011, compared with 0.982% in 2010, and is now three and a half times higher (compared with two and a half times in 2010) than the rate for payments made with foreign cards issued within SEPA, where virtually all issuers have migrated their cards to EMV.

While fraud in CNP payments with French cards declined from EUR 54.0 million in 2010 to EUR 45.0 million in 2011, the fraud rate for CNP payments is still high (1.320% outside SEPA), and well above the rate for face-to-face and UPT payments. The rate of fraud in CNP payments with French cards in SEPA fell sharply, to 0.571% in 2011 from 0.944% in 2010. The introduction of strong authentication systems, consistent with the guidelines of the European Forum on the Security of Retail Payments (SecuRe Pay – cf. chapter 1) should help to confirm this trend.

Fraud in withdrawals increased, chiefly among transactions conducted with French cards outside SEPA, where EMV use is not standardised.

Box 2

Indicators provided by law enforcement agencies

In 2011, law enforcement agencies recorded a virtually unchanged number of arrests connected with bank card fraud, reporting 234 arrests, compared with 235 in 2010, 190 in 2009 and 154 in 2008.

ATM attacks were up sharply, with 622 registered in 2011, compared with 527 in 2010, 526 in 2009, 427 in 2008, 391 in 2007, 515 in 2006, 200 in 2005 and 80 in 2004. There were also 32 attacks on payment terminals (30 in 2010). These figures corroborate the statistical uptrend noted by the Observatory in withdrawal and payment fraud. There were no attacks on card-operated fuel pumps (compared with six in 2010).

Numerous investigations into these cases were carried out nationwide. Police dismantled six labs that were counterfeiting foreign bank cards.

Box 3

Domestic fraud in CNP payments, by sector of activity

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

Table

Breakdown of domestic fraud in CNP payments, by sector of activity

(amounts in EUR millions, % share)

Sector	Fraud amount	Sector share of fraud
Travel, transportation	31.9	24.9
General and semi-general trade	21.4	16.7
Personal services	19.3	15.1
Telephony and communications	17.8	13.9
Technical and cultural products	10.8	8.4
Household goods, furnishings	9.9	7.7
Account loading, person to person sales	6.6	5.1
Professional services	3.2	2.5
Miscellaneous	2.6	2.0
Food	2.2	1.7
Online gaming	2.0	1.5
Insurance	0.4	0.3
Health and Beauty	0.1	0.1
Total	**128.3**	**100.0**

The travel/transportation, general and semi-general trade, personal services, and telephony and communications sectors were the most exposed to internet fraud, accounting for 70% of the total. A comparison of average fraud rates for each sector of activity provides additional information, revealing that some sectors, including technical and cultural products and household goods and furnishings, have considerable exposure despite accounting for a small portion of the total fraud amount.

Note also that the fraud rate in the online gaming sector fell steeply in 2011, to 0.303% compared with 0.478% in 2010 and 0.740% in 2009, and is now below the average rate for all sectors combined (cf. chart). This decline is attributable to the gradual introduction of one-time authentication systems by online gaming sites, in line with the Observatory's recommendations and the complementary awareness actions by the online gaming regulator.

Chart

Domestic fraud rate for CNP payments, by sector of activity

(%)

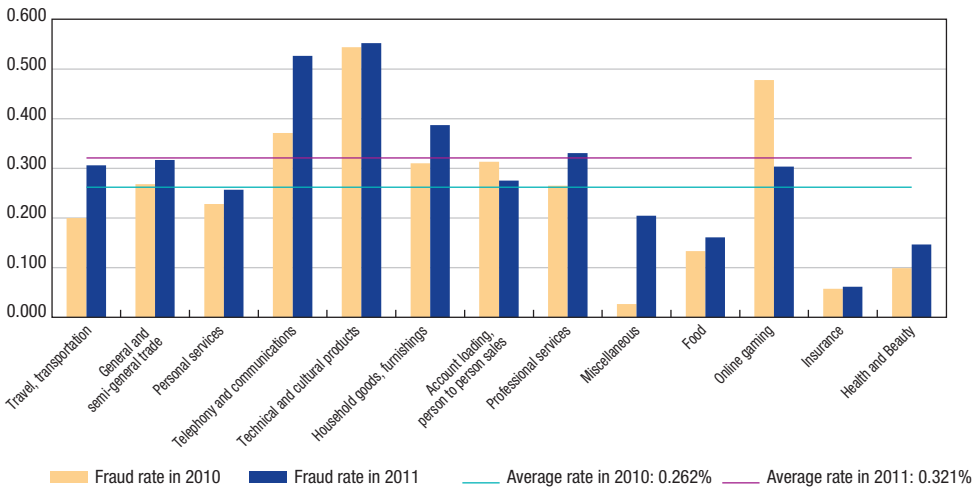


Table 4

Breakdown of international fraud by transaction type

(% rate, amounts in EUR millions)

French issuer – foreign acquirer [a]	**2008**	**2009**	**2010**	**2011**
Payments	0.655	0.679	0.795	0.561
	(99.3)	(105.2)	(39.8)	(30.5)
- o/w face-to-face and UPT	0.286	0.406	0.655	0.369
	(32.0)	(44.7)	(25.8)	(16.0)
- o/w card-not-present	1.698	1.350	1.310	1.320
	(67.2)	(60.5)	(14.0)	(14.5)
- o/w by post/phone	*1.284*	*1.016*	*1.193*	*1.011*
	(11.2)	*(9.7)*	*(3.8)*	*(3.1)*
- o/w online	*1.815*	*1.440*	*1.360*	*1.440*
	(56.0)	*(50.8)*	*(10.2)*	*(11.4)*
Withdrawals	0.399	0.331	0.596	0.800
	(19.1)	(16.5)	(15.1)	(20.5)
Total	**0.594**	**0.594**	**0.728**	**0.638**
	(118.3)	**(121.6)**	**(54.9)**	**(51.0)**
French issuer – SEPA acquirer				
Payments	–	–	0.396	0.300
			(49.1)	(43.1)
- o/w face-to-face and UPT	–	–	0.112	0.140
			(9.2)	(12.6)
- o/w card-not-present	–	–	0.944	0.571
			(40.0)	(30.5)
- o/w by post/phone	–	–	*0.566*	*0.643*
			(4.0)	*(5.6)*
- o/w online	–	–	*1.021*	*0.557*
			(36.0)	*(24.9)*
Withdrawals	–	–	0.052	0.040
			(1.5)	(1.2)
Total	**–**	**–**	**0.331**	**0.255**
			(50.6)	**(44.3)**
Foreign issuer [b] **– French acquirer**				
Payments	0.339	0.397	0.982	1.056
	(65.4)	(74.1)	(63.2)	(80.7)
Withdrawals	0.110	0.055	0.103	0.042
	(5.6)	(2.8)	(1.4)	(0.6)
Total	**0.291**	**0.324**	**0.831**	**0.892**
	(71.0)	**(76.8)**	**(64.5)**	**(81.3)**
SEPA issuer – French acquirer				
Payments	–	–	0.239	0.155
			(33.8)	(24.3)
Withdrawals	–	–	0.032	0.017
			(1.2)	(0.8)
Total	**–**	**–**	**0.195**	**0.122**
			(35.0)	**(25.1)**

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

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 fraudsters;
- appropriated card numbers, when a card number is copied without the cardholder's knowledge or created through card generation processes (which use programs to generate random card numbers) and then used for CNP transactions;
- "other" fraud, which covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts by means of identity theft.

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

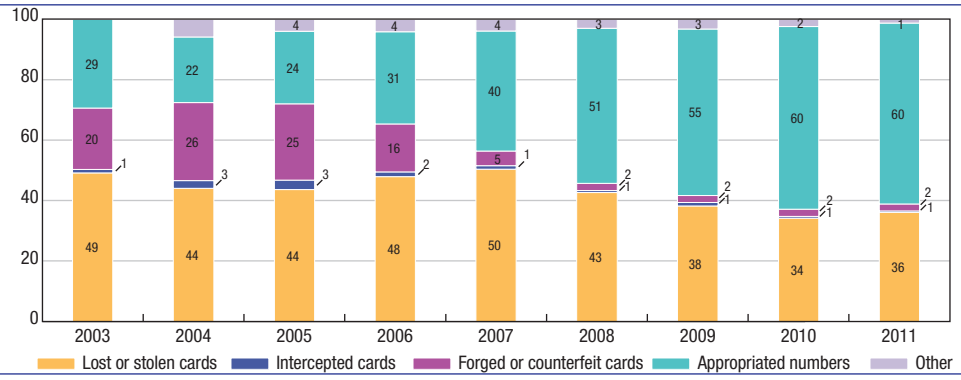
Fraud involving the use of appropriated card numbers for CNP payments is the most common type of fraud (59.9%), although it declined slightly from 60.5% in 2010. After falling for three years in a row, fraud involving lost or stolen cards accounted for 36.1% of fraudulent domestic payments, up from 34.2% in 2010. This trend corroborates the increase in fraud noted in face-to-face payments and withdrawals, which requires a card that has not yet been reported lost or stolen. Counterfeit cards accounted for just 2.3% of fraudulent domestic payments (2.4% in 2010).

"Other" fraud was stable. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for some 40% of the fraud involving these cards.

Chart 4

Breakdown by fraud type (domestic transactions, fraud amount)

(%)



Source: Observatory for Payment Card Security.

Table 5

Breakdown of domestic payment fraud by fraud type and by type of card in 2011

(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	36.1	74.8	36.5	1.5	22.2
Intercepted cards	1.1	0.5	0.5	0.2	0.6	8.9
Forged or counterfeit cards	4.9	2.3	4.1	2.0	0.8	12.7
Appropriated numbers	126.6	59.9	125.4	61.2	1.2	18.7
Other	2.7	1.3	0.2	0.1	2.5	37.5
Total	**211.5**	**100**	**204.9**	**100**	**6 .6**	**100**

Source: Observatory for Payment Card Security.

Technology watch

1| Mobile phones as payment terminals

Electronic payment terminals (EPTs) evolve regularly, reflecting technological changes affecting payment cards (such as the migration to EMV – Europay MasterCard Visa – standards) or communication networks and protocols (GPRS – General Packet Radio Service, 3G, Wifi networks, NFC[1], and so on). The security implications of these developments for payment terminals need to be routinely reviewed. In recent years, the Observatory has examined several of these developments, notably those relating to the EMV migration (2009 Annual Report, chapter 3, p. 38), "thin" terminals (2009 Annual Report, chapter 3, p. 35) and the security of UPT networks (2008 Annual Report, chapter 3, p. 35).

At present, devices that allow a merchant with a physical point of sale to accept card payments are devoted solely to these payment transactions.[2] They provide a range of functions, including payment display, card recognition and validation (stripe or chip), PIN (Personnal Identification Number) entry (for chip cards) and secure transmission of transaction data to the acquirer's servers.

With recent technological developments, however, other devices can now perform some or all of these functions, even though it is not their primary role to do so. Smartphones,[3] i.e. mobile phones with advanced technical capabilities, look set to play a bigger role in this context. Several solutions are already on the market, particularly in the USA, offering services to highly mobile small businesses, such as photographers, tradesmen and delivery firms. These solutions can be used, for example, to collect a payment at the place where the service is provided, or to ease queues at large retailers by adding acceptance points according to demand. While for the time being these solutions occupy a marginal share of the services offered by the payments industry, they may well take on much greater importance, as they allow any person or entity with an ordinary smartphone to easily collect payments without the need for special equipment. This explains their rapid rise in environments where traditional payment terminals have struggled to establish themselves.

The Observatory has analysed the functioning and security of mobile phone-based payment terminals in order to assess the security criteria for implementing this new approach to payment acceptance in France. The following analysis begins by reviewing the solutions that currently exist on the market, which are grouped according to whether or not a physical device is connected to the mobile phone. It then describes the associated security issues.

1|1 Different approaches to using mobile phones as EPTs

Acceptance of card payments using a mobile device entails different functionalities depending on whether a card reader is used and the security checks performed (verification of card expiry date, holder signature, PIN). This section looks at the functional processes for accepting cards on mobile phones used as payment terminals, with or without an associated external physical device.

1|1|1 Solutions where the mobile phone is not connected to a physical device

To collect payments by phone without a card reader, an application on the phone is used to reproduce an EPT interface. As when accepting online card-not-present (CNP) payments, the merchant must first be registered

1 Near Field Communication (NFC) is a protocol that is widely used for contactless payments (2009 Annual Report, chapter 3, p. 25). GPRS, 3G and Wifi networks employ wireless communication technologies that allow terminals to dialogue with the electronic payment servers used to acquire payment transactions.

2 Applications for managing affinity programmes are considered to be linked to transactions. However, they are not addressed in the following analysis.

3 Smartphones are mobile phones equipped with functions that go beyond telephony to include internet access, email, games and music. Although the same functions can be performed using other types of mobile device, such as ultra-portable laptops and touch screen tablets, this study concentrates on smartphones because of their high market penetration. In what follows, the terms telephone, mobile phone and smartphone will be used interchangeably.

with an acquiring bank or payment institution offering a transaction acquisition service. To collect payments, the merchant connects to a special website or opens an application (usually password-protected), then indicates the transaction amount. The holder is then asked to enter the card number[4] and expiry date, as well as the card verification number (CVx2[5]) provided that the acceptance network supports these added security measures.[6] The transaction unfolds as for a typical online payment. If there is no system for printing a receipt, one may be emailed provided that an address can be entered in the payment application.

This solution is extremely practical from the merchant's point of view because there is no need for an additional physical device to accept card payments using a phone. However, the payment process may be more cumbersome, since the card's 16-digit number as well as the three- or four-digit verification number,[7] where applicable, need to be entered on a touch screen. In addition, although the purchase is conducted with the card present at the time of payment, the transaction is considered to be the equivalent of a CNP transaction, which means that it does not offer the same guarantees as a face-to-face payment.

This system is already available in France. With Ogone's m-Terminal, for example, payment card information may be entered on a touch screen.

1|1|2 Solutions where the mobile phone is connected to a physical device

A number of new solutions has recently emerged in which the mobile phone is connected to a physical device, ranging from a simple card reader to a dock, and where data encryption is used to promote convergence between the functionalities offered by mobile phones and payment terminals.

Card readers

In contact mode

On North American and Asian markets, a range of solutions are now available – examples include Square, Intuit, Swiff, Payfirma, Simply Swipe It and Payware – in which the mobile phone is connected to a card reader. Once the service registration formalities have been completed,[8] the merchant must download the payment application to the phone, then enter a contract number along with the activation key mailed out when the merchant signed up for the service. Subsequently, to open the application, a personalised secret code must be entered that was chosen by the merchant when using the service for the first time. Taking a card payment entails the following steps: the merchant opens the payment application, connects the reader to the smartphone, enters an amount and then swipes the card's magnetic stripe using the reader. Once the stripe has been read and data consistency checks carried out, the holder validates the payment by signing on the phone touch screen.

Card identification and consistency checks may also be performed in a secure manner by means of a dialogue with EMV-compliant[9] cards. Information about the EMV migration process in Europe (see chapter 2) shows that virtually all smartcards have been migrated, meaning that they can dialogue securely with compatible terminals. As a result, EMV-compliant solutions to check card authenticity are emerging in certain European countries. Once again, the holder validates payment by signing the touch screen of the mobile terminal.[10]

In contactless mode

By inserting an NFC chip in a smartphone, it is possible for that device to communicate contactlessly

4 Some solutions allow a login to be associated with a pre-saved card number, particularly in the case of online e-purses.
5 MasterCard CVC2 (Card Verification Code) and Visa CVV2 (Card Verification Value).
6 Some card payment schemes use the CVx2 only for CNP sales.
7 Three digits for CB, Visa and MasterCard cards; four digits for American Express cards.
8 The same as those conducted in the case of a terminal without a physical reader.
9 Body comprising American Express, JCB, MasterCard and Visa.
10 This system does not require PIN entry and verification and thus does not meet the requirements of certain schemes (including the "CB" consortium) for the acceptance of face-to-face card payments.

with a card, which must also be fitted with an NFC chip. This connection may then be used in two ways:

- simplified mode: it can be used to automate the entry of card numbers in the context of an application as described in 1|1. Contactless communication makes the solution more user-friendly, because the holder does not have to re-enter card data;

- NFC technology can also be used by the card and smartphone as part of a conventional contactless payment: the dialogue between the card and the mobile device can then be used to implement the security processes applicable to this environment, such as EMV standards.

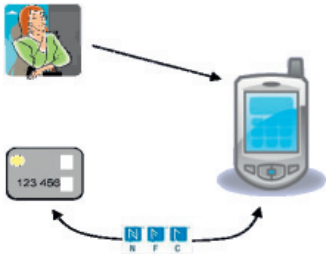
Card readers with data encryption

The most advanced stripe and chip readers include, in addition to the reading system used with the solutions described above, a cryptographic module to encrypt data before they are sent to the smartphone. Communications are thus encrypted end-to-end, and only the acquirer or the service provider operating the solution can decrypt the card data.

Box 1

Different approaches to using mobile phones as payment terminals

- ***No physical reader***



(card data are entered in contact or contactless mode)

- *With **stripe***

*or **chip card reader***

(data may or may not be encrypted by the physical device)

- *With a **dock***

(the overall unit offers functions very similar to those of a conventional payment terminal)

Docks

More sophisticated systems, such as Ingenico's iSMP solution, are positioned to compete directly with conventional payment terminals, since they include a smartcard reader, a dedicated keypad and optional receipt printing and barcode reading functionalities. These devices are similar to mobile phone docks. The reader and phone typically communicate through a mini USB connection or a proprietary jack (Apple type).

These terminals provide enhanced protection to the transaction environment by conducting cryptographic checks on card and holder authentication data directly on the peripheral device and not on mobile phone. The presence of secure elements, such as the dedicated keypad and the smartcard reading system, means, unsurprisingly, that these terminals cost more to manufacture. Proof of payment is provided to the holder either by printing a receipt, if the external system is fitted with a printing module, or by sending an email giving the transaction details.

1|2 Security issues linked to the use of mobile phones as payment terminals

1|2|1 Legal environment and standards applicable to acceptance

Legal environment applicable to payment card acceptance

The function of an EPT is to take card payments in accordance with the requirements laid down by the issuing network (such as the "CB" Bank Card Consortium, Visa or MasterCard) and agreed on by the acquirer (bank, payment institution, private network) and the acceptor in an acceptance agreement.

Since in France there are no legal or regulatory provisions defining what is meant by "acceptor", contractual provisions cover the possibility offered to individuals or entities of performing this function. The entry on the market of companies offering the solutions described in section I should therefore be analysed further by participants in the acquisition chain, to assess the appropriateness of the existing contractual framework with regards to the legal nature of the potential beneficiaries of these solutions.

The activity of these participants should also be assessed with respect to the provisions of the Payment Services Directive:[11] if these participants receive payments on an account in their name and then transfer the funds on to different beneficiaries, which would come under the heading of payment services as defined by point II of Article L. 314-1 of the *Monetary and Financial Code*, they should comply with the requirements for admission to the profession and obtain payment institution status.[12]

Terminal security standards and certification

Participants in the acceptance and acquisition of payment cards must comply with the security rules and standards set down by payment schemes. As regards cards and terminals, the schemes include these rules and standards in their processes for approving devices intended for holders and merchants.[13]

11 Directive 2077/64/EC of 13 november 2007.
12 Art. L. 522-6 of the *Monetary and Financial Code*.
13 See 2010 Annual Report, chapter 4, p. 41.

The security rules include PCI measures prepared by the Payment Card Industry Security Standards Council (PCI SSC).[14] These measures apply globally to all payment chain participants (banks, acquirers, merchants, service providers operating payment platforms, etc.) that participate in PCI member card payment schemes, both for cross-border transactions, but also for domestic transactions in the case of cards that are co-badged with a domestic card payment scheme.[15] Given their scope, these measures act as *de facto* standards.

PCI measures are designed to prevent card data from being stolen and fraudulently used. PCI SSC has drawn up several sets of rules, including PIN Transaction Security (PCI PTS) rules, which apply to terminal manufacturers and cover the security of systems that allow a PIN to be entered during point-of-sale card transactions. Payment Application Data Security Standard (PA DSS) rules, meanwhile, seek to protect applications used to store, process or transmit card data during authorisation and settlement processes.

The EPC[16] has also developed functional and security specifications, which are set out in its *SEPA Cards Standardisation Volume – Book of Requirements*. The security section draws on the above-mentioned PCI rules. These provide core requirements for all hardware (cards and terminals) used within SEPA.[17]

Furthermore, to ensure that cards and terminals attain a level of security that complies with current market standards, the EPC has begun discussions aimed at creating a harmonised certification framework in Europe for cards and terminals, based on a common evaluation methodology. The ultimate goal is to enable mutual recognition of certificates issued by different certification authorities and more generally to regulate the evaluation and certification process.

Among these authorities, the following are notably active in the area of terminals:

- EMVCo[18] for EMV standards, which have two compliance levels: Level 1 (interoperability between cards and acceptance terminals) and Level 2 (security rules that must be complied with once contact has been established between the chip and the terminal);
- PCI SSC for PCI specifications.

1|2|2 Security issues linked to the use of mobile phones in this environment

Card authentication

The card authentication mode depends on the hardware configuration.

No physical device

If the mobile phone is used on its own, the holder enters the card data (PAN – Primary Account Number, expiry date, CVx2) in the merchant's application. The card is authenticated by entering the CVx2, which, according to PCI rules, must not be stored either on the mobile phone or subsequently on the servers of the acquirer.

If the phone is connected to a reader

If the hardware configuration means that the mobile phone is set up like a payment terminal (i.e. connected to a card reader or dock), the target security level should be that of a face-to-face transaction. Currently, the only way to authenticate a card with certainty through proven cryptographic procedures is to have a chip, which, among other things, prevents data on magnetic stripes from being captured and used for fraudulent purposes.[19]

14 PCI SSC was set up by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International (see 2009 Annual Report, chapter 1, p. 9).
15 This is true for the majority of cards issued in France by the members of the "CB" Bank Card Consortium.
16 The European Payments Council, a body representing banks in Europe, is in charge of developing SEPA instruments.
17 Visa has also published *Visa Best Practices for Mobile Payment Acceptance Solutions* Version 1.0, which are also derived from the PCI rules.
18 EMVCo includes American Express, JCB, MasterCard and Visa.
19 A technique known as "skimming". See chapter 5 of the 2010 Annual Report.

Holder authentication

The holder authentication mode is closely linked to hardware configuration, as described in chapter 1.

No physical device

The transaction is akin to a CNP transaction, as mentioned above. Given the particularly high fraud rate for this category of transaction, enhanced cardholder authentication methods should be deployed, as the Observatory has been recommending since 2008.

If the phone is connected to a reader

Whether the card is authenticated using a stripe or a chip, entry of the holder's PIN is the only way to authenticate the holder with certainty. However, the use of a stripe card reader alone is not enough to meet SEPA security standards.[20] Communication between the card and the terminal must make it possible to establish a secure channel that is protected by cryptographic processes capable of guaranteeing the integrity and confidentiality of shared information, including the PIN.

In addition, PIN entry procedures must comply with certain rules, as mentioned above (card payment scheme best practices, EPC functional and security specifications, all based on compliance with PCI measures). Only terminals with secure keypads are eligible for PCI PTS certification. This is not the case for mobile phones, unless they are considered as a single unit with a dock that itself complies with the rules.

Protection of transaction data

The challenge is to protect transaction data (chiefly the card number, expiry date, PIN and any transaction certificates) shared by the communicating devices, i.e. the physical reader, mobile phone and acquisition servers.

Data held on the payment terminal

Some peripheral devices, such as stripe and chip card readers, send card data to the mobile phone via its analogue audio jack. To avoid the risks of data compromise during this phase, which is exposed to man-in-the-middle attacks,[21] the data must be protected by state-of-the-art cryptographic processes. Some systems have these functions built in and can encrypt the data when read using encryption modules, as mentioned above.

Next the data on the phone must be protected before they are sent to acquisition servers or payment concentrators. The main operating systems used on mobile terminals (Apple's iOS, Google's Android, Windows Phone, Nokia's Symbian, Samsung's Bada) have been designed with the general public in mind and strive to be accessible and user-friendly. For this reason, the security of the operating system, which is crucial to the protection of payment applications, is a weak link in the development of mobile payment applications. Moreover, since these applications can be downloaded remotely onto mobile phones, acceptors are exposed to the risk of distributing false payment applications that are actually designed to steal cardholders' confidential data.

To address this lack of protection, additional measures could be taken to guard against the risks of compromise for mobile terminals. This could be achieved, for example, through a policy of controlling access to mobile phone system resources and the possibility of encrypting data on mobile phones. In addition, an application isolation and signature mechanism could round out the security arrangements guaranteeing the quality and integrity of payment applications.

This type of security mechanism seems particularly important for payment applications because these applications are not eligible for PCI SSC certification. In June 2011, PCI SSC conducted an examination of

20 One of the requirements of the SEPA Card Framework is that EMV standards must be used.
21 This type of attack consists in intercepting the data between an issuer and a receiver without their knowledge.

the risks associated with accepting card payments on mobile phones in the context of PA-DSS validation. The analysis concluded that mobile applications that were eligible for PA-DSS certification were strictly confined to:

• terminals complying with PCI PTS standards (currently on version 3.1), i.e. capable of strictly separating payment-related functions and protecting PIN entry. This would include conventional payment terminals currently on the market and exclude mobile phones;

• mobile phones that are designed specifically for payment acceptance and that are delivered by the manufacturer with an in-built application. These environments by definition have a higher security level.

Currently, no smartphone available in France is eligible to apply for PCI certification. Accordingly, all stakeholders need to study the possibility of using such devices to take payments, by conducting special risk analyses to reassess the level of security requirements applicable to each payment situation.

Between the mobile phone and the acquirer's servers

Since the issue is the same for all mobile terminals, the security of communications between mobile terminals, payment concentrators and acquisition servers is a subject on which the Observatory has previously issued recommendations in earlier reports.[22] These recommendations also apply to the use of mobile phones as acceptance terminals.

Because the use of open networks based on the Internet Protocol (IP) involves numerous interconnected operators, there is a risk of data compromise. To ensure data confidentiality and integrity, end-to-end protection for communications must be implemented, such as that provided by VPNs.[23] SSLv3[24] is usually used to provide protection for open networks that are accessible by mobile phone. Implementing these measures is the only way to protect against the risk of transaction data being intercepted and modified for fraudulent purposes.

1|3 Conclusion

The payment terminals market has witnessed many developments in recent months, with the emergence of solutions using advanced mobile devices, in particular smartphones. These solutions involve the use of secure websites or applications that are downloaded onto the mobile phone, which may be connected to a stripe or chip reader, or even a dock.

Since smartphones are by definition multi-application, multi-task devices without secure elements, they seem at first glance fairly incompatible with the requirements usually placed on conventional payment terminals, which are designed specifically for the function.

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

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

22 2008 Annual Report (security of UPT networks) and 2009 Annual Report (security of "thin" payment terminals).
23 Virtual Private Networks, which offer end-to-end data encryption.
24 Secure Socket Layer version 3. Its successor, Transport Layer Security (TLS) versions 1 and higher, is also suitable, of course.

2| Digital wallets and card payments

Card payments, which were initially developed to meet the needs of face-to-face transactions, have evolved over recent years, with the development of card-not-present (CNP) sales generally and online commerce in particular. These changes raise new usage-related issues, notably because:

- cards may be awkward to use online, since the holder has to manually enter the 16-digit card number, expiry date and verification number;

- holders may be reluctant to share their card information for fear that it might be stolen and used for fraudulent purposes.

"Alternative" payment solutions have emerged to address these problems. The following study considers alternative solutions that take the form of digital wallets, defined as solutions that allow the user to provide a trusted third party with payment and personal data, which are stored for later use, notably to place payment orders.

These solutions make it possible to perform a payment transaction by entering identifiers, such as a mobile phone number or email address, and without having to re-enter sensitive information such as account or card data each time a transaction is carried out.

In keeping with the mandate entrusted to the Observatory, this study considers only digital wallets that may be used to make card payments, although other payment instruments may also be supported. After briefly reviewing the characteristics of these alternative payment solutions, the study analyses security aspects, notably protection of card data and user authentication, as well as their impact on payment chain participants. The study does not seek to describe the legal framework applicable to digital wallets, including the scope of participants' respective responsibilities.

2|1 Digital wallets and the risks to which they are exposed

2|1|1 Solutions covered by this study

The solutions reviewed by this study include digital wallets offered by:

- firms that specialise in online payment services, such as Paypal and FiaNet through the Kwixo service;

- more conventional firms, such as Crédit Mutuel, with its Pay2You products;

- phone companies, via the Buyster service;

- card payment schemes, such as *Cartes Bancaires*, Visa and MasterCard.

Many of these wallets are widely accepted. However, they may also be offered and accepted only by a single merchant, for example if the wallet is designed to hold card numbers with the merchant so that customers do not have to re-enter them when making payments.[25] Examples include the solutions provided by Fnac and Amazon.

2|1|2 Using a digital wallet

To use a digital wallet the user must first sign up for the service. This is usually done online. The user is asked to enter:

- personal information: address, phone number, email, etc.;

- card data: number and expiry date of one or more payment cards.[26]

Once the data are saved, the user is given identifiers that allow access, comprising a login (usually a phone number or email address) and a password. These identifiers are subsequently used to make payments to merchants that accept the payment solution.

25 This is usually called a one-click service.
26 Or the user's bank details if services are extended to include transfers and direct debits, which are not addressed by this study.

A digital wallet may be used to make person-to-person transfers. Such transfers are initiated in the same way as payments to merchants, so they involve similar security measures and processes.

A digital wallet may also be used to put funds in an electronic money account.[27] This option allows the payment service provider to keep on its books flows linked to users' payment transactions. Managers of such accounts must then usually be authorised as a credit institution or electronic money institution.

2|1|3 Risks to alternative payment solutions

These types of solutions are exposed to various risks, relating to the storage of sensitive data (account or card data) and the reuse of these data without the knowledge of the rightful holder.

Compromise of card data following an attack on digital wallet servers

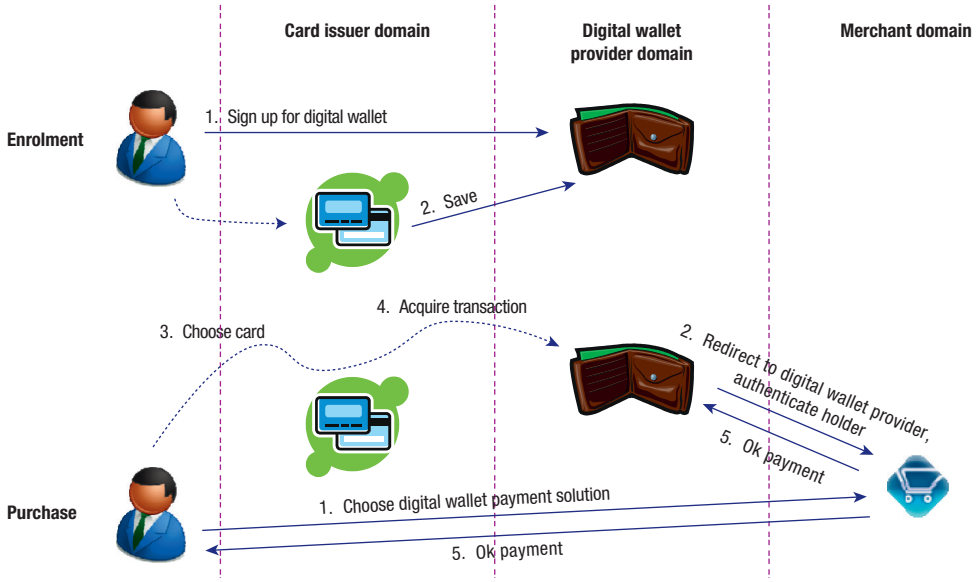
Providers of digital wallet solutions have to store the data saved by users. These data include identity and payment information, including users' payment card numbers. The fact that these data are concentrated in one place makes them a target for crime rings looking for large volumes of information. Providers of these solutions have been the victims of data theft in the past.[28]

Saving fraudulent card data in a digital wallet

If the level of security is not sufficiently high at enrolment, criminals could legitimately sign up for digital wallets and use them to save cards whose data have been compromised.

Box 2

Using a digital wallet



27 Generally called an electronic purse.
28 In April 2011, for example, two million payment card numbers were stolen from Sony's Playstation Network.

Fraudulent use of digital wallet

Theft of the identifiers needed to use a digital wallet would give access to the payment instruments saved in the wallet. The wallet's protection level must therefore be sufficiently high to ward off fraud aimed at using the wallet without the knowledge of the rightful holder.

2|2 Security issues raised by alternative payment solutions and impacts on participants

2|2|1 Security measures

Given the risks described above, providers of digital wallets need to implement security measures to protect sensitive data and verify the identity of holders both when they save payment cards and when they use their wallets.

Protecting sensitive data

The saving and storing of payment card data are subject to security rules drawn up by PCI-SSC.[29] The rules are set down in PCI-DSS[30] measures, which seek to protect the data transmitted through or stored in the information systems of the acquisition chain. These measures must therefore be complied with when a provider stores card data on its servers. Compliance with PCI rules is assessed through a certification process conducted by PCI-SSC-approved organisations.

In France, in accordance with Data Privacy Act 78-17, these processing operations must also be reported in advance to the CNIL,[31] which will check disclosure arrangements and the consequences of implementing these processing operations.

Finally, careful consideration should be given to the distribution of responsibilities between the parties involved in the payment solution. Responsibility may lie with the merchant, the technical provider or the acquirer. Relations between these parties should be set down formally to clarify each participant's respective responsibilities.

Saving cards

Criminals target payment instruments with the lowest levels of protection. Fraud may shift to sites that accept payments by digital wallets if the data of compromised cards can be stored in wallets that are legitimately opened by criminals.

For this reason, steps must be taken to ensure that the cardholder is indeed who he or she claims to be at the time when the card data are saved in the digital wallet and that the holder of the wallet is indeed the rightful holder of the payment instruments that he or she wants to include in the wallet. Providers of digital wallets therefore need to implement a variety of solutions to safeguard integrity when data are saved and to combat the risk of fraudulent use of digital wallet (see above).

The Observatory thus recommends that digital wallet providers arrange for enhanced authentication of the holder by the card issuer using one-time solutions,[32] which may be based on security protocols such as 3D-Secure or equivalents.

Note in addition that some digital wallet providers include additional security measures to limit the risks of fraudulent use of wallets in the first few months:

- some providers ask customers to carry out a card transaction with a randomly selected small value, which must be confirmed by the holder to ensure that the holder does indeed have access to transaction statements for the card in question. This solution does however have the drawback for the holder of having to initiate a transaction without knowing the amount;

- other providers track the operation of the wallet for a set period before lifting certain thresholds imposed at the beginning.

29 The Payment Card Industry Security Standard Council, which is made up of the founding schemes, namely American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.
30 PCI – Data Security Standard, see chapter 1, 2009 Annual Report.
31 France's Data Privacy Agency. See *http://www.cnil.fr/*.
32 See 2010 Annual Report, chapter 3, p. 39.

Fraudulent use of digital wallets

If identifier information is stolen (see above), the holder should be protected against fraudulent use of payment instruments saved in the digital wallet.

The Observatory recommends that digital wallet providers do the following:

- conduct risk analyses to determine whether payment transactions have been carried out under unusual circumstances that might cause them to be blocked. Naturally, such analyses would be linked to the use made of digital wallets under the provider's responsibility;[33]

- apply one-time authentication systems, either in all cases or based on the above-mentioned risk analyses. Ideally, this authentication would be conducted by contacting the issuer of the card contained in the wallet, or at least by using a means of authentication (mobile phone number for example) whose security is guaranteed by the digital wallet provider.[34]

2|2|2 Impacts on payment chain participants

In France,[35] the standard rules in the *Monetary and Financial Code* for managing payment instruments apply to payment transactions performed using digital wallet solutions, notably in terms of:

- consent to execute a payment transaction;

- irrevocability of payment orders;

- the deadline for executing payment transactions in value dates;

- refunds for improperly executed or unauthorised transactions.

The holder may save payment cards in the wallet that were issued by a different institution from the wallet provider. If a fraudulent transaction is perpetrated in this setting, the holder is bound by contractual obligations:

- under the contract between the holder and the card issuer, to which the holder must report any unauthorised use of the payment instrument;

- under the general terms of use of the digital wallet provider, which also include the requirement to report fraudulent use of the payment instrument.

The digital wallet provider may be liable for a fraudulent transaction if the point of compromise falls within its scope of responsibility. Moreover, the steps that users need to take to contact the card issuer and/or wallet provider to dispute a transaction must be clearly indicated.

The Observatory recommends that digital wallet providers take steps to ensure contractual transparency and compliance with respect to users as regards saving and using payment instruments within their solution.

Furthermore, the Observatory recommends that digital wallet providers and issuers introduce technical and organisational measures to ensure the traceability of transactions conducted using digital wallets. In particular, holders should be able to identify payees.

33 Example criteria: unusual amount, high risk profile, unverified account, etc.
34 In particular with protection when saving, changing or updating this means of authentication.
35 For transactions outside Europe, see the 2009 Annual Report, Annex A, p. 55.

2|3 Conclusion

The emergence of digital wallets is contributing to the increased diversity of payment solutions by providing users with resources that are tailored to their uses. However, the growing array of options must not come at the cost of the security of payment instruments, which could undermine confidence in existing means of payment and prompt fraud to shift to less well-protected solutions.

For these reasons, the Observatory recommends the following:

- all participants should implement measures to protect sensitive data (including data linked to payment cards);

- digital wallet providers should use systems to enable one-time authentication of the holder by the issuer when the card is saved in the wallet;

- digital wallet providers should conduct risk analyses resulting in one-time authentication for payments that are viewed as risky.

Finally, contractual transparency must be ensured as the use of digital wallets grows. The provision of payment instruments, particularly at a time when CNP and face-to-face uses are converging, requires clear rules for the management of payment instruments and transactions. Also, responsibilities must be defined and shared between users, merchants and the providers of such solutions.

3| Progress on the migration to EMV

The implementation of the EMV ("Europay, MasterCard, Visa") specifications for chip cards in Europe represents a major issue in the fight against cross-border fraud. It concerns both cards themselves and accepting systems (payment terminals, ATMs, UPTs), which need to migrate to the new specifications in order to achieve a uniform level of protection throughout Europe. As it has done in the past seven years, the Observatory measured the progress on EMV migration by collecting statistics on the migration process in France and Europe from the "CB" Bank Card Consortium and the European Payments Council (EPC). These figures show that the migration process is mostly complete throughout Europe, although European banks within the EPC are slightly behind on their commitment to complete migration by the end of 2010.

3|1 Progress on the migration to EMV in France

Migration to the EMV standards is practically complete in France. By the end of March 2012, according to statistics compiled by the "CB" Bank Card Consortium, 100% of "CB" cards, 99.5% of payment terminals and UPTs, and 100% of ATMs were EMV-compliant. The remaining 0.5% of terminals and UPTs, which are rarely used, will migrate at the time of their normal replacement.

3|2 Progress on the migration to EMV in Europe

In Europe, according to the data provided by the EPC for the period going up to the end of March 2012, 87.8% of the four-party cards in use in the 27 countries of the European Union are now EMV-compliant. This represents an increase of 2.2 percentage points in comparison with March 2011, after last year's strong 15.8 point increase, as several of the least advanced countries caught up. The actual situation varies from country to country (see Box 3). Whereas efforts to achieve compliance with SEPA interoperability rules began from early 2008 onwards, several countries still lag well behind the rest. However, the majority of cards are now EMV-compliant in all EU countries.[36]

36 Except Poland, for which the EPC lacks recent data.

EMV card deployment remains markedly higher in the countries of Northern Europe.

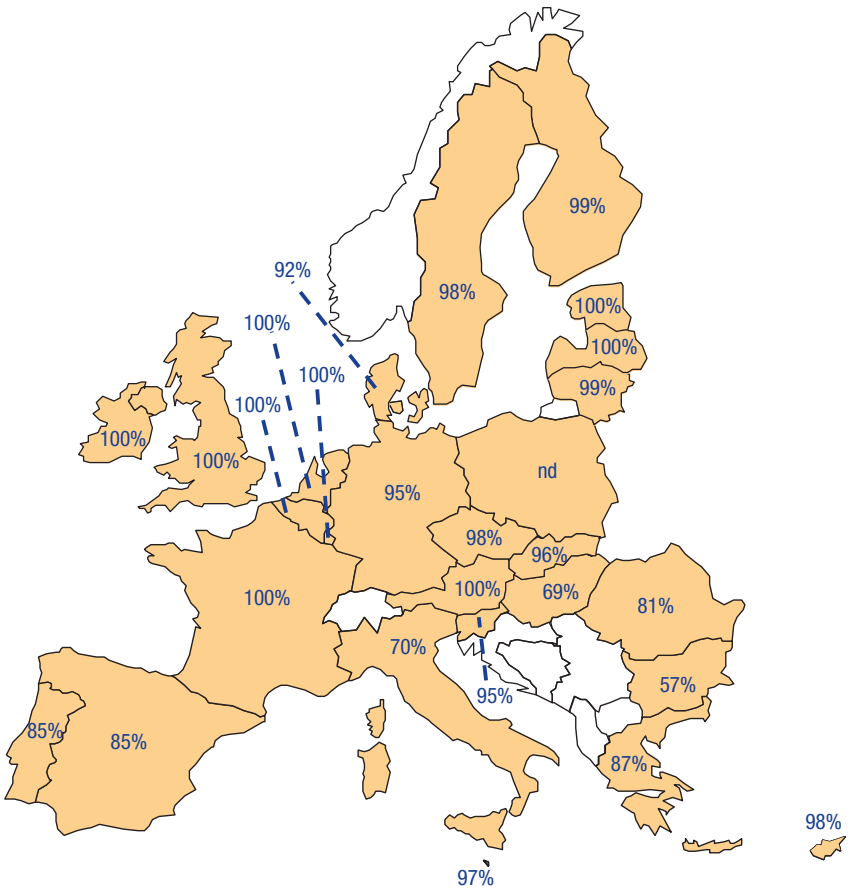
On the acquisition side, the migration to EMV progressed at a slower pace than in previous years, but is now well advanced: at end-March 2012, 94.5% of payment terminals (see Box 4) and 96.7% of ATMs (see Box 5) were EMV-compliant. This represents an increase of 2.5 percentage points for payment terminals and 0.1 of a point for ATMs in comparison with March 2011. There are no longer material differences between the countries of Southern Europe, where the migration process was much faster, and those of Northern Europe.

Countries nearing completion of the migration process may encounter problems replacing the last segments of acceptance systems that are infrequently used.

The migration of ATMs is virtually complete in most countries.[37]

Box 3

Deployment of EMV cards in Europe

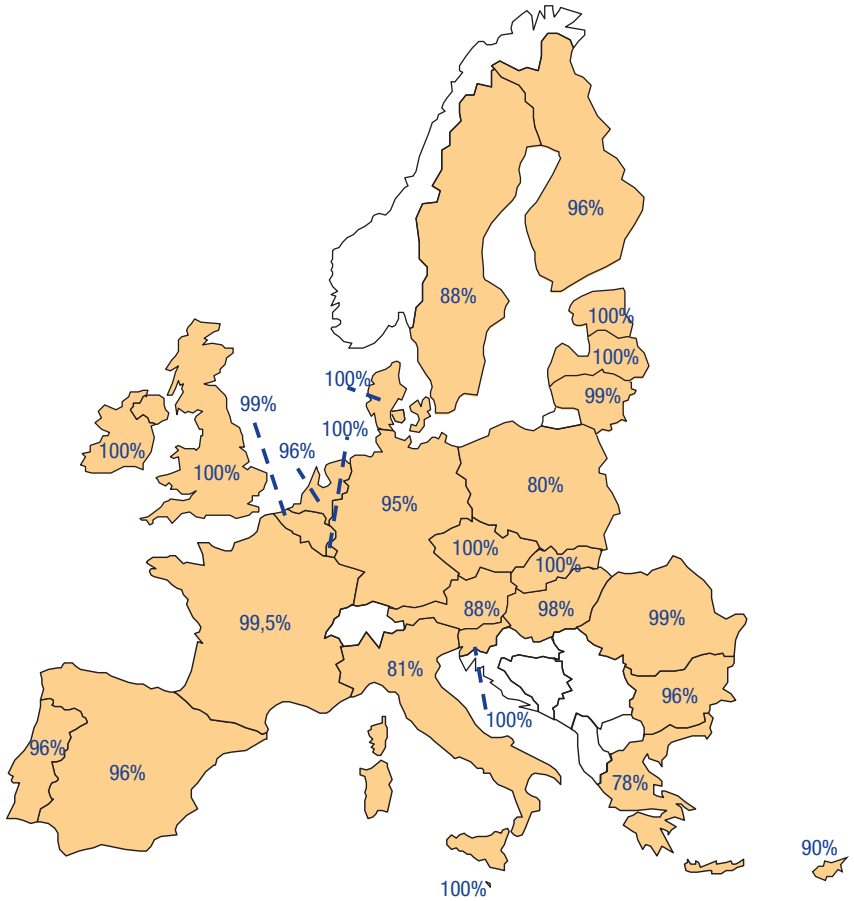


Source: European Payments Council – March 2012.

37 Note that the EPC does not have updated data for Italy. The statistics provided should therefore be treated with caution.

Box 4

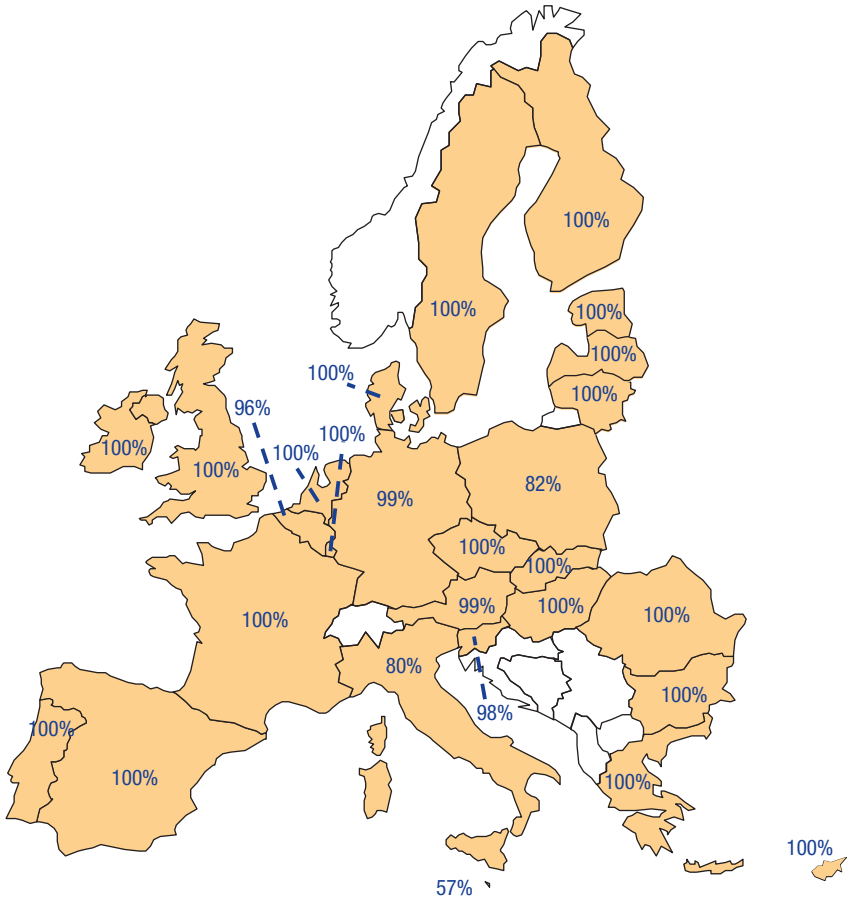
Deployment of EMV terminals and UPTs in Europe



Source: European Payments Council – March 2012.

Box 5

Deployment of EMV ATMs in Europe



Source: European Payments Council – March 2012.

International cooperation in the fight against fraud

One of the tasks assigned to the Observatory is to prepare fraud statistics and to issue recommendations to payment chain participants to prevent fraud. Given the European and even global nature of the payment card market, the scope of these recommendations now goes beyond the domestic setting, and the Observatory's actions form part of a wider international drive to harmonise security measures.

In light of the financial stakes and the sophisticated techniques now being employed, the fight against payment card fraud is a top priority both in France and internationally. As part of its 2011 Annual Report, the Observatory therefore decided to conduct a review of participants in the domestic anti-fraud effort and describe international cooperation arrangements.

This study was conducted using information gathered from representatives of relevant government agencies, specialised domestic, European and international bodies, and the banking sector.

1| The fight against fraud: participants pursue different but complementary objectives

The Observatory's review reveals that many participants are involved in the fight against fraud. Their approaches differ depending on where they are in the payment chain, with the result that all the main issues are addressed, from preventing fraud and ensuring that components are at the requisite technical level, to dismantling rings when fraud is discovered, and, in the case of supervisors and overseers, maintaining confidence in cards as a means of payment.

1|1 Credit institutions want to limit the financial impact of fraud

Issuers and acquirers of payment cards generally bear the financial costs of fraud and have therefore built this risk into their security policies.

According to them, two subjects require special attention: risk linked to the use of forged or counterfeit cards and the risk that card numbers could be misappropriated and used, especially online.

Issuers and acquirers thus play an active part in developing innovative technologies to combat these types of fraud. Major projects in this regard include the migration to EMV standards,[1] which addresses the first risk, and the deployment of one-time authentication,[2] which addresses the second.

Credit institutions have also developed transaction scoring tools, which receive daily data on authorisations and collections of card payment transactions to monitor fraud trends. These systems are continually being enhanced and modified, and enable banks to respond quickly if anomalies arise. However, they are based on the historical transaction data held by the individual institution, which may only have a partial view of the card market in France and abroad. Domestic and international card payment schemes therefore play a vital role by making it possible to gain a broader view of fraud.

Surveillance and incident response services delivered by computer security incident response teams (CSIRTs) and computer emergency response team (CERTs) round out the framework. These specialised firms provide cutting-edge technical expertise, particularly to banks, to deal with threats to networks (Internet) or to software used in corporate information systems. Some banks also have these resources in-house.

1 The migration to EMV standards was the subject of a study in the 2010 Annual Report, chapter 1, p. 11.
2 See the 2010 Annual Report, chapter 3, p. 33 and the 2011 Annual Report, chapter 1, p. 13.

1|2 The need to ensure the technical security of components

The security of payment cards is based on the advanced technology of their components.[3] These components have to be regularly reviewed to make sure that they are still state-of-the-art and capable of withstanding increasingly sophisticated attacks by criminals.

In France, to ensure that this is the case, independent security certification and evaluation schemes are in place for payment cards and acceptance terminals used by card payment schemes. The card payment schemes have integrated the certification and evaluation schemes within their processes for authorising the components that are allowed to operate on their networks. The *Cartes Bancaires* ("CB") payment scheme, for example, uses a security certification scheme supervised by ANSSI[4] for cards, and another one run by PayCert and dedicated to terminals.

These two schemes in turn rely on a small group of authorised testing firms, which ANSSI and PayCert regularly review to ensure that they still possess the high skill levels required. Card components, for example, are tested at special Information Technology Security Evaluation Centres (CESTIs), of which there are three in France (Leti, Serma and Thales). Elitt, another testing firm, has built up expertise in evaluating acceptance terminals. Once certified, products are regularly assessed over their life to ensure that they are able to withstand new forms of attack.

1|3 Investigating and dismantling crime rings

Since the payment card is a widely accepted means of payment in France, its unlawful use in money laundering, terrorist financing and fraud more generally creates the need for nationwide warning mechanisms, and well-organised, extremely expert teams to respond to these types of activities.

Tracfin, which reports to the Ministry of the Economy, Finance and External Trade, is responsible for combating illegal financial networks, money laundering and terrorist financing. To this end, it receives suspicious transaction reports (STRs) from financial institutions. Tracfin may forward this information to the public prosecutor's office if its own investigations confirm the suspicions.

France's law enforcement agencies are organised into different levels, which has resulted in the establishment of a number of specialised units:

• within the Central Directorate of the National Police Force's Criminal Investigation Division, the Sub-Directorate for the Prevention of Organised and Financial Crime (SDLCODF) is responsible for intelligence, strategic analysis and relations with government agencies on, among other things, specialised crime. The sub-directorate itself therefore comprises several central offices, some of which have an active role in the fight against payment fraud, such as the Central Office for the Prevention of Major Financial Crime (OCRGDF) and the Central Office for the Prevention of Information and Communication Technology Crime (OCLCTIC), which is in charge of the Central Unit for the Prevention of Payment Card Counterfeiting (BCRCCP);

• within the *Gendarmerie nationale*, which is actually a branch of the French armed forces, the Technical Unit for Judicial Research and Documentation comprises a Finance Division and an Anti-Cybercrime Division, which is responsible for centralising and using judicial information on crimes and offences. These two divisions are heavily involved in the fight against payment card fraud;

• these specialised departments are aided by units offering technical expertise, including the National Police Force's Central Unit for IT and Technological

3 For cards, those components encompass chipsets and payment applications embedded into them. For terminals, operating systems are also included in the perimeter.

4 The National Agency for Information Systems Security. ANSSI has a national mandate covering the security of information systems. In this regard, the agency is in charge of defining and verifying the application of standards regarding the protection of government related information systems. One of its missions is to provide services for monitoring, detecting, issuing warnings about and responding to IT attacks, notably against government networks. ANSSI can provide expertise and technical assistance to government agencies and companies that are deemed to be critical because of the products or services that they supply. It may thus be asked to provide assistance if new types of fraud arise.

Evidence and the Engineering and Digital Crime Division of the Crime Research Institute, which is part of the *Gendarmerie nationale*. These units conduct technical investigations using highly sophisticated techniques.

This organisation is supported on the ground, at police and *Gendarmerie* level, by digital technologies investigators (NTECHs) and cybercrime investigators (ICCs), who have specific training in new technology crimes.

1|4 Supervisors and overseers want to maintain confidence in cards as a payment instrument and licensed payment service providers

In France, the Banque de France is responsible for overseeing cashless payment instruments, by virtue of the provisions of the *Monetary and Financial Code* (Article L. 141-4 *et seq.*).

The primary objective of the Banque de France is thus to maintain confidence in the use of payment instruments, including cards, by promoting the adoption of best security practices by all participants in a uniform manner throughout the country.

To achieve this, the Banque de France conducts risk analyses for each instrument and prepares security frameworks. Through documentary audits and on-site inspections, it ensures that participants and their technical providers comply with these frameworks. Where applicable, it may recommend that reporting entities implement security measures to prevent fraud. In the area of payment cards, the Banque de France carried out an assessment of all domestic card payment schemes active in France in 2008/2009. It also made several important recommendations to payment chain participants, including the recommendation to deploy one-time authentication to protect online banking websites and online card payments in 2008, and the recommendation to enhance the security of the CB scheme's EMV smartcards in 2006 (switch to Dynamic Data Authentication – DDA – technology to fight more effectively against payment card counterfeiting).

Furthermore licensed payment service providers fall under the supervision of the French *Autorité de contrôle prudentiel* (ACP), especially with regard to operational risk generated by the provision and management of payment instruments (Articles L612-1 and 612-2 of the *Monetary and Financial Code*).

2| A need for cooperation between participants

Thus, banks (and payment service providers more generally), law enforcement agencies, certification bodies, testing firms and banking authorities all play an active part in preventing fraud at domestic, European and international level. To ensure that counter measures are effective as possible, participants realised that they needed to establish cooperation systems.

2|1 Banks cooperate at many levels

Banks in France belong to the French Banking Federation (FBF), which represents the French banking community within the European Banking Federation (FBE), which in turn upholds European positions at meetings of the International Banking Federation (IbFed). This pyramidal organisation enables financial institutions to share information at international level and establish shared positions, including in the area of security.

Cooperation between banks within Europe is conducted chiefly within the context of the Single European Payments Area (SEPA) initiative.[5] Thus within SEPA, in 2003 Europe's banks created the European Payments Council (EPC), which is a forum for the industry to exchange information and coordinate actions. The EPC is organised into working groups devoted to different payment instruments and covering security and anti-fraud issues, on a cross-cutting basis where appropriate.

5 The goal of the Single Euro Payments Area (SEPA) initiative is to create an integrated European payments market and thus to harmonise retail payments in euros so that they are carried out under the same conditions of security, efficiency and cost.

Depending on the topic, organisations from outside the banking sector, such as Europol, may be asked to provide input to broaden the debate.

At international level, banks may hold discussions about fraud in the context of standard setting, notably within ISO, which created a technical committee for this purpose.[6]

In the area of card transactions, in 1984 the French banking sector formed an economic interest group, called GIE Cartes Bancaires, which became the "CB" card payment scheme's governance authority and centre for operations and technical expertise. The creation of the interest group thus effectively led to the interoperability of bank networks in France, based on payment cards.

Until now, all card payment transactions have been conducted via a single interbank authorisation network, which was initially run by GIE Cartes Bancaires but then turned into a subsidiary in 2009.[7] This entity therefore occupies a central position in the operational fight against fraud.

GIE Cartes Bancaires has accordingly introduced tools to identify potentially fraudulent transactions and detect points of compromise. By virtue of its strategic position, it collaborates closely with law enforcement to provide evidence, particularly during investigations. The international networks, notably Visa, MasterCard and Amex, have developed similar tools for their members.

Regardless of the actual setup eventually determined by the relevant market players, it is essential that cooperation in the fight against fraud should be organised efficiently, especially by ensuring that information sharing between them does take place. It should be the case when the announced move to phase out the technical gateways between the "CB" scheme and the Visa and MasterCard schemes becomes effective for cross-border transactions initiated in France.

2|2 Technical cooperation: room for progress at international level

2|2|1 A handful of organisations working on technical cooperation

Within Europe, technical cooperation is primarily handled by government agencies directly in charge of the security of information systems. Indeed, existing European structures in this field have a limited impact:

• ENISA[8] is tasked with helping Member States in setting up structures and frameworks dedicated to information system security and cybercrime. ENISA generally issues technical guides that can be used as standards;

• CERT-EU is the CERT for European institutions, currently under construction and which plays an operational role in the field of cybercrime, but only for those institutions.

International structures have also been set up to allow participants to exchange information on specific issues, such as the compromise of ATMs or payment terminals. The EAST[9] group illustrates how market participants have pooled resources to promote and harmonise best practices in ATM security.

2|2|2 Certification: illustrating a real need for harmonisation on the international scene

Technical cooperation is effective in the area of hardware certification,[10] aimed at preventing the risks of fraud but also at facilitating matters for

6 TC 247 – Fraud counter-measures and controls, which is responsible for standardisation in the area of detection, prevention and control of identity, financial, product and other forms of social and economic fraud.
7 The e-rsb network, now run by a subsidiary known as *Société d'Exploitation de Réseaux et de Services Sécurisés* (Ser2S).
8 European Network and Information Security Agency, which comprises experts in the field of information and communications, industry representatives and researchers doing work on information security and networks.
9 European ATM Security Team, a non-profit group comprising card payment schemes (GIE Cartes Bancaires in France), processors and banks.
10 See the study on certification in France and Europe contained in the 2008 Annual Report, chapter 4, p. 45.

solution providers. However, more effort needs to be made, particularly at European level.

Two initiatives, addressing different areas, are worth noting:

• domestic certification schemes, under the supervision of government agencies such as ANSSI and its foreign counterparts, were quick to adopt open evaluation and certification processes along with a methodological framework relying on an international ISO standard,[11] known as the Common Criteria. To enable mutual recognition of certificates and of evaluations by accredited testing firms operating within the schemes, European Union Member States implemented recognition agreements, known as the Senior Officials Group – Information Systems Security (SOG-IS) agreement and the Common Criteria Recognition Agreement (CCRA).

This mechanism is now operational for card components, and is recognised by the Visa and MasterCard schemes.

• the international card payment schemes (Visa, MasterCard and Amex in particular) also moved quickly to collaborate within special structures devoted to cards (EMV[12] Co) and to protecting sensitive transaction-related data (PCI SSC[13]). While EMV certifications are primarily functional and do not seek to test the robustness of card components from a security perspective, PCI standards are dedicated to the card payment acceptance chain and include an evaluation by an authorised testing firm, which is followed by certification from PCI SSC.

Currently, PCI standards prevail for the certification of acceptance terminals.

While these two initiatives are different, they are increasingly converging, owing to developments over recent years:

• some Common Criteria working groups are addressing terminal certification and include the main PCI members (Visa, MasterCard, American Express), alongside government agencies, most of the domestic payment schemes, including the Groupement des Cartes Bancaires "CB", and many providers and manufacturers of solutions.

The domestic certification schemes and PCI SSC thus benefit from shared expertise on terminal attacks and security measures.

• owing to the presence of numerous domestic payment schemes in addition to the international networks, there is a strong need in Europe to simplify the non-standardised approaches to card and terminal certification. While the EPC is leaning towards the CC methodology for cards, work on CC/PCI convergence is still ongoing as regards the certification of acceptance terminals.

The EPC is also struggling to create a governance body[14] that is capable of organising the mutual recognition of functional and security certificates issued to card, terminal manufacturers and potentially to manufacturers of other devices involved in the card payment chain. This project has been supported since its inception by bank regulators as a way to harmonise the security level of components at European level.

2|3 Cooperation in enforcement that draws on well-established structures

2|3|1 Clearly defined mechanisms for cooperation at domestic, European and international level

In France, many law enforcement departments are led to investigate cases where payment cards are used illegally to commit crimes. The work of

11 ISO 15408 "Information technology, security techniques, evaluation criteria for IT security".
12 Europay MasterCard Visa, see 2010 Annual Report, chapter 1, p. 19.
13 Payment Card Industry Security Standard Council, see 2009 Annual Report, chapter 1, p. 9.
14 SEPA Card Certification Management Body (SCCMB).

these departments on the ground is supported by two levels of cooperation:

• in terms of enforcement, the central offices handle police and judicial cooperation. Specifically in the area of payment cards, OCLCTIC leads and coordinates operational measures against the perpetrators of these crimes at the nationwide level. As such, OCLCTIC coordinates police and *gendarmerie* units and maintains relations with other government agencies (customs, tax, etc.), the banking sector, consumer protection associations, and schools and universities, particularly on research. These offices also act as the points of contact for international cooperation. In this capacity, they collaborate with specialised foreign units and are the key talking partners in exchanges with Europol and Interpol;

• in terms of information-sharing at national level, the Department for Information, Intelligence and Strategic Analysis of Organised Crime (SIRASCO), an inter-ministerial department housed within the Central Directorate of the National Police Force's Criminal Investigation Division, is in charge of intelligence and strategic analysis of organised crime. SIRASCO cooperates with Tracfin in the financial field, but also with all the other central offices that might be involved, including OCLCTIC.

At European level, Europol[15] was set up in 1995 to organise cooperation, and became a European agency in 2010.[16] Europol has several benefits for Member States:

• its role is to help support law enforcement agencies in Europe by exchanging and analysing information on criminal activity. In addition to preventing terrorism and all forms of trafficking, Europol also works to combat the fraudulent use of payment cards;

• in this capacity, the agency has created a database designed to gather information on card-related fraud, and specifically on counterfeiting, notably to identify organised networks operating in several countries. Data sharing is supported by a dedicated, secure information system, called SIENA, which collects information from Member States. These data are used to perform operational analyses to reveal key links in cross-border investigations and identify priorities for anti-crime measures. This makes it easier for Member States to engage in coordinated initiatives.

Globally, the International Criminal Police Organisation, better known as Interpol, was created in 1923. Like Europol, Interpol aims to facilitate cooperation between its 188 members:

• Interpol's main task is to provide countries with a platform for sharing and analysing intelligence on crime and to highlight links between reported acts. Payment card fraud is specifically addressed by Interpol's cybercrime working group;

• to carry out its missions, Interpol has a centralised secure information system (I-24/7) that may be accessed by members. The system is backed up by an operational support team, which can quickly dispatch specialised units in the event of a serious offence. Members can also take advantage of Interpol's training centre.

2|3|2 Special networks and structures make the system even more effective

Other networks and structures have been created, both at the operational level of counter-crime measures, as well as in an effort to enhance the information gathered by organisations such as Europol and Interpol. These groups contribute, among other things, to the fight against payment card fraud:

• at the operational level, on the initiative of the G8 and following the attacks of 11 September 2001 in the USA, a network of 58 countries (G8 H24) was set up to put investigative forces in direct contact with each other to respond to urgent requests to freeze digital data and prevent evidence from being destroyed or removed;

15 European Union Law Enforcement Organisation.
16 At that time, its mandate and resources were strengthened.

• the United Nations has set up a special anti-terrorist team, which acts as a forum for liaison and exchange, and whose purpose is to assist countries in implementing international standards in this area. This structure comprises various UN entities and is in contact with Interpol, notably to fight against fraud related to payment instruments used in the financing of terrorism;

• in Europe, the European Convention on Mutual Assistance in Criminal Matters[17] includes the option for Member States to set up joint investigation teams. Within this context, the judicial authorities and investigation units of signatory countries may exchange specific information, conduct joint investigations and coordinate criminal proceedings between countries involved in the same case. Similarly, the Anti-Fraud Office, which is, among other things, responsible for protecting the financial interests of the EU against fraud, corruption and all other illegal activities, funds programmes to prevent payment fraud. Payment cards occupy an important place in such programmes, owing to their widespread use in Europe.

2|4 Cooperation between bank regulators is in place at European level, but has yet to be implemented internationally

While intra-sector cooperation is essential in the fight against fraud, inter-sector cooperation is also needed to ensure maximum efficiency. In the area of payment cards, bank regulators can play a vital role in organising this type of cooperation.

2|4|1 The Observatory for Payment Card Security, a model for cooperation

In France, the Observatory for Payment Card Security occupies a very special place. It includes representatives of central government, the banking overseer and supervisor, government agencies, payment card issuers, card payment schemes, consumers and merchants. The Observatory thus ensures that all market stakeholders are properly represented and provides a forum for discussing all topics of general interest.

By establishing a system for the statistical monitoring of fraud and conducting a technology watch, the Observatory has since its inception in 2002 played a major part in deploying and monitoring security systems for payment cards in France and hence in maintaining a high level of confidence in cards as payment instruments.

Its work has informed the thinking of numerous European players and its operational model was the inspiration for the European Forum on the Security of Retail Payments, or SecuRe Pay.

2|4|2 Banking authorities are active at European level, led by the ECB

Central bank oversight: a cooperative exercise in Europe

Under European legislation and, when relevant, thanks to their national mandate, national central banks have been assigned a central role within Europe in terms of developing effective and safe cashless payment instruments.[18]

While nationally, central banks may have different legal foundations for overseeing cashless payment instruments, their co-responsibility at EU level in conjunction with the ECB is fully established.

The payment card is the first cashless instrument to be subject to common oversight by central banks. All card payment schemes active in Europe, whether domestic or international, are thus subject to this oversight. These schemes were evaluated starting in 2008 based on a common framework.[19] The consolidated results of the evaluations are to be published in a report detailing the main

17 Article 13 of the European Convention on Mutual Assistance in Criminal Matters of 29 May 2000, supplemented by the Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between the Member States.

18 Article 127 of the Lisbon Treaty on the Functioning of the European Union provides that one of the basic tasks of national central banks is to promote the smooth operation of payment systems. Article 22 of the Statute of the European System of Central Banks indicates that national central banks must ensure efficient and sound clearing and payment systems.

19 "Eurosystem oversight framework for card payment schemes – standards", January 2008 *http://www.ecb.int/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf*

findings. Security aspects will of course occupy an important place.

The ECB and the national central banks now perform an annual exercise, similar to that conducted by the Observatory, in which they collect statistical information on card payment fraud from all active card payment schemes across Europe. This exercise has become an integral part of this oversight system. The ECB published the first report in July 2012.[20] Its findings corroborate the trends observed in France, namely that fraud in face-to-face payments is under control, while there are considerable concerns surrounding card-not-present (CNP) payments.

The need for cooperation between bank regulators

While national central banks act in concert within ECB-coordinated working groups dealing with specific payment instruments, until recently there was no body in Europe to bring together central banks and supervisors and ensure a harmonised approach by banking authorities to the security of payment instruments. The creation in February 2011 of the SecuRe Pay Forum, in which both the Banque de France and the *Autorité de contrôle prudentiel* participate, addresses this need in full. SecuRe Pay will publish its first recommendations in late 2012,[21] on the security of online banking services and online card payments, two topics identified as priorities by participating authorities.

However, to date, no equivalent permanent organisation exists at international level. It can be noted that the required harmonisation of security measures deployed for payment instruments, including cards, has been recently stressed in a report issued by the Committee on Payment and Settlement Systems (CPSS) under the Bank for International Settlements (BIS).[22]

3| Conclusion and areas for improvement

All those involved in the payment cards environment have a stake in ensuring that counter-fraud measures are as effective as possible. As they pursue different goals – regulators want to maintain confidence in payment instruments, for example, while law enforcement agencies want to dismantle rings and stop trafficking – participants have organised themselves in their different areas, with tangible results, including:

- setting security standards and introducing dedicated counter-fraud tools (banks, EPC);
- establishing hardware certification processes (card payment schemes, government agencies);
- establishing structures for gathering intelligence and punishing fraud (law enforcement);
- establishing oversight frameworks (bank regulators).

20 *Report on card fraud*, July 2012, *http://www.ecb.int/pub/pubbydate/2012/html/index.en.html*
21 A public consultation on the provisional version of these recommendations was held from 20 April to 20 June 2012, cf. *http://www.ecb.europa.eu/press/pr/date/2012/html/pr120420.en.html*.
22 "Innovations in retail payments", *http://www.bis.org/publ/cpss102.htm*.

To bolster these arrangements, cooperation between these participants and the organisations that they have created does exist at domestic, European and international level. This cooperation is bearing fruit, but improvements are possible:

• market participants (banks, card payment schemes) have set up special structures that address the question of payment card fraud. But payment schemes must be careful to ensure that they place the operational exchange of fraud-related data, which serves to detect points of compromise, above competitive considerations. Commercial interests must not be allowed to undermine the security of card transactions;

• in terms of the certification and evaluation of components, which are essential processes that make it possible to guarantee a high level of security for hardware, participants in Europe want to adopt a harmonised approach to payment cards. But work remains to be done to finalise this approach in the area of acceptance terminals, notably as regards governance aspects;

• while supervisors and overseers have made considerable progress at European level, establishing a framework for oversight of card payment schemes by the national central banks in 2008 and setting up the SecuRe Pay Forum in 2011, which was modelled on France's Observatory for Payment Card Security, there is a need to harmonise measures and hence to organise cooperation between authorities at international level, as underlined in a recent report by the CPSS dealing with innovation in the field of retail payments.

Appendixes

Security tips for cardholders

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

Be responsible

- Your card is strictly personal: do not lend it to anyone, no matter how close they are to you.
- Keep track of your card, 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 online payments:

- protect your card number: do not store it on your computer, never write it in an 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:

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 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 to unauthorised transactions, i.e. in practice cases of loss, theft or misappropriation (including by remote fraudulent use or counterfeiting) of the payment instrument, the cardholder must inform his service provider that he 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 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 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 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 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 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 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 R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the *Monetary and Financial Code* lay down the missions, composition and operating procedures of the Observatory for Payment Card Security.

Scope

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

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

2 Under the terms of section II of Article L. 521-1 of the *Monetary and Financial Code*, assimilated entities include the Banque de France, the *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 L. 511-7 and section II of Article L. 521-3 of the *Monetary and Financial Code*.

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

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);

• credit cards are backed by a credit line that carries an interest rate and with a maximum limit negotiated with the customer. These serve to make payments and/or cash withdrawals. They enable holders to pay the issuer at the end of a determined period (over 40 days in France). The merchant is paid directly by the issuer without delay;

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

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

• electronic purses are cards that store electronic money units. Under the terms of Article 1 of CRBF Regulation 2002-13, "a unit of electronic money constitutes a claim recorded on an electronic medium and accepted as a payment instrument, within the meaning of Article L. 311-3 of the *Monetary and Financial Code*, by third parties other than the issuer. Electronic money is issued against the receipt of funds. It shall not be issued for an amount that is higher in value than that of the funds received".

The above typology includes contactless payments.

Responsibilities

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

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

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

• it maintains a technology watch in the payment card field, with the aim of proposing ways of combating technological attacks on the security of payment cards. To this end, it collects all the available information that is liable to reinforce payment card security and puts it at the disposal of its members. It organises the exchange of information between its members while respecting confidentiality where necessary.

In accordance with Article R. 141-2 of the *Monetary and Financial Code*, the Minister of the Economy, Finance and External Trade may request the Observatory's opinion on various issues, setting a time limit for its response. These opinions may be published by the Minister.

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

Composition

The composition of the Observatory is set out in Article R. 142-22 of the *Monetary and Financial Code*. Accordingly, the Observatory is made up of:

- a Deputy and a Senator;
- eight general government representatives;
- the Governor of the Banque de France or his/her representative;
- the Secretary General of the *Autorité de contrôle prudentiel* and 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, mail-order sales and e-commerce;
- three qualified prominent persons chosen for their expertise.

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

The members of the Observatory, other than the members of Parliament, those representing the State, the Governor of the Banque de France and the Secretary General of the *Autorité de contrôle prudentiel*, 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, Finance and External Trade. He has a three-year term of office, which may be renewed. Christian Noyer, the Governor of the Banque de France, has been the President of the Observatory since 17 November 2003.

Operating procedures

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

The secretariat of the Observatory, which is ensured by the Banque de France, is responsible for organising and monitoring meetings, centralising the information required for the establishment of payment card fraud statistics, collecting and making available 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, Finance and External Trade and transmitted to Parliament.

The Observatory may constitute working or study groups, notably when the Minister of the Economy, Finance and External Trade 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 standing working groups: the first is responsible for harmonising and establishing fraud statistics and the second for ensuring a payment card technology watch. In 2010, the Observatory decided to set up a third working group to look at the question of 3D-Secure deployment.

Given the sensitivity of the data exchanged, the members of the Observatory and its secretariat, which are bound by professional secrecy under Article R. 142-25 of the *Monetary and Financial Code*, must maintain the confidentiality of the information that is transmitted to them in the course of their work. To this end, the Observatory's rules of procedure stipulate the members' obligation to undertake to ensure the complete confidentiality of working documents.

Members of the Observatory

Pursuant to Article R. 142-22 of the *Monetary and Financial Code*, the members of the Observatory, other than the members of Parliament, those representing the State, the Governor of the Banque de France and the Secretary General of the Prudential Supervisory Authority (*Autorité de contrôle prudentiel*), are appointed for a three-year term by order of the Minister of the Economy, Finance and External Trade. The last appointment order was issued on 29 June 2009.

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Jean-Pierre BRARD
Deputy
Nicole BRICQ
Senator replaced at the end of her mandate by
Michèle ANDRÉ
Senator

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

Philippe RICHARD
Olivier PRATO
General Secretariat

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

- The Central Director for the Security of Information Systems or his/her representative:
  Patrick PAILLOUX

Nominated on proposition by the Minister of the Economy, Finance and External Trade:

- The Senior Official for Defence or his/her representative:
  Stéphane MARTIN
  Jacques THOMAS

- The Head of the Treasury or his/her representative:
  Laurent PERDIOLAT
  Magali CESANA

Nominated on proposition by the Minister of Consumer Affairs:

- The Director of the General Directorate 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:
  Régis PIERRE
  Jérôme SIMON

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
  Thierry MEZENGUEL

Nominated on proposition by the Minister of the Interior:

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

Nominated on proposition by the Deputy Minister of Industry:

- The Director General for Businesses or his/her representative:
  Mireille CAMPANA

Representatives of payment card issuers

Yves BLAVET
Head of Payment Instruments
Société Générale
Jean-Marc BORNET
Director
Groupement des Cartes Bancaires
Jean-François DUMAS
Vice President
American Express France
Bernard DUTREUIL (until 20 November 2011)
replaced by **Willy DUBOST**
(since 21 November 2011)
Director Systems and Means of Payment
Fédération bancaire française
Bernard GOURAUD
Technologies Director
Banque Populaire – Caisse d'Épargne
François LANGLOIS
Director, Institutional Relations
BNP Paribas Personal Finance
Frédéric MAZURIER
Administrative and Financial Director
Carrefour Banque
Gérard NEBOUY
CEO
Visa Europe France
Emmanuel PETIT
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
National Confederation – Associations familiales catholiques (CNAFC)
Valérie GERVAIS
General Secretary
Association FO Consommateurs (AFOC)
Christian HUARD (until 20 November 2011)
replaced by **Ariane POMMERY**
(since 21 November 2011)
General Secretary
Association de défense d'éducation et d'information du consommateur (ADEIC)
Jean-Pierre JANIS
Representative
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Representatives of merchants' professional organisations

Philippe JOGUET
Department Head, Regulation and Sustainable Development
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
Representative
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

Philippe CAMBRIEL
Executive Vice-President
Gemalto
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 collected in 2011 that the Observatory for Payment Card Security received from:

- the 130 members of the "CB" Bank Card Consortium, with international data provided by MasterCard and Visa Europe France;
- nine three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Carrefour Banque, Crédit Agricole Consumer Finance (Finaref and Sofinco), Cofidis, Cofinoga, Diners Club and Franfinance;
- issuers of the electronic purse Moneo.

Total number of cards in circulation in 2011: 85.8 million
- 64.7 million four-party cards ("CB", MasterCard and Moneo);
- 21.0 million three-party cards.

Number of cards reported lost or stolen[1] in 2011: around 745,000

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

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

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

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

Table 1

The payment card market in France in 2011 – Issuance

(volume in millions; value in EUR billions)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	**Value**	**Volume**	**Value**	**Volume**	**Value**
Four-party cards						
Face-to-face and UPT payments	6,904.07	308.46	125.39	8.17	28.89	3.04
Card-not-present payments excl. online payments	119.73	9.64	12.06	0.88	2.94	0.31
Card-not-present online payments	380.48	29.62	94.09	4.24	9.75	0.70
Withdrawals	1,507.83	114.58	27.52	3.03	17.99	2.57
Total	**8,912.10**	**462.30**	**259.06**	**16.32**	**59.59**	**6.62**
Three-party cards						
Face-to-face and UPT payments	133.34	14.89	5.05	0.84	6.79	1.30
Card-not-present payments excl. online payments	3.11	0.18	na	na	na	na
Card-not-present online payments	6.72	0.95	2.61	0.22	0.48	0.09
Withdrawals	4.27	0.38	na	na	na	na
Total	**147.43**	**16.39**	**7.67**	**1.06**	**7.27**	**1.39**
Grand total	**9,059.53**	**478.69**	**266.73**	**17.38**	**66.86**	**8.01**

Source: Observatory for Payment Card Security.

Table 2

The payment card market in France in 2011 – Acquisition

(volume in millions; value in EUR billions)

	French issuer, French acquirer		SEPA foreign issuer, French acquirer		Non-SEPA foreign issuer, French acquirer	
	Volume	**Value**	**Volume**	**Value**	**Volume**	**Value**
Four-party cards						
Face-to-face and UPT payments	6,904.07	308.46	144.94	10.57	35.21	4.68
Card-not-present payments excl. online payments	119.73	9.64	6.19	1.40	2.13	0.82
Card-not-present online payments	380.48	29.62	16.75	2.09	3.34	0.48
Withdrawals	1,507.83	114.58	28.47	4.89	7.03	1.47
Total	**8,385.27**	**462.30**	**196.35**	**18.94**	**47.71**	**7.44**
Three-party cards						
Face-to-face and UPT payments	133.34	14.89	4.99	1.49	4.55	1.58
Card-not-present payments excl. online payments	3.11	0.18	na	na	na	na
Card-not-present online payments	6.72	0.95	0.41	0.08	0.41	0.09
Withdrawals	4.27	0.38	na	na	na	na
Total	**147.43**	**16.39**	**5.41**	**1.57**	**4.96**	**1.67**
Grand total	**9,059.53**	**478.69**	**201.76**	**20.51**	**52.67**	**9.11**

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 2011 – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face and UPT payments	517.1	45,147.2	112.5	11,075.4	85.5	14,521.3
Lost or stolen cards	451.3	41,724.7	41.0	3,785.1	18.2	3,442.5
Intercepted cards	11.8	367.2	0.7	40.6	0.1	7.1
Forged or counterfeit cards	47.4	2,929.1	23.1	2,987.1	48.2	8,294.9
Appropriated numbers	1.0	63.1	45.4	4,067.5	17.2	2,481.8
Other	5.6	63.2	2.3	195.1	1.8	294.9
Card-not-present payments excl. online payments	384.5	25,159.8	60.1	5,644.3	24.3	3,117.7
Lost or stolen cards	2.2	153.4	15.6	1,593.6	7.3	994.3
Intercepted cards	0.0	1.3	0.2	2.4	0.1	2.4
Forged or counterfeit cards	0.0	1.1	12.7	1,062.4	5.8	702.8
Appropriated numbers	382.2	25,003.1	30.9	2,944.1	10.9	1,399.8
Other	0.0	0.8	0.6	41.9	0.2	18.4
Card-not-present online payments	795.8	101,203.7	321.3	24,112.5	85.3	10,671.3
Lost or stolen cards	6.8	880.8	88.4	6,733.9	32.3	3,055.7
Intercepted cards	0.0	1.0	0.3	22.0	0.1	9.2
Forged or counterfeit cards	0.1	17.3	71.4	4,763.8	31.8	2,942.8
Appropriated numbers	788.9	100,302.2	159.0	12,240.6	49.0	4,602.2
Other	0.0	2.4	2.2	352.2	0.3	61.3
Withdrawals	119.8	33,382.2	5.7	1,199.6	121.7	20,525.8
Lost or stolen cards	112.4	32,042.7	3.7	808.7	7.0	1,089.5
Intercepted cards	0.5	111.9	0.0	3.9	0.1	6.4
Forged or counterfeit cards	6.1	1,115.4	1.8	345.7	110.7	18,714.3
Appropriated numbers	0.0	2.5	0.1	6.7	0.6	92.3
Other	0.7	109.7	0.2	34.7	3.3	623.3
Total	**1,817.2**	**204,892.9**	**499.6**	**42,031.8**	**344.9**	**48,836.1**

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 2011 – Acquisition

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		SEPA foreign issuer, French acquirer		Non-SEPA foreign issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face and UPT payments	517.1	45,147.2	146.8	21,641.0	306.1	76,015.1
Lost or stolen cards	451.3	41,724.7	48.2	2,324.9	40.8	11,030.3
Intercepted cards	11.8	367.2	3.1	117.6	0.5	163.3
Forged or counterfeit cards	47.4	2,929.1	12.2	2,746.5	94.6	23,704.3
Appropriated numbers	1.0	63.1	78.5	16,223.6	167.8	40,570.2
Other	5.6	63.2	4.9	228.4	2.3	547.0
Card-not-present payments excl. online payments	384.5	25,159.8	na	na	na	na
Lost or stolen cards	2.2	153.4	na	na	na	na
Intercepted cards	0.0	1.3	na	na	na	na
Forged or counterfeit cards	0.0	1.1	na	na	na	na
Appropriated numbers	382.2	25,003.1	na	na	na	na
Other	0.0	0.8	na	na	na	na
Card-not-present online payments	795.8	101,203.7	na	na	na	na
Lost or stolen cards	6.8	880.8	na	na	na	na
Intercepted cards	0.0	1.0	na	na	na	na
Forged or counterfeit cards	0.1	17.3	na	na	na	na
Appropriated numbers	788.9	100,302.2	na	na	na	na
Other	0.0	2.4	na	na	na	na
Withdrawals	119.8	33,382.2	2.9	822.3	2.3	611.4
Lost or stolen cards	112.4	32,042.7	2.5	705.4	1.2	332.2
Intercepted cards	0.5	111.9	0.1	31.3	0.0	3.4
Forged or counterfeit cards	6.1	1,115.4	0.2	55.1	1.0	250.5
Appropriated numbers	0.0	2.5	0.0	10.1	0.1	22.4
Other	0.7	109.7	0.1	20.4	0.0	2.9
Total	**1,817.2**	**204,892.9**	**149.7**	**22,463.4**	**308.4**	**76,626.5**

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 2011 – Issuance

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		French issuer, SEPA foreign acquirer		French issuer, non-SEPA foreign acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face and UPT payments	6.22	2,990.27	5.29	1,511.70	5.68	1,470.43
Lost or stolen cards	2.24	407.28	1.90	159.72	0.33	143.06
Intercepted cards	0.56	211.84	0.21	171.71	0.06	23.10
Forged or counterfeit cards	1.34	299.94	1.54	602.55	4.45	940.35
Appropriated numbers	0.66	107.04	1.58	542.12	0.81	360.74
Other	1.43	1,964.16	0.06	35.60	0.03	3.18
Card-not-present payments excl. online payments	0.30	239.25	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Appropriated numbers	0.17	11.04	na	na	na	na
Other	0.13	128.21	na	na	na	na
Card-not-present online payments	10.07	3,011.32	6.58	744.10	2.82	741.61
Lost or stolen cards	2.10	805.71	1.75	26.54	0.16	66.70
Intercepted cards	0.71	310.93	0.03	2.57	0.01	9.15
Forged or counterfeit cards	2.66	535.42	1.23	71.40	0.98	280.87
Appropriated numbers	3.69	1,008.55	3.48	624.32	1.65	378.87
Other	0.90	350.70	0.09	19.26	0.02	6.13
Withdrawals	1.95	359.19	na	na	na	na
Lost or stolen cards	1.55	249.36	na	na	na	na
Intercepted cards	0.26	66.45	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Appropriated numbers	0.02	9.34	na	na	na	na
Other	0.12	34.05	na	na	na	na
Total	**18.54**	**6,600.02**	**11.87**	**2,255.79**	**8.50**	**2,212.03**

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 2011 – Acquisition

(volume in thousands; value in EUR thousands)

	French issuer, French acquirer		SEPA foreign issuer, French acquirer		Non-SEPA foreign issuer, French acquirer	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face and UPT payments	6.22	2,990.27	1.15	493.00	2.96	962.28
Lost or stolen cards	2.24	407.28	0.06	11.90	0.11	49.61
Intercepted cards	0.56	211.84	0.00	0.02	0.00	0.00
Forged or counterfeit cards	1.34	299.94	0.69	149.26	1.93	321.74
Appropriated numbers	0.66	107.04	0.40	314.04	0.86	580.00
Other	1.43	1,964.16	0.00	17.79	0.06	10.94
Card-not-present payments excl. online payments	0.30	239.25	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Appropriated numbers	0.17	11.04	na	na	na	na
Other	0.13	128.21	na	na	na	na
Card-not-present online payments	10.07	3,011.32	4.70	2,126.15	9.41	3,685.65
Lost or stolen cards	2.10	805.71	0.40	77.92	0.78	340.94
Intercepted cards	0.71	310.93	0.01	0.12	0.04	0.55
Forged or counterfeit cards	2.66	535.42	1.14	507.24	3.39	1,438.16
Appropriated numbers	3.69	1,008.55	3.14	1,464.02	5.11	1,885.07
Other	0.90	350.70	0.02	76.34	0.09	20.83
Withdrawals	1.95	359.19	na	na	na	na
Lost or stolen cards	1.55	249.36	na	na	na	na
Intercepted cards	0.26	66.45	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Appropriated numbers	0.02	9.34	na	na	na	na
Other	0.12	34.05	na	na	na	na
Total	**18.54**	**6,600.02**	**5.85**	**2,619.16**	**12.37**	**4,647.93**

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

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

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

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

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

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

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

Fraud typology

The Observatory has in addition defined a fraud typology that makes distinctions between.

The origin of the fraud:

• lost or stolen cards: the fraudster uses a payment card obtained without the knowledge of the lawful cardholder, following card theft or loss;

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

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

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

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

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

Fraud techniques:

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

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

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

• 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;

3 Personal Account Number.

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

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

Types of payment:

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

Distribution of losses between:

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

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

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

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 the distribution and to limit the number of copies per person.

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
Direction de la Communication
de la Banque de France

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

Orders
Observatoire de la sécurité des cartes de paiement
011-2324
Telephone: +1 42 92 96 13
Fax: +1 42 92 31 74

Imprint
Banque de France

Website
www.observatoire-cartes.fr

ISSN 1768-2991