2012 ANNUAL REPORT
OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

bservatoire
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 2012
of the Observatory for payment card security

addressed to

The Minister of the Economy and Finance
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

CHAPTER 4: EUROPEAN AND INTERNATIONAL REGULATORY DEVELOPMENTS AND RECOMMENDATIONS ON PAYMENT CARD SECURITY 41

APPENDIXES

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

- *a stocktaking of measures to protect internet card payments (Part 1);*
- *the 2012 fraud statistics (Part 2);*
- *a summary of the Observatory's technology watch activities (Part 3), containing two studies: one on the security of contactless card payments, and one on fraud techniques targeting card transactions;*
- *a study on European and international regulatory developments and recommendations on payment card security (Part 4).*

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 tenth Annual Report of the Observatory for Payment Card Security, *covering the 2012 financial year, contains four sections, summarised as follows.*

Part 1: measures to protect internet card payments

The Observatory has conducted an annual opinion survey of cardholders on this topic since 2010 and collects statistical data from banks and their technical providers. The findings reveal that further progress was made in 2012.

Users now come into contact more regularly with authentication systems and are more familiar with them. Nine out of ten online shoppers now say that they have heard of a protection solution other than the card number and verification code requested during online transactions, while two of out three said that they had already encountered strong authentication systems. This is partly due to the increase in the proportion of secure internet payments, which accounted for 27.5% of the total amount in 2012, up from 23% in 2011. But efforts must be kept up to ensure that e-merchants engage in more widespread deployment of protection solutions enabling strong cardholder authentication, such as 3D-Secure, wherever possible and appropriate. This position was upheld by participants at the conference on this topic organised in November 2012 by the Observatory. Against this backdrop, in 2013 the Banque de France is teaming up with the "CB" Bank Card Consortium and collaborating closely with banks to work with the e-merchants that suffer from the greatest amount of fraud to help them make their internet payments more secure.

These initiatives are now being taken forward within a European framework. The European forum on the security of retail payments (SecuRe Pay) has issued recommendations calling for strong cardholder authentication to be adopted on a wide scale for the highest-risk internet payments by 1 February 2015.

Part 2: fraud statistics for 2012

The fraud rate was up slightly for the fifth year in a row, standing at 0.080% in 2012, corresponding to a total fraud of EUR 450.7 million. By comparison, in 2011 the rate was 0.077% and total fraud amounted to EUR 413.2 million.

The increase in fraud reflected two key trends:

- *a 7.1% rise in domestic fraud, linked to:*

  – a surge in attacks on automated teller machines (ATMs) (up 73% compared with 2011) and points of sale (POS) (2.5-fold increase on 2011), which have become the preferred targets for organised fraud rings, and a continued high number of thefts of cards with PINs. In response to the confirmation of these trends that were already in evidence in 2011, the Observatory again reminds cardholders to be on their guard and reiterates the best practices to follow when making payments to a merchant or on the internet, or when making withdrawals (see Appendix 1);

– the continuing sustained growth in fraud involving card-not-present (CNP) payments, even though the fraud rate for internet payments fell for the first time since 2008 to reach 0.290% (compared with a historical high of 0.341% in 2011). This favourable development reflects efforts made by e-merchants to phase in solutions such as 3D-Secure that enable one-time cardholder authentication in internet payments.

Even so, the amount of fraud in CNP payments increased amid sustained growth in internet payments and a partial shift in fraud to CNP payments by mail or phone. The fraud rate for CNP payments remains 20 times higher than the rate for face-to-face payments. Overall, CNP payments accounted for 9.2% of the value of domestic transactions but for 61% of the total amount of fraud.

Accordingly, the Observatory is calling on e-merchants, particularly those suffering the highest amounts or rates of fraud, to continue to implement solutions to enable strong cardholder authentication in internet payments wherever possible and appropriate.

The fraud rate for face-to-face payments remained at a low level (0.015%), unchanged from 2011.

- *a significant increase (11.2%) in international fraud linked to:*

  – growth in internet fraud (37%), which may be attributable to a partial shift in domestic fraud to this channel, as measures have been phased in to protect internet payments in France, while international sites are less well guarded. The deployment of strong authentication solutions, which has been spurred on by the recommendations of the SecuRe Pay forum, should however see this trend reverse in Europe in the near future;

  – a resurgence in cases of card theft and/or compromise of card data, notably during trips to Latin America or South-East Asia, leading to an increase in fraud in face-to-face payments and withdrawals, with swift use of compromised data making it hard for payment schemes to spot unusual behaviour by cardholders.

The Observatory has seen positive effects from efforts undertaken in Europe in recent years to combat fraud, and notably from extensive use of EMV-compliant smartcards at points of sale and withdrawal. A comparison of fraud rates for international transactions within Europe (Single European Payments Area – SEPA) and outside Europe (non-SEPA) shows that regions that have not adopted EMV are suffering the consequences of a major shift in fraud.

Note that in 2012, Visa, MasterCard, American Express and Discover (Diners Club International) announced a set of incentives to promote the adoption of the EMV standard in the United States by 2015. This shift is expected to bring benefits, particularly in terms of combating magnetic stripe forgery, for French cards as regards face-to-face payments and withdrawals in the United States, and for US cards as regards face-to-face transactions in France.

Part 3: technology watch on fraud techniques and the security of contactless card payments

Security of contactless card payments: *following the proliferation of contactless cards and payment terminals and the recent publication of studies on their security, the Observatory decided to update its analyses of 2007 and 2009. It found that the risks linked to eavesdropping on contactless transactions and unlawful remote activation of cards remain low because of the challenges involved in implementing the requisite technical procedures. Moreover, the financial gains for fraudsters are limited since only small-value contactless payments may be made without entering the PIN.*

Accordingly, the Observatory considers that reputational risk is the primary risk associated with contactless card payments. Given the need to maintain user confidence in this payment instrument, however, the Observatory is reiterating its earlier recommendations. In this context, issuers have promised that they will provide cardholders with solutions that either prevent use in contactless mode (protective cases) or remotely disable the contactless function (scripts), or issue cards that do not offer this function when so requested by cardholders. Also, as it has stated before, the Observatory feels it would be worth examining the introduction of a special primary account number (PAN) for contactless payments to prevent compromised data from being reused via other channels, and notably online. In the case of internet transactions, the Observatory recommends continuing to deploy measures aimed at protecting CNP transactions through strong authentication.

Fraud techniques: *payment cards and acceptance solutions enjoy high levels of security in France. Fraud in card transactions remains under control and is at extremely low levels for withdrawals and face-to-face payments. The Observatory nevertheless decided to conduct a review of existing fraud techniques and describe the measures intended to reduce the risks of attack and reuse of compromised data.*

One key finding of the study is that because of the large volumes of information held in the databases of merchants and payment service providers, firms must put in place adequate protective measures to restrict unlawful access to these data by criminals and particularly to prevent these data from being reused in CNP payments.

In face-to-face payments, continued vigilance is needed for payment terminals and unattended payment terminals (UPTs). Certification and authorisation processes for these devices need to be constantly adjusted to take account of the latest development techniques.

The Observatory recommends furthermore that merchants and participants in the acquisition chain pay close attention to acceptance devices and keep careful logs for the equipment

deployed in face-to-face environments to prevent any attempts to tamper with or switch such equipment. Cardholders are also urged to be on their guard when making face-to-face payments or withdrawals (see Appendix 1).

To prevent compromised data being reused via the online channel, which is especially exposed to fraud, the Observatory recommends using strong cardholder authentication as well as a card verification code.

Part 4: regulatory developments and international recommendations on card payments in Europe and worldwide

The Observatory decided this year to conduct a stocktaking of regulatory developments and recommendations relating to card payments in Europe and worldwide.

Given the need to maintain a high level of security for this instrument while at the same time promoting the development of different types of use, the challenge for regulators and overseers is to continually adjust the operational and legal frameworks deployed around payment cards. The integrated nature of economic trade and payments additionally creates the need to coordinate regulatory practices to avoid generating competitive distortions between participants and limit the opportunities for fraud.

In 2007, European lawmakers began harmonising the regulatory framework for payment law to facilitate the introduction of the European single market for cashless payments and promote competition. Discussions launched in 2012 by the European Commission to identify and remove barriers restricting market integration should lead to changes in the near future to the legal framework for payments within Europe aimed at creating more efficient, modern and safer means of payment. Responding to rising fraud in card payments during online shopping, in 2011 Europe's national supervisors and overseers set up the SecuRe Pay forum, whose first report, published in January 2013, contains recommendations to enhance the security of internet card payments.

The Bank for International Settlements (BIS) is leading the international work in this area. A 2012 report by its Committee on Payment and Settlement Systems (CPSS) looked at innovative payments (including by card) and their security.

Stocktaking of measures to protect internet card payments

The Observatory regularly monitors fraud in card-not-present (CNP) payments in France, which totalled EUR 138.8 million in 2012 (for a fraud rate of 0.299%), as well as the anti-fraud methods deployed by participants in the payment chain. Among the measures recommended by the Observatory, the most commonly-used solution is the phasing-in of strong cardholder authentication based on one-time codes for internet payments wherever possible and appropriate.

As in the 2011 report, this chapter describes the progress made in implementing this recommendation (1|) along with initiatives by the Observatory and the Banque de France to make e-merchants more aware of the need to enhance the security of internet payments (2|).

1| Stocktaking of measures to protect internet card payments

1|1 Progress in deploying 3D-Secure

To monitor the deployment of strong authentication solutions by issuers and identify difficulties or areas for improvement, since 2011 the Observatory has conducted semi-annual campaigns to collect statistical data from banks and their technical providers, which it uses to measure quantitative and qualitative developments in the implementation of strong authentication. The data gathered by the Observatory point to a marked improvement in the deployment rate for such solutions in 2012 among issuers and merchants alike.

1|1|1 88% of cardholders have now been provided with functional authentication systems

Virtually all cardholders have now been provided with at least one strong 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 84% to 88% of the total population of online shoppers.

1|1|2 The failure rate for secure transactions fell to around 18%

The failure rate for transactions decreased to 18% from 20% in 2011. While this rate may still seem high at first glance, it does not take account of failures followed by a successful attempt or of attempted fraud. The deployment of protective solutions for the most at-risk payment transactions may additionally be a factor in the high failure rate for these transactions. This failure rate should be compared with the failure rate observed for non-authenticated card payments, which has not yet been collected but which is expected to be monitored beginning next year.

The range of observed failure rates among financial institutions operating in France is narrowing, reflecting bilateral exchanges on good practices between the Banque de France and institutions.

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 texting-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 continues to increase as e-merchants gradually switch over

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 23% to 27.5% over one year, notably owing to awareness-raising initiatives conducted by the Observatory and the Banque de France among e-merchants (cf. below). This latest increase fell in the wake of the shift to strong authentication by major e-retailers, such as Voyages-SNCF, Air France, Orange, and, more recently, Mistergooddeal.

1|2 Authentication solutions have become more familiar to users, who are encountering them more often

Building on previous surveys that measured the perception of online shoppers who had encountered strong authentication solutions when making internet card payments, the Observatory decided this year to assess the change in the percentage of online shoppers who are familiar with and have used strong authentication solutions.

The study was conducted by Harris Interactive and surveyed 993 individuals offering a representative sample of the French population aged 16 and over.

1|2|1 Authentication solutions for internet card payments are now widely known to online shoppers…

Nine out of ten online shoppers say that they are familiar with a protective solution in addition to the card number and verification code requested during online transactions, and more than eight out of ten knew of at least one strong authentication solution, notably the practice of sending a text message with the one-time code method. The proportion of online shoppers who knew of at least one strong authentication solution increased by 37% this year, notably thanks to increased usage.

1|2|2 … and are more and more widely used

The proportion of online shoppers who said that they had used a strong authentication solution, principally the sending of a text message with a one-time code method, increased by 40% compared with last year's survey. Accordingly, two out of three online shoppers said that they had already encountered strong authentication.

Increased use of these solutions is naturally connected to the phasing-in of authentication solutions by e-merchants, which were targeted by the Observatory and the Banque de France during initiatives aimed at raising awareness about the risks of fraud.

2| Initiatives conducted by the Observatory and the Banque de France to make e-merchants more aware about enhancing the security of internet payments

2|1 Organisation of a conference in 2012 on protecting internet card payments and publication of a brochure to raise awareness among e-merchants

Statistics published by the Observatory in recent years show that online transactions are especially vulnerable to fraud. Accordingly, on 12 November 2012, the Observatory organised a conference on protecting internet card payments.

The event was chaired by Banque de France Governor Christian Noyer, who is also president of the Observatory. It was attended by more than 180 participants, including the representatives of more than 70 e-commerce firms.

The conference gave participants an opportunity to share their experience on ways to effectively combat fraud in internet card payments. Discussions revealed that the prevention effort requires the use of additional tools to detect the payments presenting the highest fraud risk and protect them via strong authentication.

It was concluded that strong authentication solutions should now be introduced on a wide scale to reduce fraud in internet card payments. These resources should also be tailored to reflect technological developments and consumer habits, particularly the growing trend towards using mobile phones to order and pay online.

Digital wallets may offer one way to protect internet payments. However, the Observatory called on the industry to keep up the drive to propose solutions offering strong authentication across all distribution channels.

Following this conference, the Observatory published a brochure (in French) for e-merchants on protecting internet payments, and posted it on its website (*www.observatoire-cartes.fr*).

This brochure recaps best practices for preventing fraud in internet card payments, including a section on the conditions for the successful deployment of strong authentication.

The brochure was supplemented with an online set of frequently asked questions to answer general, technical and legal queries and help merchants understand the strong authentication mechanism.

2|2 Bilateral meetings with e-merchants that are especially exposed to the risks of fraud

In early 2013, the Banque de France teamed up with the "CB" Bank Card Consortium to hold meetings with e-merchants suffering from especially high amounts and/or rates of fraud.

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

The following conclusions emerged from the initial round of meetings:

• interviewed e-merchants agreed to deploy – in most cases in 2013 – strong cardholder authentication solutions for the highest-risk transactions;

• many e-merchants pointed out that they are often the target of fraud that goes beyond mere payment instrument fraud but belongs rather to the broader category of cyber-crime (identity theft, etc.). They accordingly stressed the need to have contact persons within law enforcement who understand the transverse nature of cyber-crime;

• some e-merchants are the targets of fraud involving anonymous prepaid cards. They said it would be useful to be able to identify prepaid cards more easily in order to monitor them more carefully and be in a position to block them if fraud is spotted. It should be noted that in 2012 the Observatory continued its study into the use of anonymous prepaid cards, and its president wrote to the Minister for the Economy and Finance underlining the fraud and terrorist financing risks posed by these products and suggesting amendments to the framework of rules.

The Observatory's working groups will follow up on these different points.

3| Conclusion: steady increase in the level of online security thanks to efforts by all parties

The opinion survey conducted for the third year in a row by the Observatory and the statistics submitted by banks and their technical providers show that real progress was made in terms of protecting online card payment transactions in 2012. Increased familiarity with the solutions deployed for this purpose reflects their use by e-merchants and should have a positive impact on fraud statistics in the medium term.

The Observatory recommends that banks and merchants keep up their efforts to combat fraud in CNP transactions, whose level remains high (see Chapter 2, section 4|):

• since banks have now virtually completed deployment of strong authentication solutions, the challenge now facing some institutions is to improve success rates for secure transactions;

• the widespread introduction by merchants of one-time authentication solutions, and hence of

3D-Secure, with activation based on a risk analysis, remains a priority for the Observatory. The adoption of 3D-Secure by several major e-merchants in 2012, including Mistergooddeal, should play a determining role in ensuring the broader introduction of this protocol among large e-merchants.

These measures are now being taken forward within a European framework. The SecuRe Pay forum has issued recommendations calling for strong cardholder authentication to be adopted generally for the highest-risk internet payments by 1 February 2015.

Fraud statistics for 2012

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 2012 statistics is presented below. It includes an overview of the different fraud trends for three-party cards and four-party cards, fraud trends for domestic and international, face-to-face and card-not-present (CNP) transactions, as well as payment and withdrawal transactions, and fraud trends for different types of fraud involving lost or stolen cards, intercepted cards, forged or counterfeit cards, and misappropriated card numbers. In addition, Appendix 5 to this report presents a series of detailed fraud indicators.

1| Overview

The total value of card payments amounted to EUR 561.5 billion in 2012, up 5.2% compared with 2011. The annual growth rate was weaker than in 2011 (7.1%) and slightly below the five-year average (6.2%), but was higher than in 2009 (2.9%) and 2010 (4.4%).

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 511 billion in transactions in France and in other countries made with 67.3 million four-party cards issued in France (including 1.97 million electronic purses and 3.42 million contactless cards);*
- *EUR 17.4 billion in transactions primarily in France with 18.4 million three-party cards issued in France;*
- *EUR 32.1 billion in transactions in France with foreign three-party and four-party cards.*

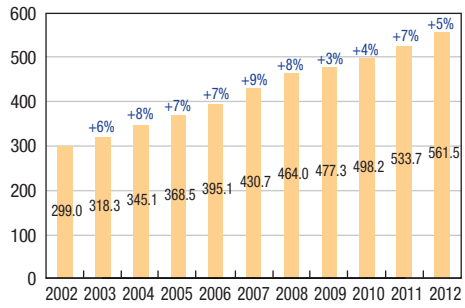
Data were gathered from:

- *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.*

Chart 1

Value of transactions

(EUR billions)

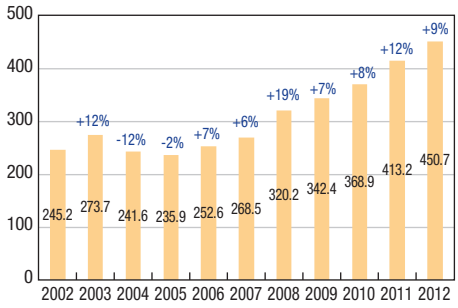


Source: Observatory for Payment Card Security.

Chart 2

Amount of fraud

(EUR millions)



Source: Observatory for Payment Card Security.

The total amount of fraud increased sharply, rising by 9.1% compared with 2011 to reach EUR 450.7 million in 2012, reflecting two key trends:

• another substantial increase in fraud in international transactions (11.2% compared with 2011) following an exceptional decline in 2011. International transactions accounted for 10.3% of the total value of transactions but for 49.8% of the total amount of fraud;

• an increase in fraud in domestic transactions (7.1% compared with 2011), which, as every year, mainly involved CNP payments. Overall, CNP payments accounted for 9.2% of the value of domestic transactions but for 61% of the total amount of domestic fraud.

As a result, the fraud rate for card payments and withdrawals in 2012 recorded by French schemes stood at 0.080%, a slight increase for the fifth year running.

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 0.065% in 2012, up from 0.061% in 2011. Issuer fraud totalled EUR 345.2 million, compared with EUR 306.8 million in 2011.

The rate of acquirer fraud, which covers all fraudulent payments and withdrawals made in France with all French and foreign cards, fell slightly to 0.062%, corresponding to fraud of EUR 331.9 million, from 0.063% and EUR 317.8 million in 2011.

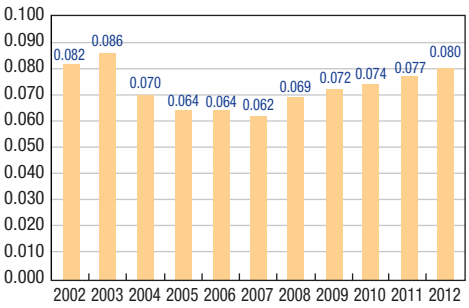
The number of cards reported lost or stolen in 2012, and for which at least one fraudulent transaction was recorded, increased by 3% to 767,000, remaining at a high level after the sharp growth noted in 2011 (16% compared with 2010).

The average value of a fraudulent transaction fell to EUR 125 from EUR 130 in 2011.

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)

	2008	2009	2010	2011	2012
Four-party cards	0.070 (304.3)	0.072 (324.3)	0.074 (351.5)	0.077 (394.9)	**0.080 (434.4)**
Three-party cards	0.054 (16.0)	0.068 (18.2)	0.080 (17.4)	0.083 (18.3)	**0.076 (16.3)**
Total	0.069 (320.2)	0.072 (342.4)	0.074 (368.9)	0.077 (413.2)	**0.080 (450.7)**

Source: Observatory for Payment Card Security.

The fraud rate for four-party cards was 0.080% in 2012 (compared with 0.077% in 2011), rising for the fifth year in a row. The fraud rate for three-party cards was 0.076% in 2012 (compared with 0.083% in 2011), marking a decrease after increasing for four consecutive years.

Issuer and acquirer fraud rates for four-party cards were 0.066% and 0.062% respectively, compared with 0.061% and 0.062% respectively in 2011. The average value of a fraudulent transaction was EUR 122, after EUR 127 in 2011.

Issuer and acquirer fraud rates for three-party cards were 0.051% and 0.071% respectively, compared with 0.059% and 0.071% respectively in 2011. The average value of a fraudulent transaction was EUR 345 in 2012, after EUR 321 in 2011.

3| Geographical breakdown of fraud

The decline in fraud in international transactions noted in 2011 was not repeated in 2012, with the amount of fraud climbing 11.2% compared to the previous year to EUR 224.3 million.

The amount of fraud in international transactions remains slightly lower than fraud in domestic transactions, which also increased compared with 2011, rising 7.1% to EUR 226.4 million.

Even so, because of the transaction values involved, the fraud rate for international transactions, at 0.387%, was still around eight times higher than the rate for domestic transactions (0.045%).

International transactions thus account for 49.8% of the total amount of fraud, even though they make up just over 10.3% of the total value of card payments.

Table 2

Geographical breakdown of fraud

(% rate, amounts in EUR millions)

	2008	2009	2010	2011	2012
Domestic transactions	**0.031 (130.9)**	**0.033 (144.0)**	**0.036 (163.8)**	**0.044 (211.5)**	**0.045 (226.4)**
International transactions	**0.427 (189.4)**	**0.449 (198.4)**	**0.423 (205.0)**	**0.367 (201.7)**	**0.387 (224.3)**
- o/w French issuer and foreign acquirer[a]	0.594 (118.3)	0.594 (121.6)	0.728 (54.9)	0.638 (51.0)	0.759 (62.5)
- o/w French issuer and SEPA acquirer	–	–	0.331 (50.6)	0.255 (44.3)	0.316 (56.3)
- o/w foreign issuer[b] and French acquirer	0.291 (71.0)	0.324 (76.8)	0.831 (64.5)	0.892 (81.3)	0.699 (78.2)
- o/w SEPA issuer and French acquirer	–	–	0.195 (35.0)	0.122 (25.1)	0.132 (27.3)
Total	**0.069 (320.2)**	**0.072 (342.4)**	**0.074 (368.9)**	**0.077 (413.2)**	**0.080 (450.7)**

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

The increase in fraud in international transactions carried out using cards issued in France notably reflects enhanced security solutions in France (EMV standards for face-to-face payments, one-time cardholder authentication for the highest-risk internet payments), which have forced fraudsters to shift their focus to international transactions.

Among these international transactions, fraud is lower for transactions carried out within SEPA than for those carried out in non-SEPA countries:

- the fraud rate for transactions in France using foreign cards issued outside SEPA (0.699%) is more than five times higher than the rate for transactions carried out using foreign cards issued in SEPA (0.132%);

- the fraud rate for transactions outside SEPA with cards issued in France (0.759%) was around two and a half times higher than the rate for transactions conducted within SEPA with the same types of cards (0.316%).

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

In this regard, note that in 2012, Visa, MasterCard, American Express and Discover (Diners Club International) announced a set of incentives to encourage EMV adoption in the United States.

In particular, the transfer of liability from the card issuer to the merchant in the case of fraud, beginning in October 2015 for point of sale (POS) that have not migrated to EMV, should act as a strong incentive for US issuers to adopt the EMV standard for new cards issued and for US merchants to migrate their terminals to EMV by October 2015 at the latest.

These developments are expected to bring benefits, particularly in terms of combating magnetic stripe forgery, for French cards as regards face-to-face payments and withdrawals in the United States, and for US cards as regards face-to-face transactions in France.

4| Breakdown of fraud by transaction type

The Observatory's classification of card payment transactions distinguishes face-to-face payments and unattended payment terminal (UPT) payments made

Table 3

Breakdown of domestic fraud by transaction type

(% rate, amounts in EUR millions)

	2008	2009	2010	2011	2012
Payments	0.036 (111.7)	0.038 (123.2)	0.041 (137.3)	0.049 (177.8)	0.049 (190.0)
o/w face-to-face and UPT	0.015 (44.5)	0.014 (41.0)	0.012 (36.2)	0.015 (48.1)	0.015 (51.2)
o/w card-not-present	0.252 (67.2)	0.263 (82.2)	0.262 (101.1)	0.321 (129.6)	0.299 (138.8)
o/w by post/phone	*0.280* *(28.5)*	*0.263* *(30.3)*	*0.231* *(27.3)*	*0.259* *(25.4)*	*0.338* *(29.4)*
o/w internet	*0.235* *(38.8)*	*0.263* *(51.9)*	*0.276* *(73.9)*	*0.341* *(104.2)*	*0.290* *(109.4)*
Withdrawals	0.018 (19.1)	0.019 (20.8)	0.024 (26.5)	0.029 (33.7)	0.031 (36.4)
Total	**0.031** **(130.9)**	**0.033** **(144.0)**	**0.036** **(163.8)**	**0.044** **(211.5)**	**0.045** **(226.4)**

Source: Observatory for Payment Card Security.

at POS or at fuel pumps, ticket machines, etc., from card-not-present payments made on the internet, by mail, 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 (see Table 3), the figures show that:

• the fraud rate for face-to-face and UPT payments was steady at 0.015%. These types of payments accounted for over 67% of domestic transactions but just 23% of the total amount of fraud.

The fraud rate for withdrawals increased by 6% compared with 2011 to 0.031%. This mainly reflected a surge in attacks on ATMs – automated teller machines – (approximately 1,100 in 2012, or 73% more than in 2011) and POS (about 110 in 2012, or 2.5 times more than in 2011), which have become preferred targets for organised fraud rings, and a continued high number of card thefts with PINs.

In response to this confirmation of trends that were already in evidence in 2011, the Observatory again reminds cardholders to be on their guard and reiterates the best practices to follow when making payments to a merchant or when making withdrawals (see Appendix 1).

• the fraud rate for CNP payments fell to 0.299%, but was still 20 times higher than the rate for face-to-face payments. The fraud rate for internet payments, in particular, declined to 0.290% from 0.341% in 2011, while the rate for payments by mail or phone continued to increase, rising to 0.338%, after 0.259% in 2011. These initial results obtained for internet payments reflect efforts by issuers and e-merchants to deploy solutions such as 3D-Secure that enable strong cardholder authentication for the payments representing the highest fraud risk. It should be noted however that fraud in internet payments has partially shifted to other types of CNP payments. Amid sustained growth in electronic commerce, CNP payments accounted for just 9.2% of the value of domestic transactions but for 61% of the total amount of fraud (the same as in 2011).

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 highest-risk payments (see Chapter 1 of this report).

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

Fraud in CNP payments to foreign e-merchants made using French cards surged to EUR 61.6 million in 2012 compared with EUR 45.0 million in 2011. One explanation for this is a partial shift in domestic fraud to this channel following the phasing-in of solutions to protect internet payments by online commerce sites in France, while foreign websites may be less well protected.

Fraud rates for CNP payments were especially high outside SEPA (1.551%), and there was a sharp increase in the fraud rate for CNP payments made using French cards within SEPA (0.735% in 2012 compared with 0.571% in 2011). The deployment of strong authentication solutions, which has been spurred on by the recommendations of the SecuRe Pay forum (see Chapter 1), should however see this trend reverse in Europe in the near future.

Fraud was also up in face-to-face and UPT payments with French cards in non-SEPA countries (EUR 44.5 million in 2012 compared with EUR 36.5 million in 2011). This was attributable to a resurgence in cases of card theft and/or compromise of card data, notably during trips to Latin America or South-East Asia, with swift use of compromised data making it hard for payment schemes to spot unusual behaviour by cardholders.

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

Table 4

Breakdown of international fraud by transaction type

(% rate, amounts in EUR millions)

French issuer – foreign acquirer[a)]	2009	2010	2011	2012
Payments	0.679	0.795	0.561	0.687
	(105.2)	(39.8)	(30.5)	(37.8)
o/w face-to-face and UPT	0.406	0.655	0.369	0.456
	(44.7)	(25.8)	(16.0)	(19.8)
o/w card-not-present	1.350	1.310	1.320	1.551
	(60.5)	(14.0)	(14.5)	(18.0)
o/w by post/phone	*1.016*	*1.193*	*1.011*	*1.150*
	(9.7)	*(3.8)*	*(3.1)*	*(4.0)*
o/w internet	*1.440*	*1.360*	*1.440*	*1.720*
	(50.8)	*(10.2)*	*(11.4)*	*(14.1)*
Withdrawals	0.331	0.596	0.800	0.904
	(16.5)	(15.1)	(20.5)	(24.7)
Total	**0.594**	**0.728**	**0.638**	**0.759**
	(121.6)	**(54.9)**	**(51)**	**(62.5)**
French issuer – SEPA acquirer				
Payments	–	0.396	0.300	0.372
		(49.1)	(43.1)	(55.3)
o/w face-to-face and UPT	–	0.112	0.140	0.131
		(9.2)	(12.6)	(11.7)
o/w card-not-present	–	0.944	0.571	0.735
		(40.0)	(30.5)	(43.6)
o/w by post/phone	–	*0.566*	*0.643*	*0.532*
		(4.0)	*(5.6)*	*(6.5)*
o/w internet	–	*1.021*	*0.557*	*0.788*
		(36.0)	*(24.9)*	*(37.1)*
Withdrawals	–	0.052	0.040	0.036
		(1.5)	(1.2)	(1.1)
Total	**–**	**0.331**	**0.255**	**0.316**
		(50.6)	**(44.3)**	**(56.3)**
Foreign issuer[b)] – French acquirer				
Payments	0.397	0.982	1.056	0.739
	(74.1)	(63.2)	(80.7)	(77.7)
Withdrawals	0.055	0.103	0.042	0.033
	(2.8)	(1.4)	(0.6)	(0.6)
Total	**0.324**	**0.831**	**0.892**	**0.699**
	(76.8)	**(64.5)**	**(81.3)**	**(78.2)**
SEPA issuer – French acquirer				
Payments	–	0.239	0.155	0.158
		(33.8)	(24.3)	(26.6)
Withdrawals	–	0.032	0.017	0.017
		(1.2)	(0.8)	(0.7)
Total	**–**	**0.195**	**0.122**	**0.132**
		(35)	**(25.1)**	**(27.3)**

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

Box 2

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.[1] 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
General and semi-general trade	28.8	21.0
Travel, transportation	25.7	18.8
Personal services	24.6	17.9
Telephony and communications	15.8	11.5
Household goods, furnishings, DIY	10.6	7.8
Technical and cultural products	8.3	6.0
Account loading, person to person sales	7.6	5.5
Professional services	6.6	4.8
Food	3.1	2.3
Miscellaneous	2.8	2.0
Online gaming	2.4	1.8
Insurance	0.5	0.4
Health and Beauty	0.2	0.1
Total	**137.0**	**100.0**

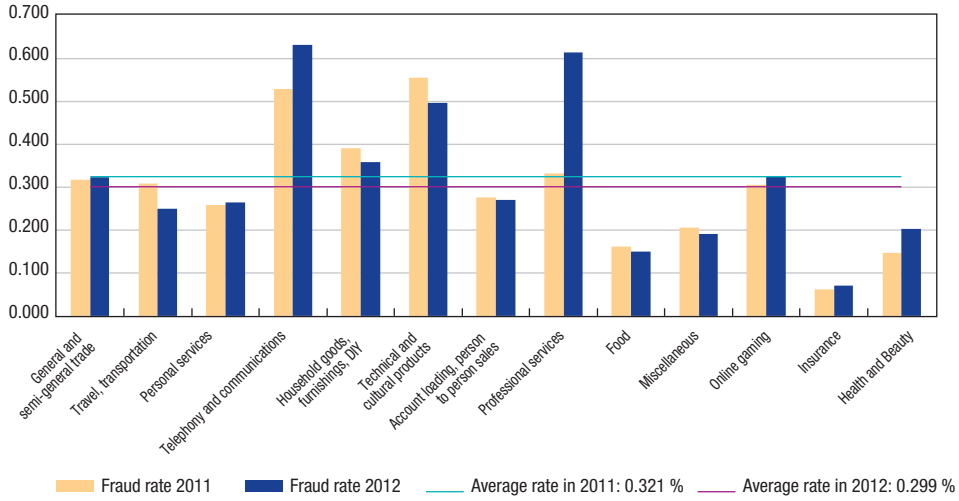
The general and semi-general trade, travel/transportation, personal services, and telephony and communications sectors were the most exposed to internet fraud, accounting for 69% of the total. A comparison of average fraud rates for each sector of activity provides additional information, revealing that some sectors, including technical and cultural products and professional services, have considerable exposure despite accounting for a small portion of the total fraud amount.

The travel/transportation sector is no longer at the top of the rankings, and fraud in this sector fell in 2012 to EUR 25.7 million compared with EUR 31.9 million in 2011. This decline is attributable to the introduction of strong cardholder authentication systems by major players in the sector (in particular Voyages-SNCF and Air France).

Chart

Domestic fraud rate for CNP payments, by sector of activity

(%)



1 *Cf. Appendix 6 for sector descriptions.*

5| Breakdown by fraud type

The Observatory breaks down fraud into the following types:

• lost or stolen cards that fraudsters use without the knowledge of the lawful cardholders;

• intercepted cards stolen when issuers mail them to lawful cardholders;

• forged or counterfeit cards, when an authentic payment card is forged by modifying magnetic stripe data, embossing or programming. A counterfeit card is produced using data gathered by the fraudster;

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

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

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

Fraud involving the use of misappropriated card numbers for CNP payments is the most common type of fraud (61.2%), and increased slightly from 59.9% in 2011. After increasing to 36.1% in 2011, fraud involving lost or stolen cards fell, accounting for 34.9% of fraudulent domestic payments. Counterfeit cards accounted for just 2.6% of fraudulent domestic payments, a slight increase from 2011 (2.3%).

"Other" fraud was down. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for some 35% of the fraud involving these cards.

Table 5

Breakdown of domestic payment fraud by fraud type and by type of card in 2012

(amounts in EUR millions, % shares)

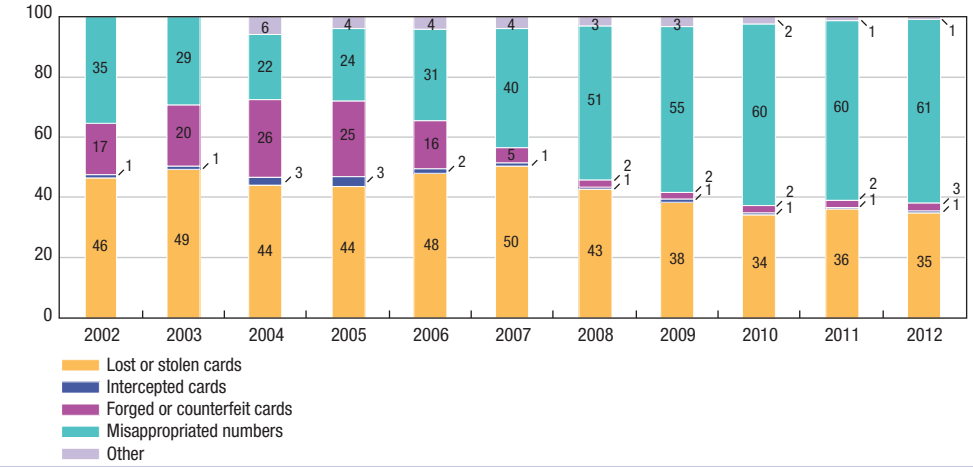
	All types of cards		Four-party cards		Three-party cards	
	Amount	Share	Amount	Share	Amount	Share
Lost or stolen cards	78.9	34.9	78.1	35.4	0.8	14.7
Intercepted cards	1.1	0.5	0.6	0.3	0.5	9.8
Forged or counterfeit cards	6.0	2.6	5.3	2.4	0.6	11.7
Misappropriated numbers	138.5	61.2	136.8	61.9	1.6	30.1
Other	1.9	0.8	0.1	0.0	1.8	33.7
Total	226.4	100.0	221.0	100.0	5.4	100.0

Source: Observatory for Payment Card Security.

Chart 4

Breakdown by fraud type (domestic transactions, fraud amount)

(%)



Source: Observatory for Payment Card Security.

Box 3

Indicators provided by law enforcement agencies

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

ATM attacks jumped to around 1,100 in 2012, compared with 634 in 2011, 527 in 2010, 526 in 2009, 427 in 2008, 411 in 2007, 526 in 2006, 200 in 2005 and 80 in 2004. There were also 100 attacks on POS (compared with 33 in 2011) including 26 on payment terminals (32 in 2010) and 28 on card-operated fuel pumps (none in 2011). These figures corroborate the statistical uptrend noted by the Observatory in withdrawal and payment fraud.

Technology watch

1| Security of contactless card payments in the light of recent developments

In its 2007 and 2009 annual reports, the OSCP examined the security of contactless cards and put out recommendations to promote controlled development in this area.

While in 2007 the deployment of contactless cards was still limited, the 2009 study sought to revisit the recommendations to take into account the expected spread of these cards and the introduction of pilot schemes for contactless payments by mobile phone.

In view of the growth in the number of contactless cards now on the market, the proliferation of compatible terminals and the publication of research on issues relating to this technology, the Observatory decided to update its previous studies as part of its 2012-2013 work programme. Since there were fewer noteworthy developments over the period in contactless payments by mobile phone, the following study concentrates primarily on the security of contactless card payments.

1|1 Action on the Observatory's recommendations (2007/2009)

The Observatory was quick to begin looking at the question of contactless payments. In its 2007 and 2009 annual reports, the Observatory published security analyses along with recommendations covering the identified risks. A review of these recommendations follows.

1|1|1 Prevent fraudulent gathering of card data

Contactless media may be exposed to the risk that data exchanged by radio waves with the payment terminal could be captured. They may also be used to generate payment transactions without the cardholder's knowledge. Although these risks are mitigated by individual or cumulative thresholds that cause media to switch back to contact mode when breached, in 2009 the Observatory recommended that issuers continue to explore simple solutions to activate and disable the contactless payment mode.

One solution mentioned in 2009 uses protective cases to block the radio waves that can be picked up by contactless cards' antennae.

Other solutions to disable the contactless payment mode are also possible. For cards, implementation of EMV (Europay MasterCard Visa) scripts for transactions in contact mode (for example when withdrawing money from an ATM – automated teller machine) makes it possible to disable the contactless function following a request from the cardholder or issuer.

The Observatory notes that contactless card issuers are now in a position to follow its recommendations, either by providing protective cases, which are easy to distribute, or by introducing an EMV script-based function in their systems to disable contactless mode. Some institutions also say they are ready to provide their cardholders on request with cards that do not offer the contactless functionality.

1|1|2 Limit the scope for reusing compromised data

To limit the scope for reusing compromised data, in 2009 the Observatory recommended examining the possibility of providing payment media with a special primary account number (PAN) for contactless face-to-face payments that is different from the PAN used in contact mode. This would protect compromised card numbers from being reused for something other than a contactless payment, since the issuer's authorisation system would block any other use.

Contactless cards do not currently offer this functionality, which is still being studied. However, the risks associated with the reuse of compromised data seem limited for several reasons:

• in the case of a face-to-face sale, the data on the contactless chip transmitted by the card to the terminal are different from those contained on the magnetic stripe, making it impossible to clone a valid stripe card with data captured in a contactless transaction;

• in the case of a CNP sale, it remains theoretically possible to reuse compromised data via the contactless interface because some transactions may be accepted without a card verification code. In 2008, the Observatory recommended always using the card verification code in CNP sales, since this number is printed on the back of the card but is not transmitted in card/payment terminal exchanges.

In the case of transactions with French merchants, the "CB" Bank Card Consortium has made it mandatory to use the card verification code since 2008 for "CB" transactions initiated online ("CB" card issuers are required to refuse a transaction if the card verification code is not given). The consortium is currently engaged in initiatives aimed at sharply reducing the number of transactions without card verification codes, with a particular focus on mail and phone transactions.

In the case of transactions with foreign merchants, the Visa and MasterCard international card payment schemes are also calling for widespread use of card verification codes, notably through the actions of the European Payments Council (EPC) in Europe.

An effective way to combat fraud in CNP sales conducted over the internet is to introduce one-time cardholder authentication when shoppers make purchases on merchant websites. The Observatory has been recommending this measure for several years in France, and was joined in this in early 2013 by SecuRe Pay, a forum of European supervisors and central banks.[1]

1|2 Recent developments (2009-2013)

The security of contactless payment cards and near field communication (NFC), the technology used in this area, was the subject of a variety of publications and presentations[2] in the first half of 2012. Some potential weak spots were identified. The Observatory reviewed this information to determine whether it needed to adjust its recommendations to issuers.

The publications dealt chiefly with eavesdropping on communications between a contactless card and a payment terminal to retrieve the exchanged data for use in fraudulent transactions. They also looked at activation of contactless media beyond the short distance required for legitimate payments with a view to entering into contact with the payment card and having it execute transactions without the holder's knowledge. Potential developments were described for these different scenarios, which included extending the range for eavesdropping or activating contactless devices (to a few metres rather than a few centimetres during normal operation). The Observatory looked at whether these technical procedures called into question its analyses of 2007 and 2009, which had previously flagged these risks.

The studies also describe new weak spots that could allow a fraudster to attempt to block a payment card by opening communications through the contactless interface to check the PIN used in contact mode.

1 Recommendations available at: *http://www.ecb.int/press/pr/date/2013/html/pr130131_1.en.html*.
2 Presented notably at the Hackito Ergo Sum conference in April 2012.

1|2|1 Eavesdropping on contactless transactions and unlawful remote activation of media

Affected data

The published studies covered the type of information that could be compromised during eavesdropping of communications between a contactless card and a payment terminal or other NFC-compatible reading solution, including the cardholder's name, the card's PAN and expiry, a partial copy of the data on the card's magnetic stripe and a history[3] of the most recent transactions carried out in contact or contactless mode (up to 100 or so transactions depending on the issuer's personalisation settings).

However, at the urging of card payment schemes, issuers' procedures for personalising contactless cards have changed since these studies were released. For the vast majority of cards issued in France, the cardholder's name can no longer be accessed during contactless exchanges. As regards accessing the transaction history on contactless media, the "CB" scheme has taken the step of prohibiting these data from being read by the contactless interface, a measure that applies to all products now presented for approval.

Eavesdropping on communications

Eavesdropping consists mainly in using a specific solution to intercept and retrieve the information exchanged between a contactless card and a compatible payment terminal. The attacking solution does not need to provide power to the contactless card, because the legitimate terminal does this. Positioning and distance challenges make this an extremely complicated type of attack to carry out, as the Observatory has noted in the past. To date, only special hardware and a lab-type controlled environment can reproduce this kind of scenario. Bringing in additional devices to extend eavesdropping distances merely raises further operational difficulties.

Unlawful remote activation – opening communications with the card

This type of attack consists in activating the contactless card in place of a legitimate system, such as a payment terminal during a transaction between a cardholder and merchant. To do this, an NFC reader combined with an active antenna are needed to power the card. The activation distance for the medium varies in a non-linear fashion according to the antenna used and the power provided by the system. It has been demonstrated that this distance cannot be extended beyond a few dozen centimetres, again under conditions that are difficult to reproduce outside a laboratory. Moreover, the strength of the magnetic field needed to directly activate the card at greater distances might present a danger to the criminal and his surroundings, rendering this scenario unrealistic in practice.

To get round these physical challenges, a system of relays could be used to reduce the activation distances and hence the intensity of the required magnetic field. This would consist in using intermediate devices to relay the signals between an attacking reader and a legitimate payment terminal. The Observatory looked at this possibility in 2007 and concluded that there was a low level of risk, mainly owing to the technical challenges involved in actually implementing the solution and keeping within the transaction time. Moreover, the potential gains for the criminal and any accomplices are minimal, since contactless transactions involve small amounts and are subject to thresholds.[4] The Observatory will however remain watchful for developments in this type of attack.

3 Date, country, amount and currency mainly.
4 Both for the number of transactions and also the total cumulative amount, before having to switch back to contact mode with PIN entry.

Box 1

Protecting personal data

France's Data Protection Act[1] seeks to protect citizens against harm arising from the use of computer resources. It applies to all processing of data of a personal nature, whether the person is directly or indirectly identifiable, for example by means of an identification number.

Contactless payment cards are thus subject to this legislation. Accordingly, issuers must comply with various rules, including the requirement to ensure that data are appropriate and proportionate given the proposed use by the party responsible for processing. Issuers must also ensure that such data are protected.

France's Data Protection Agency (CNIL) considers that making the cardholder's name accessible via the contactless interface, whereas this information is not used to conduct a payment transaction, is inappropriate. Moreover, such disclosure poses a risk to the privacy of cardholders, who may be identified by this means. The CNIL notes that this information is no longer accessible in contactless mode with "CB" cards.

Similarly, the CNIL considers that having the history of payments made in contact and contactless modes accessible via the contactless interface also raises privacy issues, by making it possible to obtain information on the cardholder's habits and travel. The CNIL has noted the decisions already taken on this point and will consider proposed developments in light of the principles set down by law.

The CNIL also considers that the ability to obtain the PAN by opening up communications with the card or by intercepting legitimate transactions remains a point to watch, since this personal information is protected by law.

The CNIL has published a summary of these points at http://www.cnil.fr/cb-sans-contact/

1 *Data Protection Act 78-17 of 6 January 1978 (amended), which states that "*Information technology should be at the service of every citizen. Its development [...] shall not violate human identity, human rights, privacy, or individual or public liberties*".*

1|2|2 Locking contactless payment cards

The published studies highlighted the possibility that fraudsters could deliberately lock payment cards by opening communication with the contactless interface to verify the PIN. While the chances of guessing the card's actual PIN are slim, since only three attempts are allowed, such an attack could, according to the studies, cause the card to be locked after three failed attempts.

The Observatory has found that cards issued in France are not vulnerable to this type of attack, because they cannot be contacted through their contactless interface for PIN verification purposes.

Another potential attack consists in attempting to reach the maximum number of transactions for the payment card by asking it to perform numerous transactions through its contactless interface. The card has a specific counter for this purpose.

However, since reaching the limit would take several hours given the time needed to complete each transaction, this type of attack seems unrealistic.

1|3 Conclusions of the Observatory's work

The Observatory reviewed studies published in early 2012 on the security of contactless payment cards to determine whether the analyses and recommendations that it issued in 2007 and 2009 were still valid. Given the sharp growth in compatible terminals and the mass issuance of contactless

payment cards, the Observatory will continue to closely monitor this question to ensure that those involved in deploying these solutions have a full command of all the security aspects.

The abovementioned analyses show that the risks linked to eavesdropping on contactless transactions and unlawful remote card activation remain weak because they entail challenging technical procedures that necessitate lab-type equipment and environments. In addition, the presence of thresholds for contactless transactions, which are limited to small payments, greatly reduces the financial gains from fraud in the event of loss or theft. The Observatory will however remain attentive to developments in this area.

Furthermore, the Observatory notes that certain areas of weakness depend to an extent on issuers' card personalisation settings, some of which limit or even eliminate the risks linked to the disclosure of information that may be retrieved through the contactless interface. In France, for example, contactless cards issued today can no longer be used to capture the cardholder's name. Also, the new card products authorised by the "CB" Bank Card Consortium do not permit access to the payment history. In any event, these data cannot be used to carry out a fraudulent payment transaction.

The Observatory believes that there is currently no risk of cards being locked if fraudsters attempt to conduct repeated "verify PIN" attempts on the contactless interface or carry out many contactless transactions in a bid to reach the limit on the card's transaction counter. Cards issued in France cannot be used to verify the PIN in the first scenario, while the practicalities of the second scenario render it unrealistic.

In view of the above, the Observatory considers that the main risk associated with contactless card payments is reputational risk, but that no noteworthy fraud-related consequences need to be highlighted. That being said, given the progress in current initiatives in France and to maintain cardholders' confidence in this payment instrument, the Observatory reiterates the recommendations made in 2009.

As regards disabling the contactless function of payment cards, issuers have made a commitment to provide users with protective cases, or to introduce solutions to enable remote deactivation of the contactless function, or to replace contactless cards with media that do not have the functionality at the request of cardholders. The use of a specific PAN for contactless payments – an area recommended for study in 2009 – could also help to foil any attempts to capture card data for fraudulent reuse through other channels and particularly in CNP sales over the internet. In the case of internet sales, the Observatory recommends pursuing the deployment of measures to protect CNP transactions through one-time authentication.

The Observatory also recommends that issuers and card payment schemes continue to implement measures to limit the exchange of sensitive information during transactions in contactless mode. Eavesdropping on communications and the possibilities for subsequent reuse of compromised data could be nullified by encrypting communications between contactless cards and payment terminals. A study of the costs and benefits of this type of measure could be conducted to assess the technical feasibility and scope in terms of fraud prevention.

The Observatory stresses that these measures must be implemented within an international setting. It therefore calls on payment chain participants to take concerted action with their counterparts in Europe and beyond to increase the effectiveness and scope of their initiatives. In this respect, building on work by the Observatory, SecuRe Pay has taken on the subject of contactless payments, initially via mobile phone, with a view to issuing recommendations in this area.

2| Fraud techniques

Fraud in card transactions is under control in France and at extremely low levels, especially for withdrawals and domestic face-to-face payments. However, this is a key area for the Observatory which has, since its inception, monitored fraud techniques and recommended measures to limit and mitigate them.

Reflecting technological change and the growing number of international payments, fraud techniques have evolved considerably in recent years. Accordingly, while previous reports may have spotlighted certain methods, the Observatory decided that it needed to update its review of fraud techniques.

Whether the fraudster is seeking personal gain or to expose gaps in protection systems, he captures card data either by stealing authentic media or by deploying tools to misappropriate[5] or create card data to reuse them in the payment chain. While determining the origin of fraud in these different cases is complex, evidence shows that fraud can affect the whole payment chain, including the card itself, but also acceptance and information systems. In terms of reuse, however, CNP internet transactions (distance sales) are the prime channel for reusing card data (cf. Chapter 2 of this report: *Fraud Statistics for 2012*). In this regard, since 2008 the Observatory has stressed the need to introduce one-time authentication for online transactions on a general basis, since this is one of the truly effective ways to reduce the opportunities for reusing card data.

After listing the compromise (capture) techniques currently observed, this section of the report looks at measures used to combat card data capture before describing the tools used to reduce the scope for reusing misappropriated data.

2|1 Techniques for compromising card data

Internal or external attacks targeting information systems are the most fruitful because they make it possible to obtain large quantities of data. Attacks on cards, mobile phones, payment terminals and cash-out machines (COMs) are hard to perform and execute on a large scale because of the inherent qualities of the hardware. Regardless of the methods used, however, these attacks have a major impact because the payment card has become such an everyday tool.

2|1|1 Via information systems

Since card data are conveyed right along the payment chain, they may be subject to capture by people with malicious intent. Each point in the chain therefore needs adequate protection. These include users' (consumers or merchants) personal computers, merchant databases for CNP transactions, payment concentrators for face-to-face transactions and processor-managed systems in all cases. Mobile phones, which are more recent arrivals in the card ecosystem, now present another potential target in the same way as computer hardware.

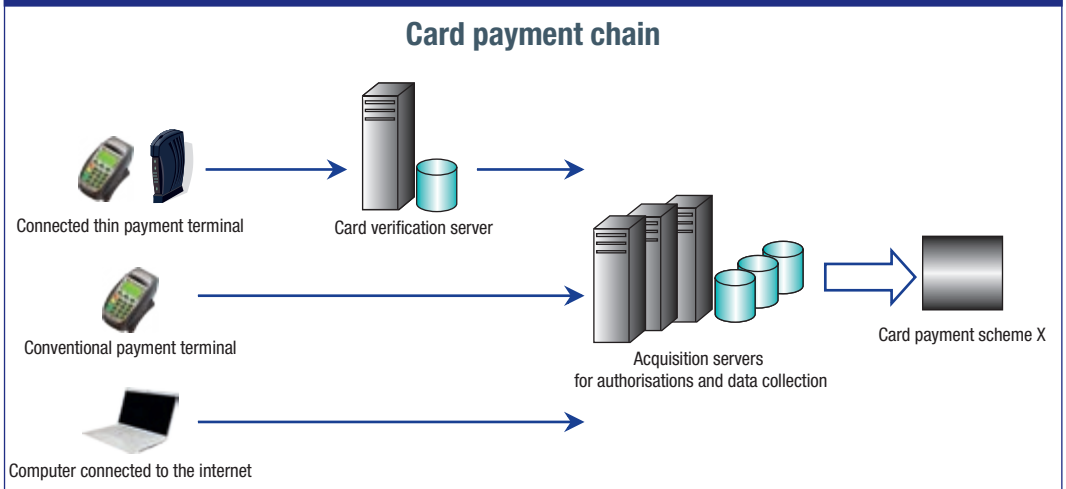
Personal computers may be the victims of attacks aimed at capturing insufficiently protected data. This type of attack requires the user to first unknowingly install malware[6] contained in seemingly trustworthy sources. Card data entered on the computer may, for example, be captured by means of keylogger malware that records keystrokes.

Mobile phones, which are increasingly used for card payment transactions,[7] may also be affected by malware that infects the device in order to compromise the user's personal data, including card data. This type of software may also misappropriate one-time codes sent by the card issuer to the rightful user, enabling the fraudster to complete a transaction on a secure site. ZitMo (for "Zeus in the Mobile") is an example of this type of malware.

Beyond individual attacks, the databases compiled at different stages of transactions have become extremely attractive to criminals because of the volume of useable data. In recent years, theft of

5 Misappropriation of card data implies that a portion of the data is compromised without the knowledge of the lawful cardholder.
6 Malware is all or part of a piece of software that is designed to damage an information system.
7 Whether as a payment instrument or for authentication.

Box 2



bank data held by merchants or card data processors (Wal-Mart, Sony, Heartland Payment Systems, RBS Worldpay and others) have received media coverage following cases of online compromise or malware introduced into systems through physical media (USB keys, hard drives, etc.).

2|1|2 Through the internet

A fraudster may get cardholders to share their personal data, including card data (PAN, PIN, expiry, card verification code) or authentication data (mobile phone number to which one-time codes are sent). This is called phishing. This type of attack is usually based on sending emails that display logos or visual identities known to recipients (belonging to credit institutions or merchants, for example) and asking victims to connect to a bogus website whose sole purpose is to collect sensitive information. Vishing is a variant that employs other channels, such as the telephone, in the same way.

Pharming consists in manipulating DNS servers[8] to redirect the user to a bogus website that looks the same as the legitimate site. Criminals may also create complete fake e-commerce sites to fraudulently gather funds and/or card data.

2|1|3 By mail or over the phone

During MOTO[9] transactions, which involve some manual processing, people with malicious intent may record card data during payments or reservations.

2|1|4 Via acceptance devices or networks

Acceptance devices (UPTs, COMs and payment terminals) may be subject to physical or logical attacks aimed at misappropriating card data. This section will address frauds linked directly to the use of a payment or withdrawal card.

8 DNS servers associate the names of websites (easy to remember) with their IP addresses (series of numbers).
9 Mail Order Telephone Order, i.e. transactions initiated by mail or telephone (voice).

Physical attacks on acceptance devices

Acceptance devices and networks conveying data between them and acquisition servers may be targeted by attacks aiming to capture card data.

In the case of UPTs and COMs, the most widely used technique is skimming, which consists in capturing the data contained on cards' magnetic stripes without the cardholder's knowledge.[10] The approach used is usually discreet enough to avoid attracting attention. For example, the entire front of the machine or just the card slot may be fake to disguise the illegal device. The approach is typically combined with a video camera and/or a fake keypad to capture the PIN and may also include systems to store or transmit compromised data.

Another technique is to keep the card in the automated terminal so that it may be reused later. To do this, the criminal inserts a device, which may be fairly rudimentary,[11] in the automated machine, watches the PIN being entered on the keypad, and retrieves the card once the cardholder has left. This technique is akin to card theft.

Similar skimming techniques may be used with POS payment terminals to capture stripe data or the cardholder's PIN.

Logical attacks on acceptance devices

In addition to the physical methods described above, a second category of attacks aims to exploit security gaps in the logical elements of automated machines and terminals. The goal is to inject malicious code into the systems of these devices to alter their behaviour or take control over their components (keypad, screen and printer). These attacks may be perpetrated by people with special access to these devices, such as maintenance personnel and operators.

Attacks on networks

Networks themselves may be the targets of attacks when data are exchanged between acceptance devices, payment concentrators, where applicable, and acquirers' servers. These data are transmitted over networks that use two different technical approaches: wireless (Bluetooth, Wifi or GPRS) or wired (cable or fibre optic). In both cases, the internet protocol (IP), on which the internet is based, is now the main communication protocol used.

Accordingly, IP networks may be targeted by fraudsters seeking to exploit vulnerabilities in order to gain access to devices or capture exchanged data.

2|1|5 Via the card itself

Aside from stealing cards, attempting to disrupt card protection systems remains a prime activity for fraudsters and hackers because of the potential publicity. Publications in recent months have shed light on various scenarios involving attacks on payment card security in contact and contactless modes.

The introduction of effective protection measures, a summary of which is provided in Table 1 at the end of this section, has limited the scope of such attacks, which may require laboratory conditions to be feasible and effective.

Theft and counterfeiting of legitimate instruments

The physical theft of a payment instrument so that the criminal can use it instead of the lawful cardholder is a type of attack. To maximise the potential value of each instrument stolen, the fraudster usually tries to get the card's PIN as well and ensure that it takes as long as possible for the cardholder to report the payment instrument stolen.

10 For more on this topic, see the Observatory's 2010 report.
11 A variety of techniques are used, referred to collectively in France as the "Marseilles snare".

This allows the card to be used at ATMs, in payment terminals and for all types of online transactions.

The "man-in-the-middle" attack, which first emerged in 2012, consists in fooling the automatic controls run by a payment terminal and a lost or stolen card by manipulating the link between the two. However, this technique is extremely complicated to implement and cannot be used for transactions authorised online or cash withdrawals, which greatly limits their appeal for criminals, who are chiefly interested in the ability to withdraw cash.

Some fraudsters also use software that generate card data[12] to reuse them in CNP transactions.

Attacks on cards in contactless mode

The Observatory was quick to study the security implications of contactless payments by card and mobile phone. These concerns led to the publication of security analyses together with recommendations covering the risks identified in the 2007 and 2009 reports, which are updated in this report (cf. Chapter 3: *Update on the security of contactless card payments*).

2|2 Measures to prevent card data capture

While combating social engineering attacks is largely based on first raising awareness among potential victims, information systems must meet security standards that can mitigate the identified risks.

2|2|1 Protecting against attacks on information systems

In general, information systems must be protected against internal and external threats and accordingly be covered by security analyses aimed at establishing protective measures that are suited to the environment in which these systems operate.

The information systems used to carry out card payment transactions fall into this framework. Their operators need to establish a security policy and regularly assess the risks to which they are exposed. Various methods are available for this, including the Ebios method, which is prepared and maintained by France's National Agency for Information Systems Security (ANSSI), and the ISO 27000 series of standards.

Given the highly sensitive nature of the data conveyed or stored on these systems, they are subject to additional Payment Card Industry (PCI)[13] measures developed by the PCI SSC[14] consortium. These measures apply globally to all participants in the acceptance and acquisition chain, including acquiring banks, merchants and service providers operating payment platforms. Several series of measures have been established under the PCI Data Security Standard (PCI DSS) to protect data, whether they are transmitted through information systems in the card payment acquisition chain or stored in these systems. More recently, PCI SSC published a guide to applying these measures to cloud computing,[15] which included identifying the responsibilities of each participant within this architecture.

In the area of attacks on databases, a draft European directive on measures to ensure a high common level of network and information security across the Union[16] is currently under discussion. It could require banks, but also e-merchants, to introduce data protection systems that are consistent with a risk assessment and to report to the authorities any breaches of databases containing customer information and particularly information about payment instruments.

12 Through successive iterations, this kind of software generates card numbers, expiries and sometimes card verification codes.
13 For more on PCI measures, see the Observatory's 2010 report.
14 The Payment Card Industry Security Standards Council was established by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.
15 Consists in making shared IT resources available and accessible via a telecommunications network.
16 Draft Directive 2013/0027 (COD) – Ordinary legislative procedure – pending first reading in Parliament.

2|2|2 Protecting against online attacks

While the gradual deployment of one-time authentication for internet purchases reduces the risks that card data captured without the cardholder's knowledge will be reused, raising user awareness about questions of security is still the only way to combat social engineering attacks. All payment chain participants have to take the initiative to communicate effectively on these issues using all available channels, including mail, email and websites. Cardholders must be encouraged to use only trustworthy websites whose security level is consistent with the terms of reference given in these communications.

Finally, the abovementioned security policy must encompass measures ensuring the security of data at the moment when they are entered in the systems. To ensure that there is a reliable audit trail, the policy should provide for a log to be made every time the information system is accessed to enter or modify data needed to conduct transactions.

2|2|3 Protecting against card data capture by email or phone

Employee wrong-doing is usually responsible for compromise in this setting. Acceptance solutions that limit interaction between merchants and payment instruments must therefore be given priority. It is also important to limit card data access to duly authorised employees and to refrain from keeping sensitive data when no longer required.

2|2|4 Protecting against attacks on acceptance systems or networks

Protection for the acceptance chain is based on protecting all of its individual components as well as the solutions that link them together.

Measures to prevent physical attacks on acceptance devices

Operators of UPTs and COMs have a variety of technical means at their disposal to prevent the risk of skimming. Anti-skimmers are extensions affixed to automated machines to prevent criminals from adding on their own equipment.

Banks need to protect their equipment against fraudsters looking to introduce systems to copy card data. Cardholders, meanwhile, must remain on the watch for tampering with UPTs and ATMs.

The Observatory recommends that institutions that operate automated machines raise awareness among employees about the risks to these devices to help them spot any tampering promptly and keep any evidence that will help law enforcement investigations.

There are two sorts of measures that can help acquiring institutions to protect themselves against the risk of skimming on payment terminals:

- it is vital to raise awareness among merchants about the need to be attentive at all times to suspicious behaviour by employees or customers involving payment terminals;

- card payment schemes and acquiring institutions need to be able to spot any attempt during transactions by an illegal system to intrude into authorisation networks. Accordingly, the Observatory recommends that affected players ensure strict traceability for acceptance devices at POS based on information transmitted by these devices.

Measures to prevent the injection of malicious code

In 2008, the Observatory recommended tightening up the security of the operating systems used by automated machines, notably by disabling

or eliminating unused software components and functionalities, and by restricting access to certain data.

Given the identified risks, these recommendations may now be extended to payment terminals, which should be developed in accordance with state-of-the-art techniques. This also implies carrying out regular tests including the operating system and the applications housed on these devices to continually assess the overall level of security and ability to withstand attacks.[17]

The Observatory also recommends that affected players take account of these development techniques in the processes for certifying and approving these devices.

Measures to protect networks

The linkages between acceptance devices and acquiring servers are based on the use of open networks. They are protected by payment chain participants through implementation of the measures recommended by the card payment schemes, either directly or via PCI SSC.[18]

Among other things, PCI DSS measures require card payment data sent over open networks to be encrypted to ensure their protection. In France, the "CB" Bank Card Consortium also requires transaction data to be encrypted even when sent over virtual private networks. It additionally requires use of the TLS[19] security protocol or equivalent, which covers authentication of payment concentrators and acquisition servers using certificates.

Where automated machines and terminals communicate using wireless technologies, encryption and authentication measures are recommended for exchanges between these devices and wireless access points linked to wireless networks, as allowed by Wifi and GPRS.

2|2|5 Protecting against attacks on payment cards

The man-in-the-middle type fraud described in 2|1|5 can only be carried out in face-to-face transactions where the cardholder's PIN is verified locally.

One possible protective measure would therefore be to require all transactions to be authorised online. However, this would mean that the network would have to be appropriately sized and longer transaction times would have to be accepted.

Given these challenges, the "CB" Bank Card Consortium has gravitated towards another solution based on anticipating a scheduled transition to CDA,[20] a new method of authenticating cards during exchanges with terminals. The Observatory recommends that affected players continue to migrate cards and terminals to this new authentication mode within a timeframe consistent with the underlying risk.

As regards measures to protect transactions carried out in contactless mode, the Observatory reiterates (cf. Chapter 3: *Update on the security of contactless card payments*) the measures recommended in 2007 and 2009, which now need to be considered from an international perspective. It accordingly encourages issuers to provide protective cases for cardholders or to introduce measures to remotely disable the contactless function. It stresses once again the value of introducing a separate PAN for contactless payments to foil attempts to capture this number and reuse it through other channels. Furthermore, the Observatory recommends conducting a study of the costs and benefits of developing the contactless communication protocol to enable encryption as standard of the data conveyed through this channel.

17 One method is fuzzing, which consists in injecting random data to the inputs of a computer programme and then assessing the effects.
18 These measures are detailed in the Observatory's 2008 report.
19 Transport Layer Security has replaced Secure Socket Layer version 3 (SSL V3). This is a security protocol that ensures the integrity and confidentiality of exchanged data as well as authentication of communicating devices.
20 Combined Data Authentication: this authentication method, which is included in the EMV standard, uses the card's authentication key to sign transaction data.

2|3 Measures to prevent reuse of misappropriated data

Irrespective of the channel through which card data are compromised, they are mostly reused in CNP sales environments (cf. Chapter 2: *Fraud Statistics for 2012*) since internet payments currently appear less well protected than face-to-face payments, whose security measures have proven their effectiveness.

2|3|1 In CNP sales

To combat the steady rise of CNP payment fraud, in 2008 the Observatory recommended two types of measures:

• first, systematic use of the card verification code, which is written on the card but not sent during exchanges between the card and the payment terminal, makes it possible to ensure that card data have not been compromised by skimming, as described in 2|1|4. This measure is recommended by card payment schemes, which are lobbying to have it adopted generally at international level;

• second, the Observatory recommends that payment chain participants (issuers, acquirers and merchants) implement strong cardholder authentication for transactions that are deemed to be high risk. As part of the approach now being taken forward on a Europe-wide basis by SecuRe Pay, the e-merchant community generally should start analysing transactions potentially requiring one-time authentication.

2|3|2 In face-to-face transactions

Use of the EMV standard developed by the EMVCo[21] consortium ensures a high level of security for card transactions in face-to-face settings.

Back in 2003, the Observatory recommended generalising use of EMV for face-to-face transactions. It regularly monitored progress in Europe's migration to the standard, which is now virtually complete, publishing the results in its annual reports.

In the longer term, and given the spreading use of smart cards internationally, the Observatory recommends that issuers remove sensitive data that may be used to carry out face-to-face payments from magnetic stripes.

Furthermore, to combat wrong-doing by employees, priority should be given to acceptance solutions that limit interaction between merchants and payment instruments during face-to-face transactions, to allow cardholders to keep control of their payment instruments at all times. It is also important for merchants to be constantly on their guard, keeping watch on how customers use payment terminals.

In addition to security solutions for cards, acquirers have other technical means at their disposal to limit the reuse of cards compromised in face-to-face transactions, such as downloading lists of blocked card numbers to terminals.

2|4 Conclusion and guidance for affected participants

Despite enjoying a high level of security, card data are subject to attacks as they move along the payment chain. Potential points of compromise present themselves in both the physical and virtual worlds, necessitating constant vigilance by all participants in all environments.

The main targets are information systems and networks, because of the volume of data stored or conveyed by these infrastructures, for which adequate protection measures, such as PCI DSS, must be implemented. But more conventional methods targeting automated machines are also in use. Accordingly, protecting machines and payment terminals must remain a priority for manufacturers

21 EMVCo is made up of American Express, JCB Cards, MasterCard and Visa.

and developers beginning with the design phase, when state-of-the-art methods must be applied. The Observatory recommends that certification or approval bodies include these requirements in their own procedures.

The Observatory repeats its advice to cardholders to be on their guard and recommends that merchants be extremely watchful to ensure that devices used for face-to-face transactions are not switched. The Observatory also recommends that acquisition chain participants keep careful logs for the equipment deployed in face-to-face environments to prevent any attempts to tamper with or switch such equipment. The same level of traceability should be applied to data entered during CNP transactions.

The members of the Observatory (notably banks, card payment schemes, merchant and consumer associations and public bodies such as ANSSI) have posted materials on their websites[22] with information about some of these good practices.

The Observatory also reiterates its earlier recommendations aimed at limiting the reuse of compromised data in CNP transactions. Measures to promote widespread use of the card verification code and strong cardholder authentication (the latter for the highest-risk transactions) must continue to be the focus of a sustained drive by all members of the payment chain, in view of the fraud rates recorded for this channel.[23]

With fraud techniques evolving all the time, the Observatory will pay close attention to the rapid rise of new payment modes using cards, digital wallets and mobile phones, and to the deployment of appropriate security measures by participants as part of efforts now being taken forward in a European and international setting.

22 Cf. Table 2 at the end of this section.
23 Cf. Chapter 2 of this report: *Fraud Statistics for 2012*.

Table 1

Security measures recommended by the Observatory in previous reports

Type of risk	Recommended measures	Report
Counterfeiting	Insert hologram	2003
	Use cryptographic processes for component identification	2003
	Certify components (cards, terminals)	2005, 2007, 2009
Card theft	Introduce EMV standard generally	2003, 2005, 2007
	Authenticate cardholders using PIN	2007, 2009
	Set thresholds for transactions in contactless or prepaid mode	2007, 2009
	Use fraud detection systems	2003, 2009
Compromise of card data	Fight phishing, communication campaigns	2004, 2006
	Ensure end-to-end data protection (encryption), use private networks	2003, 2004, 2005, 2006, 2008, 2009
	Use card verification code for CNP transactions	2004, 2008, 2009
	Use virtual dynamic cards	2005, 2008
	Protect sensitive data by applying international standards	2005, 2006, 2007, 2008, 2009
	Enhance physical security of automated machines and instant issue systems	2006, 2008
	Restrict use of stripe readers in automated machines	2006
	Use dedicated PAN for certain modes (contactless, mobile)	2007
	Have function to disable radio transmissions in contactless mode	2007, 2009
	Use cases that block radio waves	2007, 2009
Online identity theft	Strong cardholder authentication (also called one-time authentication)	2008

Table 2

Examples of good practices – links to websites of bodies represented within the Observatory

GIE Cartes Bancaires	*http://www.cartes-bancaires.com/spip.php?article73*
	http://www.cartes-bancaires.com/spip.php?article72
CRCAM de Paris et d'Île-de-France	*https://www.ca-paris.fr/site-securite.html*
LCL	*https://informations.lcl.fr/securite/*
BPCE	*http://www.banquepopulaire.fr/Institutionnel/a-savoir/securite-internet/Pages/securite-internet.aspx*
	https://www.caisse-epargne.fr/particuliers/ile-de-france/securite_accueil.aspx
Association Leo Lagrange pour la défense des consommateurs	*http://www.leolagrange-conso.org/03_ress_01.php?idrub=OU&rub=3*
FEVAD	*http://www.fevad.com/espace-consommateurs*
ANSSI	*http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/*
Banque de France	*http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/La_Banque_de_France/pdf/La_Banque_de_France/BDF-IDENTITES_BANCAIRES-PDFELEC_VF_1_.pdf*
Fédération bancaire française	*http://www.lesclesdelabanque.com*

European and international regulatory developments and recommendations on payment card security

The payment card is the most widely used payment instrument in France and Europe by number of transactions. The ways in which it is used have evolved with technological advances – take the introduction of contactless card and online payments, for example. The challenge for regulators and overseers is thus to continually adjust supervisory mechanisms to preserve a high level of security for this instrument while promoting new types of use.

For this reason, the Observatory decided to conduct a review of the security rules and recommendations issued by authorities both within Europe and internationally. The following chapter will cover the main factors that have shaped changes to the operational and legal framework for card payments in recent years, before looking at actual or expected regulatory initiatives to address these changes. In accordance with the tasks assigned to the Observatory, this chapter will not deal with economic questions or issues of competition.

1| New ways of using payment cards are emerging

The payment card, which was initially designed to be used in face-to-face transactions, has established itself in many countries as the payment instrument of choice for CNP transactions as well. As part of this development, the rise of e-commerce and the use of new technologies have radically changed the ways in which cards are used as payment instruments as well as the associated acceptance methods.

1|1 The internet and new technologies have driven changes in card payments

1|1|1 Security of internet transactions

As internet card payments have become more popular, so fraud has steadily grown, as shown by statistics published by the Observatory for the past few years. This prompted international card payment schemes to develop the 3D-Secure protocol, which allows issuers to conduct strong authentication of cardholders online. To encourage merchants and acquiring banks to adopt this solution, its implementation is accompanied by a shift in liability in the event of fraud from the acquirer to the card issuer.

Since this type of security solution has not been adopted on a systematic basis, internet fraud remains at a high level, accounting for 57.6% of fraud but just 9.8% of all card payments in France.[1] This warrants continued efforts by payment chain participants to constantly improve the level of security for these transactions.

1|1|2 Face-to-face payments now offer a contactless functionality

Face-to-face transactions have also changed drastically. It is now possible to conduct contactless payments using a card or mobile phone, which communicate remotely with the payment terminal through NFC technology.[2]

1 Cf. Chapter 2 of this report.
2 Near Field Communication. For more on contactless payments, see Chapter 3 section 1|2 of this report.

The Observatory considers that reputational risk is the primary risk associated with contactless card payments. However, these payments do create new risks requiring specific security measures, as described by the Observatory in this report (cf. Chapter 3). These measures combine with those aimed at protecting face-to-face transactions and seek to preserve the high level of security enjoyed by this payment channel.

On the question of conventional face-to-face payments, it is important that affected participants continue to deploy EMV specifications internationally. In this report,[3] the Observatory repeats its advice to cardholders and merchants to be on their guard to prevent any attempt to tamper with or switch acceptance devices for fraudulent reasons.

1|1|3 Emergence of mobile payments

Many initiatives and innovations have emerged around mobile payments (or m-payments). For example, mobile applications have paved the way for e-wallet services that may be used to pay for online purchases. Similarly, phones can be used to carry out CNP payments in face-to-face settings.

A key innovation is the transformation of the mobile phone into an electronic payment terminal. These solutions were originally developed for the North American market, which is still based on magnetic stripe cards. However, their commercial success has opened up numerous possibilities in Europe. Care must be taken to ensure that these solutions are adapted to be consistent with the continued use of smart cards and EMV technology.

1|1|4 Rise of prepaid cards

Use of payment cards in their original format has continued to grow with the arrival on the market of prepaid cards, which remove the need for a bank account to make card payments, thus promoting financial inclusion. When these cards are anonymous, however, there is a risk that they could be used for laundering or terrorist financing, which prompted the president of the Observatory to warn the public authorities about these dangers.

To mitigate these risks, consideration should be given to identifying transactions conducted using anonymous prepaid cards and restricting their use at national, European or even international level.

1|2 A European legal framework that has introduced new non-bank participants

European legislators began working back in 2001 to harmonise the regulatory framework for payments law to facilitate the establishment of a single European payments market and increase competition.

Accordingly, the Payment Services Directive (PSD), adopted in 2007 and transposed in France in 2009 notably through Executive Order 2009-866 of 15 July 2009, governs all relations between payment service providers and their customers in payment transactions using credit transfers, direct debits or payment cards.

In particular, this legislation defines the content of framework contracts, procedures for executing and disputing transactions, and the role and responsibilities of each participant in these processes. The PSD covers two facets of card payments as payment services, namely "execution of payment transactions through a payment card or a similar device" and "issuing and/or acquiring of payment instruments".

European Directive 2009/110/EC on electronic money (EMD2) completed the regulatory framework for payment services. This directive was transposed in France by Act 2013-100 of 28 January 2013 and defines the regulatory framework for the issuance, management and distribution of electronic money in the European Community, an area that had not been reformed since 2000. Moreover, in France, the legislation provided[4] that all provisions relating to payment services apply to issuers of electronic money and associated payment services. This is the case,

3 Cf. Chapter 3, 2|2|4.
4 Art. L. 315-5 of the *Monetary and Financial Code*.

in particular, for obligations to provide disclosures to users and the procedures for disputing payment transactions. These are key clauses in the payment service framework contract that were specified by the Order of 29 July 2009 on relations between payment service providers and their clients.

Card payments are affected by EMD2 insofar as prepaid cards may be a medium for carrying out payment transactions in electronic money. As a result, prepaid cards must be subject to the same security rules as conventional payment cards (issued by a payment or credit institution), as pointed out by the Observatory in its 2010 report.

These two directives additionally created two new categories of non-bank participants that are allowed to offer payment instruments: payment institutions and electronic money institutions. By May 2013, 16 payment institutions and three electronic money institutions had been authorised in France.

2| Necessary adjustments in response to security developments in card payments

France's lawmakers have entrusted the Banque de France with overseeing the security and orderly operation of payment systems and instruments. Accordingly, the Banque de France works with card payment players to protect the entire chain, from issuance to acceptance and processing of all card-related flows (for a detailed review of the activities of the Banque de France, see its 2012 report).

The OSCP, which comprises public bodies, card payment entities and representatives of consumer associations, rounds out the overall system.

Faced with the evolving uses of payment cards described in the previous chapter, domestic and European authorities are adapting the applicable security requirements and regulatory framework to maintain a high level of security for card payments.

This topic is also being followed at international level, as demonstrated by recent work by the BIS Committee on Payment and Settlement Systems (CPSS).

2|1 Security recommendations issued by the OSCP and SecuRe Pay

2|1|1 Security of internet transactions

Steady growth of fraud in card payments during online purchases prompted the Banque de France and the Observatory to recommend deploying strong authentication for CNP payments wherever possible and appropriate (cf. Chapter 1 of this report).

Furthermore, the ECB-backed European Forum on the Security of Retail Payments (SecuRe Pay) also published a report in January 2013 on the protection of online banking services and the security of internet card payments. SecuRe Pay was set up in 2011 and brings together EU central banks and banking supervisors.

As part of this, SecuRe Pay issued recommendations for banks and payment service providers and advised using strong authentication for the highest-risk payment transactions.

2|1|2 Security of contactless and mobile payments

In France, the Observatory was quick to examine the security of payments by contactless cards, including by mobile phone (cf. studies published in the 2007 and 2009 reports as well as in this report) and has issued a number of recommendations to ensure that this area is developed in a controlled manner.

In the context of its 2013 work programme, SecuRe Pay is also devoting attention to issues relating to card payments by mobile. The related recommendations are expected to be put out to public consultation in the final quarter of 2013.

2|2 Developments in the European supervisory framework

2|2|1 The Eurosystem's framework for supervising card payments

The legislation that established the Eurosystem made supervising payment systems one of the Eurosystem's core responsibilities,[5] in order to ensure user confidence in payment instruments.

Accordingly, the Eurosystem supported the decision taken by the main European card payment schemes to gradually replace stripe cards with smartcards requiring PIN entry. This migration to EMV standards, which was accompanied by upgrades to acceptance terminals, greatly helped to enhance the security of face-to-face card payments and prevent fraud.

In 2008,[6] the Eurosystem created a supervisory framework to assess the security and effectiveness of card payment schemes. The framework enabled Eurosystem central banks to implement harmonised supervision and obtain a consistent and standardised vision of card payment schemes. One of the five established standards covers the security, reliability and continuity of payment schemes.

This supervisory framework will soon be adjusted to reflect the security developments mentioned earlier, and particularly the recommendations recently issued by SecuRe Pay.

2|2|2 Towards a new European regulatory framework for card payments

The European Commission is keen to keep step with changes in the area of payments by promoting the development of innovative and safe new services, reiterating that payment security and user confidence are among the key factors in the development of payment services. In addition, with the establishment of SEPA,[7] the single European payments area, Europe is working to create the conditions to build a truly European card payment market.

The sharp increase in internet payments and growing use of mobile phones led the Commission to launch a public consultation in January 2012 entitled "Towards an integrated European market for card, internet and mobile payments". The feedback statement was published[8] in June 2012 and revealed a wide range of responses and expectations depending on different categories of respondent.

Following this consultation, the Commission is expected to announce new measures as part of the revision of the Payment Services Directive scheduled for July 2013.

In its response to the European Commission's consultation on reforming the PSD, France stressed that "*the security of transactions determines confidence in the payment instruments available. […] From this point of view, a harmonised European framework guaranteeing a high level of security is crucial*".

Aside from the security aspects, changes to the procedures for supervising participants that are not currently regulated and that act as intermediaries between users and payment service providers also need to be considered.

2|3 International monitoring of innovation in payment instruments

Retail payment systems are one of the action areas of the Bank for International Settlements' Committee on Payment and Settlement Systems (CPSS).

The CPSS recently examined innovation in payment instruments and notably the positioning of central banks in this regard, publishing a rapport on the topic in May 2012.[9] The report stresses the importance that central banks place on promoting the use of effective and safe payment instruments

5 "Role of the Eurosystem in the field of payment systems oversight", June 2000.
6 "Oversight framework for card payment schemes – standards", January 2008.
7 Single Euro Payments Area, which seeks to create a single range of payment instruments in euros (credit transfers, direct debits and cards) for all European countries.
8 *http://ec.europa.eu/internal_market/payments/docs/cim/gp_feedback_statement_en.pdf*.
9 *http://www.bis.org/publ/cpss102.htm*.

while at the same time supporting innovation. It also draws up an inventory of the barriers and general issues linked to innovation in payments, including the role of standardisation, the influence of user behaviour on payment instruments, which may vary from country to country, and the role of the regulator.

In terms of security, the CPSS report underlines the importance of maintaining user confidence in payment services. Technology must enhance the effectiveness of payment instruments, improving the fluidity of payments without introducing breaches in the process, particularly in terms of consenting to a payment transaction. Accordingly, the report acknowledges the value of EMV technology, which enables authentication of the card and the terminal.

As regards CNP transactions, the report identifies several points to monitor:

- the security conditions under which the merchant and/or its payment service provider keeps card data;

- the introduction of strong authentication mechanisms to effectively prevent fraud. In this respect, the CPSS notes the effectiveness of mechanisms based on at least two authentication factors.

3| Conclusion

The regulatory framework applicable to card payments has undergone substantial changes since 2008 aimed at building a harmonised market for cashless payments in Europe. These necessary modifications should be considered in the light of the innovative nature of payment cards, which creates the need to continually revise the applicable regulatory and supervisory framework to control risks, maintain a high level of security and thus preserve user confidence.

Responding to major changes in purchase and payment habits, the European Commission launched a consultation in 2012 to gather feedback from stakeholders on barriers to market integration and how these could be lifted to create more efficient, modern and safer means of payment in Europe. These discussions are likely to lead to changes in Europe's legal framework for payments.

Security questions are of primordial importance in this regard. Regulators and overseers, whether at domestic level or in collaboration within Europe, have been looking at these issues in recent years, publishing recommendations and good practices for payment chain participants. The harmonised implementation of these recommendations is a central concern for authorities and market participants, and could therefore be addressed as part of the changes to the European legal framework.

International work in this area is being taken forward by the Bank for International Settlements. A report by CPSS also looked in 2012 at innovative payments (including card payments) and their security.

Appendixes

Security tips for cardholders

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

Be responsible

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

Be aware

When paying a merchant

- Watch how the merchant uses your card. Do not let your card out of your sight.
- Make sure to check the amount displayed on the terminal before validating the transaction.

When withdrawing cash from ATMs

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

When making internet payments

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

When travelling to other countries

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

A2

Know what to do

If your card is lost or stolen

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

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

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

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

Except in the event of gross negligence on your part (e.g. you let someone see your card number and/or PIN and this person has used your card without telling you) or if you deliberately fail to comply with your contractual security obligations (e.g. you have been careless enough to tell someone the card number and/or the PIN and this person has used your card without telling you), you must submit a claim to the institution that issued the card as soon as possible and within a time limit set by law, namely 13 months from the debit date of the contested transaction. You will not be liable. The disputed amounts must be immediately refunded at no charge. Note that if the card was misappropriated in a non-European country, the time limit for submitting a claim is 70 days from the debit date of the contested transaction. Your card issuer may extend this limit, but it cannot be more than 120 days.

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

Protection for cardholders in the event of unauthorised payments

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

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

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

Domestic and intra-Community transactions

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

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

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

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

A4

Before submitting notification to block the card

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

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

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

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

After submitting notification to block the card

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

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

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

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

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

Transactions outside Europe

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

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

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

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

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

Missions and organisational structure of the Observatory

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

Scope

In its wording prior to 1 November 2009,[1] Article L. 132-1 of the *Monetary and Financial Code* defined a payment card as any card issued by a credit institution that enables its holder to withdraw or transfer funds. Because Order 2009-866 of 15 July 2009 on the conditions governing the supply of payment services and creating payment institutions maintained the scope of the Observatory's responsibilities, it was decided to keep the old definition and extend it to payment service providers, which are, under section I of Article L. 521-1 of the *Monetary and Financial Code*, credit institutions 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* – ACP). These include cards issued by a single undertaking and accepted as a means of payment for goods or services by the undertaking itself or by merchants that have signed a commercial franchise agreement with it,[3] as well as multi-provider cards, which are accepted, for the acquisition of goods or services, only at the premises of the card issuer or within a limited network of persons or for a limited range of goods and services under a commercial agreement with the issuer.[4]

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

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

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

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

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

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

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

3 These cards are exempt from the need for an approval, under point 5° of section I of Article L. 511-7 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*.

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

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

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

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

• electronic purses are cards that store electronic money units. Under 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 and Finance may request the Observatory's opinion on various issues, setting a time limit for its response. These opinions may be published by the Minister.

Composition

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

- a Deputy and a Senator;
- eight general government representatives;
- the Governor of the Banque de France or his/her representative;
- the Secretary General of the *Autorité de contrôle prudentiel* 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 and Finance. 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 to members the information required to monitor the security measures adopted and maintain the technology watch in the field of payment cards. The secretariat also drafts the Observatory's annual report that is submitted to the Minister of the Economy and Finance and transmitted to Parliament.

The Observatory may constitute working or study groups, notably when the Minister of the Economy and Finance requests its opinion. The Observatory defines the mandate and composition of these working groups by absolute majority. The working groups report on their work at each meeting of the Observatory. The groups may hear all persons that are liable to provide them with information that is useful to their mandates. The Observatory has set up standing working groups: the first is responsible for harmonising and establishing fraud statistics and the second for ensuring a payment card technology watch. In 2010, the Observatory decided to set up a third working group to look at the question of 3D-Secure deployment.

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

Members of the Observatory

Pursuant to Article R. 142-22 of the *Monetary and Financial Code*, the members of the Observatory, other than the members of Parliament, those representing the State, the Governor of the Banque de France and the Secretary General of the Prudential Supervisory Authority (*Autorité de contrôle prudentiel*) are appointed for a three-year term by order of the Minister of the Economy and Finance. The most recent appointment orders were issued on 29 October 2012 and 8 March 2013.

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Philippe GOUJON
Deputy
Michèle ANDRÉ
Senator

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

Emmanuel CARRERE
Philippe RICHARD
General Secretariat

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

- The Director General of the National Agency for the Security of Information Systems or his/her representative:
  Patrick PAILLOUX
  Pascal CHOUR
  Loïc DUFLOT

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

- The Senior Official for Defence and Security or his/her representative:
  Claude MAUDELONDE

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

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

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

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  Charles MOYNOT
  Sixtine DU CREST
  Régis PIERRE

Nominated on proposition by the Minister of the Interior:

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

Nominated on proposition by the Minister of Defence:

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

Representatives of payment card issuers

Yves BLAVET (until 7 March 2013)
Head of Payment Instruments
Société Générale
replaced by **Jean-Marie DRAGON**
(order of 8 March 2013)
Marketing Director– Everyday Money Management
La Banque Postale
Jean-Marc BORNET
Director
Groupement des Cartes Bancaires
Jean-François DUMAS
Vice-President
American Express France
Willy DUBOST
Director, Systems and Payment Instruments
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 (until 7 March 2013)
replaced by **Régis FOLBAUM**
(order of 8 March 2013)
Chairman and CEO
MasterCard France
Narinda YOU
Director
Interbank Strategy and Coordination
Crédit Agricole SA

Representatives of the Consumer Board of the National Consumers' Council

Régis CREPY
Confédération nationale – Associations familiales catholiques (CNAFC)
Valérie GERVAIS
General Secretary
Association FO Consommateurs (AFOC)
Patrick MERCIER
President
Association de défense d'éducation et d'information du consommateur (ADEIC)
Sabine ROSSIGNOL
Association Léo Lagrange pour la défense des consommateurs (ALLDC)
Frédéric POLACSEK
Conseil national des associations familiales laïques (CNAFAL)

Representatives of merchants' professional organisations

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

Persons chosen for their expertise

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

Statistics

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

- the 130 members of the "CB" Bank Card Consortium, through the consortium, MasterCard and Visa Europe France;
- 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 2012: 85.8 million
- 67.3 million four-party cards ("CB", MasterCard and Moneo);
- 18.4 million three-party cards.

Number of cards reported lost or stolen[1] in 2012: around 767,000

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 2012 – 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	7,354.49	325.41	127.23	8.10	31.55	3.23
Card-not-present payments excl. internet payments	100.78	8.56	20.15	1.22	3.11	0.34
Card-not-present internet payments	481.75	36.60	96.78	4.45	9.85	0.73
Withdrawals	1,510.21	116.89	27.00	2.99	18.50	2.73
Total	**9,447.23**	**487.47**	**271.15**	**16.76**	**63.00**	**7.03**
Three-party cards						
Face-to-face and UPT payments	127.20	13.53	5.17	0.82	6.64	1.12
Card-not-present payments excl. internet payments	2.13	0.15	na	na	na	na
Card-not-present internet payments	8.02	1.11	3.39	0.25	0.51	0.08
Withdrawals	3.68	0.33	na	na	na	na
Total	**141.04**	**15.12**	**8.56**	**1.07**	**7.15**	**1.20**
Grand total	**9,588.27**	**502.59**	**279.72**	**17.83**	**70.15**	**8.23**

Source: Observatory for Payment Card Security.

Table 2

The payment card market in France in 2012 – 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	7,354.49	325.41	160.93	11.34	43.75	5.73
Card-not-present payments excl. internet payments	100.78	8.56	6.79	1.74	3.00	1.19
Card-not-present internet payments	481.75	36.60	21.53	2.66	4.27	0.70
Withdrawals	1,510.21	116.89	23.65	3.89	7.28	1.61
Total	**9,447.23**	**487.47**	**212.91**	**19.63**	**58.30**	**9.23**
Three-party cards						
Face-to-face and UPT payments	127.20	13.53	4.55	0.95	5.05	1.86
Card-not-present payments excl. internet payments	2.13	0.15	na	na	na	na
Card-not-present internet payments	8.02	1.11	0.44	0.07	0.42	0.09
Withdrawals	3.68	0.33	na	na	na	na
Total	**141.04**	**15.12**	**4.99**	**1.03**	**5.47**	**1.95**
Grand total	**9,588.27**	**502.59**	**217.90**	**20.66**	**63.77**	**11.18**

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 2012 – 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	630.1	48,147.4	105.6	10,889.7	96.1	18,769.8
Lost or stolen cards	542.6	43,484.5	42.5	4,245.0	18.4	4,263.8
Intercepted cards	12.9	465.2	0.5	19.5	0.1	11.5
Forged or counterfeit cards	64.4	3,686.2	14.5	2,108.3	56.0	10,758.1
Misappropriated numbers	5.3	455.6	46.2	4,200.0	19.6	3,300.5
Other	4.9	55.9	2.0	317.0	1.9	435.9
Card-not-present payments excl. internet payments	422.5	29,248.2	79.9	6,496.4	27.0	3,957.9
Lost or stolen cards	0.0	2.3	8.6	802.4	4.4	711.2
Intercepted cards	0.0	0.0	0.1	3.4	0.1	2.8
Forged or counterfeit cards	0.2	7.5	13.9	1,215.1	5.2	796.1
Misappropriated numbers	422.3	29,237.8	56.8	4,418.9	16.9	2,412.4
Other	0.0	0.5	0.4	56.7	0.5	35.4
Card-not-present internet payments	824.1	107,368.2	498.7	36,139.8	113.2	13,459.3
Lost or stolen cards	1.2	156.5	60.8	4,511.1	13.4	1,785.0
Intercepted cards	0.0	0.0	0.3	13.5	0.0	2.2
Forged or counterfeit cards	0.3	48.3	93.3	7,390.5	28.1	3,287.3
Misappropriated numbers	822.6	107,146.3	342.6	24,054.0	71.0	8,312.3
Other	0.1	17.2	1.7	170.7	0.7	72.5
Withdrawals	132.0	36,223.3	5.5	1,083.1	148.8	24,651.4
Lost or stolen cards	122.8	34,500.8	3.8	806.5	5.9	1,003.1
Intercepted cards	0.6	143.2	0.0	0.3	0.0	3.4
Forged or counterfeit cards	8.6	1,577.3	1.4	220.2	135.5	22,464.7
Misappropriated numbers	0.0	2.0	0.1	9.7	1.3	214.1
Other	0.0	0.0	0.2	46.3	6.1	966.2
Total	**2,008.7**	**220,987.2**	**689.7**	**54,609.0**	**385.1**	**60,838.5**

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 2012 – 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	630.1	48,147.4	138.3	24,435.7	321.4	72,298.2
Lost or stolen cards	542.6	43,484.5	33.6	2,058.1	39.3	10,757.1
Intercepted cards	12.9	465.2	2.3	449.5	0.5	135.2
Forged or counterfeit cards	64.4	3,686.2	12.6	2,166.3	95.6	22,700.3
Misappropriated numbers	5.3	455.6	87.5	19,187.9	184.0	38,164.7
Other	4.9	55.9	2.2	574.0	2.1	540.8
Card-not-present payments excl. internet payments	422.5	29,248.2	na	na	na	na
Lost or stolen cards	0.0	2.3	na	na	na	na
Intercepted cards	0.0	0.0	na	na	na	na
Forged or counterfeit cards	0.2	7.5	na	na	na	na
Misappropriated numbers	422.3	29,237.8	na	na	na	na
Other	0.0	0.5	na	na	na	na
Card-not-present internet payments	824.1	107,368.2	na	na	na	na
Lost or stolen cards	1.2	156.5	na	na	na	na
Intercepted cards	0.0	0.0	na	na	na	na
Forged or counterfeit cards	0.3	48.3	na	na	na	na
Misappropriated numbers	822.6	107,146.3	na	na	na	na
Other	0.1	17.2	na	na	na	na
Withdrawals	132.0	36,223.3	2.6	673.5	1.8	552.6
Lost or stolen cards	122.8	34,500.8	2.2	543.4	1.0	324.3
Intercepted cards	0.6	143.2	0.0	19.7	0.0	1.1
Forged or counterfeit cards	8.6	1,577.3	0.3	92.2	0.7	210.3
Misappropriated numbers	0.0	2.0	0.1	13.1	0.1	13.8
Other	0.0	0.0	0.0	5.2	0.0	3.1
Total	**2,008.7**	**220,987.2**	**140.9**	**25,109.2**	**323.2**	**72,850.8**

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 2012 – 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	5.87	3,043.36	2.41	821.13	4.32	1,034.25
Lost or stolen cards	1.20	458.92	0.15	44.33	0.24	87.35
Intercepted cards	0.77	367.34	0.40	152.39	0.12	11.20
Forged or counterfeit cards	2.00	438.57	0.81	262.12	3.29	684.95
Misappropriated numbers	0.30	221.42	1.02	358.35	0.66	249.52
Other	1.60	1,557.11	0.03	3.96	0.00	1.24
Card-not-present payments excl. internet payments	0.15	156.47	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.02	6.03	na	na	na	na
Other	0.13	150.44	na	na	na	na
Card-not-present internet payments	6.1	2,009.70	4.18	918.97	2.88	591.64
Lost or stolen cards	0.66	166.65	0.06	4.37	0.18	29.91
Intercepted cards	0.27	124.95	0.02	19.40	0.00	2.12
Forged or counterfeit cards	0.60	195.70	0.18	8.19	1.03	130.90
Misappropriated numbers	4.35	1,400.69	3.91	886.41	1.66	428.70
Other	0.23	121.71	0.01	0.60	0.00	0.00
Withdrawals	1.31	214.32	na	na	na	na
Lost or stolen cards	1.11	167.15	na	na	na	na
Intercepted cards	0.17	39.78	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.02	4.89	na	na	na	na
Other	0.09	2.50	na	na	na	na
Total	**13.45**	**5,423.85**	**6.58**	**1,740.10**	**7.19**	**1,625.88**

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 2012 – 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	5.87	3,043.36	0.79	423.43	3.70	2,081.05
Lost or stolen cards	1.20	458.92	0.04	14.98	0.30	173.32
Intercepted cards	0.77	367.34	0.02	1.68	0.01	0.32
Forged or counterfeit cards	2.00	438.57	0.59	342.02	2.97	1,643.78
Misappropriated numbers	0.30	221.42	0.10	53.93	0.35	228.65
Other	1.60	1,557.11	0.03	10.82	0.08	34.98
Card-not-present payments excl. internet payments	0.15	156.47	na	na	na	na
Lost or stolen cards	0.00	0.00	na	na	na	na
Intercepted cards	0.00	0.00	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.02	6.03	na	na	na	na
Other	0.13	150.44	na	na	na	na
Card-not-present internet payments	6.1	2,009.70	4.83	1,718.51	10.85	3,283.87
Lost or stolen cards	0.66	166.65	0.05	24.96	0.58	162.73
Intercepted cards	0.27	124.95	0.08	52.80	0.06	13.48
Forged or counterfeit cards	0.60	195.70	0.72	428.87	3.32	1,194.52
Misappropriated numbers	4.35	1,400.69	3.89	1,185.44	6.74	1,849.30
Other	0.23	121.71	0.09	26.44	0.14	63.84
Withdrawals	1.31	214.32	na	na	na	na
Lost or stolen cards	1.11	167.15	na	na	na	na
Intercepted cards	0.17	39.78	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Misappropriated numbers	0.02	4.89	na	na	na	na
Other	0.09	2.50	na	na	na	na
Total	**13.45**	**5,423.85**	**5.61**	**2,141.94**	**14.54**	**5,364.92**

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 in the following categories.

Origin of fraud:

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

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

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

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

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

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

Fraud techniques:

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

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

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

3 Personal Account Number.

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

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

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

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

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

Types of payment:

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

Distribution of losses between:

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

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

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

Merchant sector of activity for CNP payments:

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

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

Managing Editor
Denis Beau,
Director General Operations
Banque de France

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

Editorial Secretariat
Marcia Toma

Production
Banque de France
Press and Communication Directorate

Technical production
Angélique Brunelle

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

Registration of copyright
On publication
October 2013
ISSN 1768-2991

Website
www.observatoire-cartes.fr

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

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

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