2009 ANNUAL REPORT OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

2009 ANNUAL REPORT

OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

Observatoire
de la sécurité
des cartes de paiement

31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01
Internal Postcode: 11-2324

2009
Annual Report of the Observatory for Payment Card Security

addressed to

The Minister of the Economy, Industry and Employment,
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

FOREWORD

The Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement – hereinafter the Observatory*) was created by virtue of the Everyday Security Act 2001-1062 of 15 November 2001[1]. 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)[2].

Pursuant to the sixth indent of Article L. 141-4 of the French Monetary and Financial Code, 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. Part 1 consists of a study on PCI security measures and their suitability for the French market. Part 2 details the 2009 fraud statistics. Part 3 is a summary of the Observatory's technology watch activities, while Part 4 contains a study on how cardholders perceive card security.

[1] The legal provisions relating to the Observatory are set out in Article L. 141-4 of the French Monetary and Financial Code.

[2] For the purpose 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 credit institutions. Three-party cards are issued and acquired by a small number of credit institutions.

1 | ARE PCI SECURITY MEASURES SUITED TO THE FRENCH MARKET?

As part of its task of monitoring the security policies implemented by issuers and acquirers, the Observatory conducted an assessment in 2010 to see whether the PCI (for "payment card industry") security measures shared by international card networks, which set out provisions for securely storing and using card data[3], are suited to the French market and thus identify any potential obstacles to applying the requirements in France. Key goals of the assessment included considering whether, in the case of transactions carried out in France, PCI measures appropriately address the protection needs of sensitive card data and whether the control obligations placed on participants are commensurate with risk exposure.

PCI measures apply to all participants in the acceptance and acquisition chain, i.e. merchants, acquiring banks and their service providers.

The Observatory conducted its study based on information gathered from representatives of issuing institutions, merchants, card schemes and the technical service providers involved in personalisation or device management[4].

1|1 About PCI measures

The Payment Card Industry Security Standards Council (PCI SSC) set up by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International is the body that sets PCI measures. These apply globally to all participants in the acceptance and acquisition chain (acquiring banks, merchants, service providers operating payment platforms, etc.) that participate in PCI member card payment schemes. They apply to cross-border transactions, as well as to domestic transactions in the case of cards that are co-badged with a national scheme[5]. Given their scope of application, these measures act very much as standards.

PCI measures are designed to prevent card data from being misappropriated and used for fraudulent purposes.

PCI SSC has established several sets of measures. This study will focus on the PCI Data Security Standard (PCI DSS) measures, which are intended to protect data transmitted through or stored in the information systems of the card payment acquisition chain (see Box 1)[6]:

[3] Number, expiry date, CVx2, PIN.

[4] BPCE, Société Générale, La Banque Postale, S2P, Visa Europe France (formerly SAS Carte Bleue), MasterCard, American Express, Concert International, Lafon, Atos Worldline, Lyra Network, and, grouped together, the member companies of Mercatel, FCD, Fevad, Fédération des Enseignes du Commerce Associé, UCA, FPS and the member federations of Conseil du Commerce de France (48 companies contributed to the response).

[5] Notably the case of cards issued in France by members of the "CB" Bank Card Consortium.

[6] PCI SSC has also set protection standards for UPTs (PCI UPT), terminals (PCI PED), and applications (PCI PA DSS).

Box 1 – PCI DSS measures

PCI DSS comprises 12 types of measures, divided into six areas:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

An attestation of compliance is issued once implementation of these measures has been verified. To assess compliance, specialised PCI SSC-accredited organisations conduct audits of merchants and service providers, using different methods that reflect transaction volumes. The procedures used to carry out these audits and the resulting attestation are specific to each card payment scheme. As an illustration, the procedures at MasterCard Worldwide are organised into four levels to reflect participant size:

- level 1: participants processing more than six million card transactions a year (irrespective of acceptance channel) or that have already suffered a data compromise must carry out an annual onsite security audit of their information systems and quarterly vulnerability scans of their telecommunications networks;
- level 2: participants processing between one and six million card transactions a year are required to answer the annual self-assessment questionnaire and conduct quarterly network vulnerability scans;
- level 3: participants processing more than 20,000 e-commerce card transactions and fewer than one million card transactions a year in total are also required to answer the annual self-assessment questionnaire and conduct quarterly network vulnerability scans;
- level 4: it is recommended that other participants answer the annual self-assessment questionnaire prepared by PCI SSC and conduct a quarterly evaluation of information system and telecommunications network vulnerabilities.

1|2 Suitability of PCI measures for the French market

PCI SSC governance

Parties involved in governance

The make-up of PCI SSC governing bodies, which include the five founding members, has not changed since the organisation was created in 2006. While this facilitates decision-making, notably during the regular phases of revision, some organisations surveyed by the Observatory stressed that this situation leaves participants subject to PCI measures unrepresented. These organisations believe that changes are needed to PCI SSC governance. The European Payments Council (EPC), the coordinating body for Europe's banking industry in the implementation of the Single Euro Payments Area (SEPA) project, is studying the possibility of being represented within PCI SSC. More generally, emphasis was placed on the need for the current governance arrangements to be closer to the interests that they are supposed to protect, on both a sector and regional level.

Implementation of measures

Each of the networks that belongs to PCI SSC has established its own procedures for applying PCI measures. In particular, compliance deadlines and the procedures for calculating thresholds in the certification process vary from one payment scheme to another. Most of the respondents in the Observatory's survey, which accept or process cards from different schemes, underline the need to harmonise interpretations of PCI measures in order to enhance operational efficiency and cost control.

In addition, PCI measures apply to a technological environment that is by nature evolving. As a result, PCI SSC regularly revises the measures to reflect the latest security developments. While survey respondents do not contest the need to upgrade the measures, they think that sometimes they are updated too frequently, potentially creating problems when it comes to introducing corrective measures.

Applying the measures to the French card payment environment

Scope of PCI measures

PCI DSS measures are designed to protect the entire acceptance and acquisition process. As such, they provide broad coverage of data contained on cards, i.e. both embossed data and data stored on stripes or chips. The aim is to combat all forms of compromise by taking account of the various ways that different payment channels use card data.

Merchant representatives, though, have concerns about the relevance of measures to protect stripe data on the French market. They point out that the vast majority of transactions conducted in France use the chips contained in payment cards, which thus enjoy high levels of cryptographic protection. However, it is important to protect associated data (card number and expiry date) as well as data embossed or printed on the card (same as above plus CVx2) to ensure that they are not used fraudulently, particularly in e-commerce transactions.

The same respondents observe that desensitising card data to the risk of compromise would obviate the need to comply with PCI measures, which are designed to protect information embossed on the card, recorded on the stripe or stored in the chip. While noting that merchants take steps to ensure properly secured systems, there is also the more general question of how appropriate it is for merchants to manage these sensitive data.

Overlap of PCI measures with other safety standards

Some survey respondents point out that PCI DSS measures are similar to international security standards, such as ISO 27000 standards[7], or measures that are applicable in France, such as recommendations issued by CNIL, France's National Data Protection Authority (see Box 2), and might therefore be viewed as replicating the arrangements put in place by the participants that apply them. Other respondents, however, upheld the opposite view, stressing that implementing ISO 27000 standards or CNIL recommendations helped to ensure compliance with PCI measures.

In general, similar remarks were made about the overlap between PCI DSS/PCI PED measures and EMV standard security principles, and between PCI Unattended Payment Terminal (PCI UPT) measures, which set out arrangements for the physical and logical protection of UPT electronic components, and AFAS measures[8], which are designed to prevent the misappropriation of card data from automated teller machines (ATMs) and automated fuel pumps. However, PCI measures have a wider scope than these other standards and the overall combination offers a way to cover the different channels of data compromise identified by a risk analysis.

Box 2 – CNIL recommendations

In light of the risks linked to the circulation of bank card numbers in card-not-present sales, the French National Data Protection Authority (CNIL) adopted a recommendation[9] in 2003 that applied the broad principles of Data Protection Act 78-17 of 6 January 1978 to this area. The CNIL particularly emphasised security aspects relating to the collection and processing of bank card numbers.

In accordance with its recommendation, the CNIL considers that no decision entailing an assessment of human behaviour should be solely based on automated processing of private data. In principle, the length of time for which a card number may be kept should not exceed the length of time needed to carry out the transaction for which it was collected. If a number is kept for other reasons, the explicit agreement of the person must be given. The CNIL has already issued warnings to several hotels[10] for keeping such information without first obtaining agreement. People must also be informed that data are being processed, in accordance with the provisions of Article 32 of the Data Protection Act.

With the rise of online purchasing, professionals are using new techniques to process private data, notably to prevent fraud, including tools for detecting unusual behaviour by cardholders and additional cardholder authentication techniques. Some of these arrangements could deprive cardholders of a right or bar them from entering into a contract by preventing them, even temporarily, from using their payment card, even though there are no legal or regulatory provisions to this effect. Under Article 25.I.4° of the Data Protection Act, such systems must therefore be submitted for prior authorisation from the CNIL. When reviewing these kinds of cases, the CNIL pays particular attention to cardholder information arrangements and the consequences associated with implementing these processing arrangements.

[7] Series of information security standards that define the framework for implementing a security management system, a catalogue of security measures and a risk management process.

[8] "Anti Fishing Anti Skimming", a set of measures required by the "CB" Bank Card Consortium in 2005 to protect UPTs and ATMs.

[9] (In French) http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/13/

[10] (In French) http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article//du-bon-usage-des-donnees-bancaires-collectees-par-les-hotels/#

Certification

Certification process

PCI SSC-accredited Qualified Security Assessors (QSAs) certify compliance with PCI measures. The founding members publish the list of QSAs. Card payment schemes may also require quarterly vulnerability scans, performed by Approved Scanning Vendors (ASVs), depending on the number of transactions processed annually. Acquiring institutions, meanwhile, are subject to PCI standards without being formally certified compliant by PCI SSC.

To ensure a transparent process, each of the card payment schemes publishes the list of QSAs/ASVs as well as certification audit results. Participants subject to PCI measures thus have a real-time base of information that allows them to check the quality of their equipment and the compliance of service providers to which they outsource acquisition processes.

Publications of this kind, i.e. additions to and removals from the abovementioned lists, carry an inherent risk for participants of dependence on card payment systems, which have sole responsibility for compiling and managing the lists. Changes to the lists can have damaging consequences for affected participants, especially since they operate in a highly competitive market.

Most participants queried by the Observatory point out that implementing PCI measures is a cumbersome and complex process, and that they therefore have to call in consulting firms. They emphasise the conflict of interest that may result from the fact that these companies are also typically accredited by PCI SSC to carry out compliance audits. Aside from the fact that, by virtue of their two assignments, these companies have influence over the implementation of these measures, during their work they may also gain a complete view of the security arrangements used in the participant's information system. Some respondents therefore said that companies' internal audit departments could potentially be more involved in the certification process.

Enforcement mechanisms

Non-compliance may give rise to various penalties, including:

- responsibility for any costs arising from non-compliance (fraudulent transactions, card reissuance, etc.);
- fines for acquiring banks, determined and levied independently by each PCI SSC member network, based on the number of days of non-compliance or the number of transactions performed;
- suspension of the merchant's account.

These mechanisms are based on the contractual relationship governing acceptance of a network's cards and illustrate the disciplinary aspect of PCI measures. Survey respondents do not challenge the mechanisms, but some of them commented on the large sums sometimes due to PCI SSC member networks, which may be combined with the amount of fraudulent transactions carried out over the period.

1|3 Conclusion

The feedback to the Observatory's survey underscores the need to implement measures to protect card data across the entire acceptance and acquisition process. PCI measures are a good practice in this respect and help to raise the level of security for processes and devices. The fact that these measures have been adopted by international card payment schemes, including for national cards with which co-badging agreements have been signed, makes them de facto standards.

However, there are concerns about the suitability of these measures for the French market. Some of the firms surveyed feel that PCI SSC does not do enough to take account of the special features associated with using smart cards. Conversely, others emphasise that card data can be managed in a variety of environments throughout the acceptance and acquisition process, and that there is a major risk that these data could be put to fraudulent use. Recommendations adopted by the CNIL in this area, as well as research done by the Observatory since its inception, confirm the importance of protection. The option of desensitising card data was also mentioned in this context, with merchant representatives querying the appropriateness of managing sensitive data in their environments.

Respondents felt that it was crucial to have French or European participants represented in PCI SSC to ensure that PCI measures are properly adapted to local requirements. PCI SSC governance should ideally be broadened, and the European Payments Council (EPC), which works on the interoperability of card payments in Europe, should have a seat on the PCI SSC. With this in mind, bank and merchant representatives called for the creation of a European Fraud Observatory similar to the one set up in France by the Observatory for Payment Card Security. A body of this kind would make it possible to address the needs of payment industry participants by providing guidance tailored to the European market.

In addition, the specific arrangements used by PCI SSC member card payment schemes to apply PCI measures or implement compliance assessment mechanisms are likely to make implementation more cumbersome for participants. Better coordination between card payment schemes should make it possible to address this issue.

Survey respondents also pointed out that compliance audit and enforcement procedures imposed on acceptance and acquisition participants were in some cases unnecessarily cumbersome and excessively expensive. Similarly, it is important to avoid the creation of conflicts of interest or positions of influence that accredited companies could use in connection with auditing the compliance of participants. Tangible improvements are needed on these points.

2 | FRAUD STATISTICS FOR 2009

The Observatory for Payment Card Security 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 Annex E to this report. A summary of the 2009 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, international, face-to-face and card-not-present transactions, as well as payment and withdrawal transactions, and fraud trends involving lost or stolen cards, intercepted cards, forged or counterfeit cards, and appropriated card numbers. In addition, Annex D to this report presents a series of detailed fraud indicators.

Box 3 – 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. It supplements these data with statistics compiled by France's e-commerce and distance selling federation (Fevad) from a sample of 33 companies that account for 26% of revenues in distance selling to retail customers.

The statistics calculated by the Observatory thus cover:

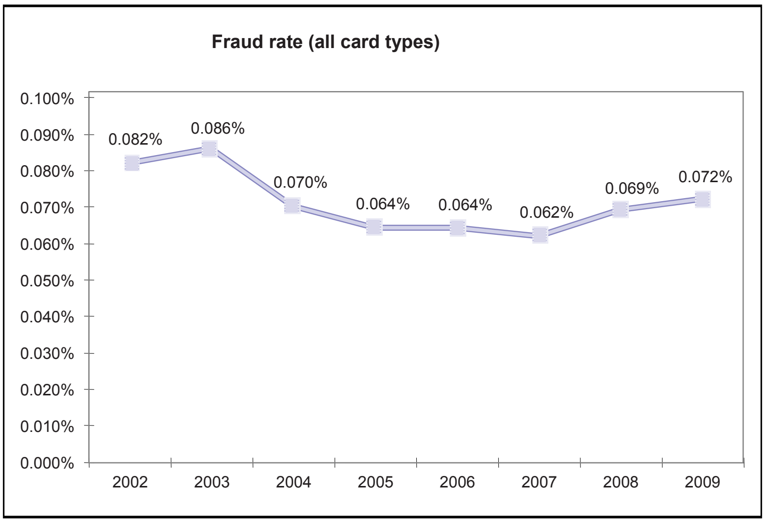
- EUR 429.4 billion in transactions in France and in other countries made with 62.4 million four-party cards issued in France (including 1.54 million electronic purses);
- EUR 24.2 billion in transactions primarily in France with 28.2 million three-party cards issued in France;
- EUR 23.7 billion in transactions in France with foreign three-party and four-party cards.

Data were gathered from:

- Ten three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco;
- The 136 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.

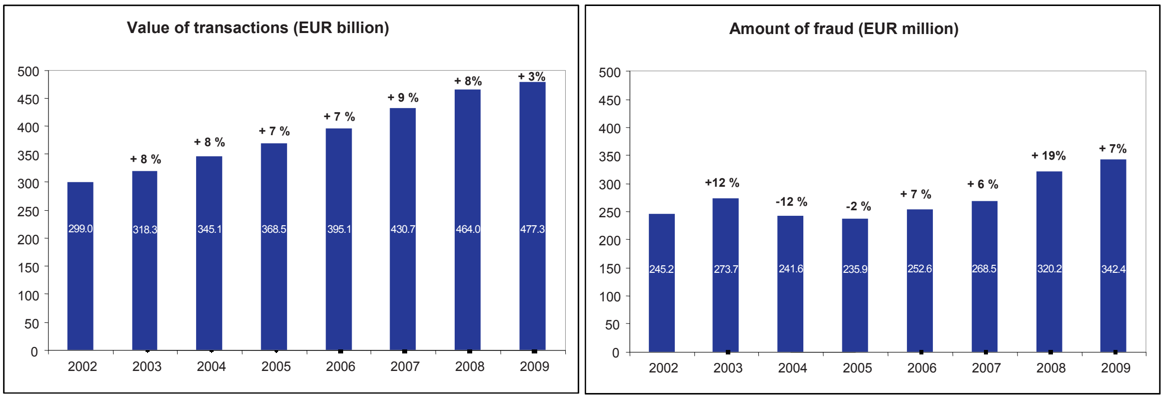
2|1 Overview

The overall fraud rate for card payments and withdrawals recorded by French schemes in 2009 stood at 0.072%, an increase on previous years (0.069% in 2008 and 0.062% in 2007 – see Table 1). This was because the increase in the amount of fraud (6.9%, from EUR 320.2 million in 2008 to EUR 342.4 million in 2009) exceeded growth in the value of transactions, which climbed 2.9% from EUR 464.0 billion in 2008 to EUR 477.3 billion in 2009 - see Table 2. The average amount of a fraudulent transaction was up slightly, from EUR 131 in 2008 to EUR 136.



Source: Observatory for payment card security

▲ Table 1 – **Fraud rate, all card types**



Source: Observatory for Payment Card Security

▲ Table 2 – **Value of transactions and amount of fraud**

The rate of issuer fraud, which covers all fraudulent payments and withdrawals made in France and in other countries with cards issued in France, increased to 0.059% in 2009, up from 0.057% in 2008. Issuer fraud thus totalled EUR 265.6 million, compared with EUR 249.2 million in 2008.

The rate of acquirer fraud, which covers all fraudulent payments and withdrawals made in France with all French and foreign cards, rose slightly to 0.048%, corresponding to fraud of EUR 220.8 million, from 0.045% in 2008 (EUR 201.9 million).

Annex D to this report contains detailed tables on the volume and value of transactions and fraud by card type, geographical area, transaction type and fraud type.

2|2 Breakdown of fraud by card type

Fraud rate
(Fraud amount, EUR million)

	2005	2006	2007	2008	2009
Four-party cards	0.064% (218.8)	0.065% (237.0)	0.063% (253.6)	0.070% (304.3)	**0.072%** (324.3)
Three-party cards	0.067% (17.1)	0.052% (15.6)	0.052% (15.0)	0.054% (16.0)	**0.068%** (18.2)
Total	0.064% (235.9)	0.064% (252.6)	0.062% (268.5)	0.069% (320.2)	**0.072%** (342.4)

Source: Observatory for Payment Card Security

▲ Table 3 – **Breakdown of fraud by card type**

The fraud rate for four-party cards was up slightly in 2009, climbing to 0.072%, which corresponds to fraud of EUR 324.3 million, compared with 0.070% (EUR 304.3 million) in 2008. Issuer and acquirer fraud rates for this type of card stood at 0.059% and 0.048% respectively, compared with 0.057% and 0.046% respectively in 2008. The average value of a fraudulent transaction was EUR 132, compared with EUR 127 in 2008.

The fraud rate for three-party cards increased sharply to 0.068% in 2009 (EUR 18.2 million), compared with 0.054% (EUR 16.0 million) in 2008. Issuer and acquirer fraud rates for this type of card were 0.053% and 0.059% respectively, compared with 0.046% and 0.042% respectively in 2008. The average value of a fraudulent transaction was EUR 324 in 2009, compared with EUR 357 in 2008.

2|3 Geographical breakdown of fraud

Fraud rate
(Fraud amount, EUR million)

	2005	2006	2007	2008	2009
Domestic transactions	**0.029%** **(97.8)**	**0.031%** **(109.6)**	**0.029%** **(114.5)**	**0.031%** **(130.9)**	**0.033%** **(144.0)**
International transactions	**0.408%** **(138.1)**	**0.362%** **(143.0)**	**0.368%** **(154.0)**	**0.427%** **(189.4)**	**0.449%** **(198.4)**
o/w French issuer and foreign acquirer	0.458% (64.1)	0.453% (76.4)	0.476% (85.3)	0.594% (118.3)	0.594% (121.6)
o/w foreign issuer and French acquirer	0.373% (74.1)	0.295% (66.5)	0.288% (68.7)	0.291% (71.0)	0.324% (76.8)
Total	**0.064%** **(235.9)**	**0.064%** **(252.6)**	**0.062%** **(268.5)**	**0.069%** **(320.2)**	**0.072%** **(342.4)**

Source: Observatory for Payment Card Security

▲ Table 4 – **Geographical breakdown of fraud**

The geographical breakdown of fraud still shows a discrepancy between domestic and international transactions. The latter account for 58% of fraud, even though they make up barely 9% of the value of card payments handled by the French schemes.

Because domestic transactions grew by 3.2%, the fraud rate for such transactions increased slightly to 0.033% in 2009 from 0.031% in 2008, thus remaining at a very low level.

The rate and amount of fraud involving international transactions both increased in 2009. The fraud rate for foreign transactions using cards issued in France remained high, at 0.594%, corresponding to fraud of EUR 121.6 million, compared with EUR 118.3 million in 2008. The fraud rate for transactions in France using cards issued in other countries rose to 0.324%, corresponding to fraud of EUR 76.8 million, compared with 0.291% (EUR 71.0 million) in 2008.

Box 4 – Breakdown of losses from fraud

Since 2007, the Observatory has estimated indicators for the distribution of losses from fraud between cardholders, merchants and banks. These overall indicators cover all three-party and four-party schemes. It is important to note that they apply only to the losses themselves, not to the total processing and insurance costs generated by fraud. The indicators show a trend, but remain theoretical and reflect only the direct breakdown of losses between participants, because they are constructed to refer to the legal and regulatory provisions governing the procedures for blocking lost or stolen cards and for disputing fraudulent card payments. In addition, they cannot capture all the commercial practices of issuers and acquirers.

Taking all schemes into account, losses from fraud in domestic transactions were distributed as follows in 2009: 2.3% for cardholders, 41.1% for issuers and acquirers, and 56.5% for merchants, mainly in distance selling. The portion borne by merchants increased further (from 53.5% in 2008) owing to growth in fraud involving card-not-present payments, an area where merchants bear most of the losses (they do not bear fraud-related costs if they use secure systems such as 3D-Secure).

Furthermore, out of the EUR 342.4 million in fraud recorded by the French schemes in 2009, it is estimated that foreign schemes bore EUR 94.5 million, or 28%. This is attributable to the application of international liability-sharing rules as part of implementation of the EMV standard and the 3D-Secure authentication mechanism for card-not-present payments.

2|4 Breakdown of fraud by transaction type

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

Domestic transactions

			Fraud rate (Fraud amount, EUR million)		
Domestic transactions	**2005**	**2006**	**2007**	**2008**	**2009**
Payments	**0.033% (82.8)**	**0.035% (92.3)**	**0.032% (95.6)**	**0.036% (111.7)**	**0.038% (123.2)**
- o/w face-to-face and UPT	0.025% (59.2)	0.024% (59.1)	0.017% (45.4)	0.015% (44.5)	0.014% (41.0)
- o/w card-not-present	0.196% (23.6)	0.199% (33.2)	0.236% (50.1)	0.252% (67.2)	0.263% (82.2)
- o/w by post / phone	na	0.194% (19.8)	0.201% (23.8)	0.280% (28.5)	0.263% (30.3)
- o/w online	na	0.208% (13.4)	0.281% (26.4)	0.235% (38.8)	0.263% (51.9)
Withdrawals	**0.017% (15.0)**	**0.019% (17.4)**	**0.020% (19.0)**	**0.018% (19.1)**	**0.019% (20.8)**
Total	**0.029% (97.8)**	**0.031% (109.6)**	**0.029% (114.5)**	**0.031% (130.9)**	**0.033% (144.0)**

Source: Observatory for Payment Card Security

▲ Table 5 – **Breakdown of domestic payment fraud by transaction type**

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

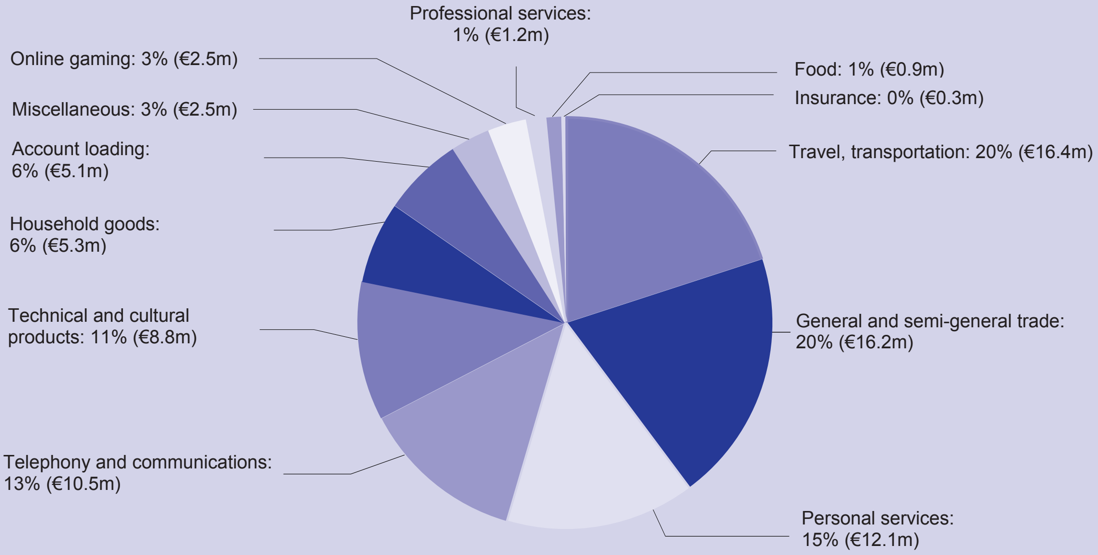
– the fraud rate for face-to-face and UPT payments continued to fall, declining to 0.014%, corresponding to fraud of EUR 41.0 million, compared with 0.015% (EUR 44.5 million) in 2008. Face-to-face and UPT payments accounted for 67% of domestic transactions, but just 28% of fraud in value terms;

– the fraud rate for card-not-present payments rose again, to 0.263% in 2009, corresponding to fraud of EUR 82.2 million, compared with 0.252% (EUR 67.2 million) in 2008. Card-not-present payments thus accounted for 7% of the value of domestic transactions but for 57% of fraud in value terms. While this increase needs to be seen in the context of the substantial growth in the volume and value of card-not-present payments (17.1% between 2008 and 2009 in value terms, including 19.7% growth in online payments), the high level of fraud recorded through this payment channel prompted the Observatory to recommend implementing measures to combat this trend. The Observatory's last report stressed the need for widespread introduction of bearer authentication mechanisms for all payments and for tougher authentication methods. Chapter 4 of this report details the findings of a qualitative study on how cardholders perceive security in online transactions and their responses to a variety of one-time authentication solutions;

– the fraud rate for cash withdrawals was stable at just 0.019%, corresponding to fraud of EUR 20.8 million, after 0.018% (EUR 19.1 million) in 2008. Withdrawals represent 25% of domestic transactions and account for 14% of the total fraud amount.

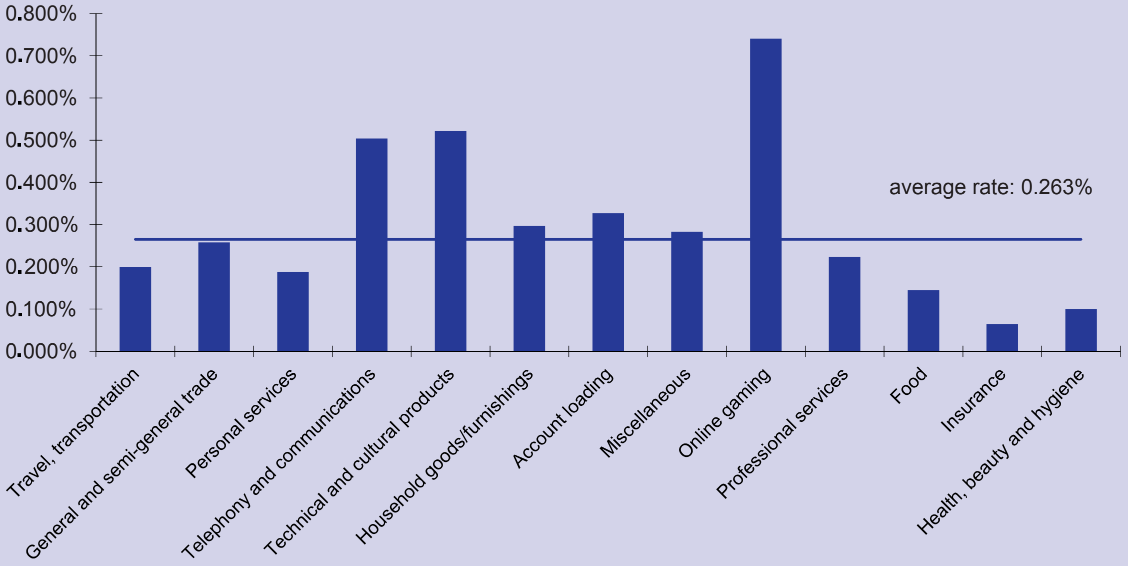
Box 5 – Domestic fraud in distance selling, by sector of activity

The Observatory has gathered data that provide information about the distribution of fraud in card-not-present payments by sector of activity. These data cover domestic transactions only.



Breakdown of fraud in card-not-present payments by sector of activity, domestic transactions (amount in EUR million)

The travel/transportation, general and semi-general trade and personal services sectors were the most exposed to fraud, accounting for 55% of the total. A comparison of average fraud rates for each sector of activity provides additional information, revealing that some sectors, including technical and cultural products and online gaming, have considerable exposure despite accounting for a small portion of the total fraud amount (cf. following chart). However, the Observatory noted that fraud rates varied considerably between merchants within the same sector depending on the security measures in place.



Fraud rate for card-not-present payments by sector of activity, domestic transactions

Source: Observatory for Payment Card Security

International transactions

	Fraud rate (Fraud amount, EUR million)			
French issuer – foreign acquirer	**2006**	**2007**	**2008**	**2009**
Payments	**0.421% (54.0)**	**0.483% (65.2)**	**0.655% (99.3)**	**0.679% (105.2)**
- o/w face-to-face and UPT	0.288% (28.1)	0.299% (30.0)	0.286% (32.0)	0.406% (44.7)
- o/w card-not-present	0.840% (26.0)	1.024% (35.1)	1.698% (67.2)	1.350% (60.5)
- o/w by post / phone	0.684% (5.7)	0.790% (7.6)	1.284% (11.2)	1.016% (9.7)
- o/w online	0.898% (20.3)	1.117% (27.4)	1.815% (56.0)	1.440% (50.8)
Withdrawals	**0.555% (22.4)**	**0.455% (20.0)**	**0.399% (19.1)**	**0.331% (16.5)**
Total	**0.453% (76.4)**	**0.476% (85.3)**	**0.594% (118.3)**	**0.594% (121.6)**
Foreign issuer – French acquirer	**2006**	**2007**	**2008**	**2009**
Payments	**0.344% (61.5)**	**0.334% (62.8)**	**0.339% (65.4)**	**0.397% (74.1)**
Withdrawals	**0.107% (5.0)**	**0.117% (5.9)**	**0.110% (5.6)**	**0.055% (2.8)**
Total	**0.295% (66.5)**	**0.288% (68.7)**	**0.291% (71.0)**	**0.324% (76.8)**

Source: Observatory for Payment Card Security

▲ Table 6 – **Breakdown of international payment fraud by transaction type**

In the case of international transactions, the Observatory has a detailed breakdown of fraud by transaction type only for transactions by French cards in other countries. In this category, fraud in face-to-face and UPT payments increased (to EUR 44.7 million in 2009, compared with EUR 32.0 million in 2008), while fraud in card-not-present payments declined slightly from EUR 67.2 million in 2008 to EUR 60.5 million in 2009. However, the fraud rate for card-not-present payments was high, at 1.350% - well above the rate for face-to-face and UPT payments (0.406%). The introduction of enhanced authentication systems should help to curb fraud in card-not-present payments, which account for just 22% of transactions but 50% of the fraud in this geographical area.

Fraud for withdrawals declined by both amount and rate. This was true for international transactions made using French cards and for transactions made in France with foreign cards.

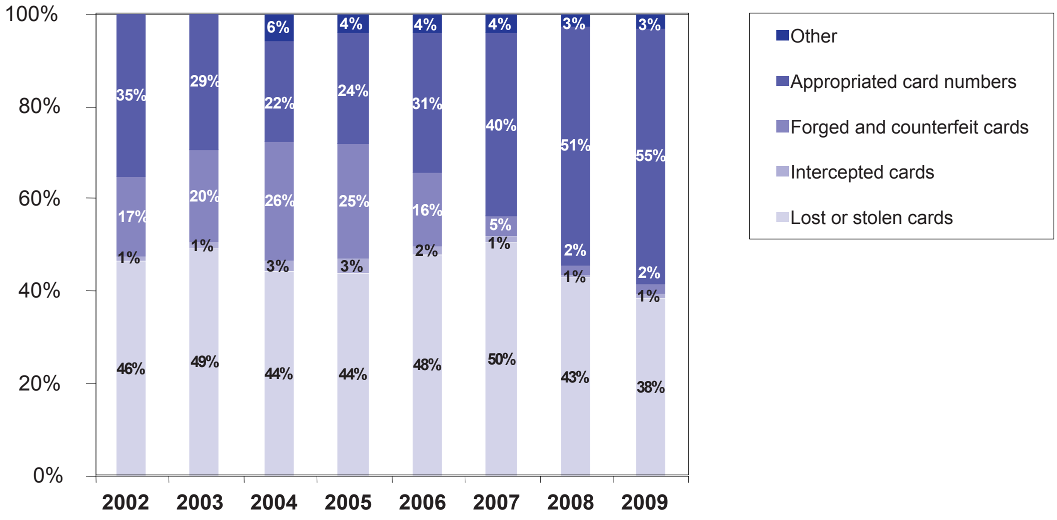
2|5 Breakdown by fraud type

The Observatory breaks down fraud into the following types:

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

- Appropriated card numbers, when a card number is copied without the cardholder's knowledge or created through card generation processes (which use programs to generate random card numbers) and then used for card-not-present transactions;
- "Other" fraud, which covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts with a false identity.

The following chart shows national fraud trends for all payment cards. The breakdown covers payments only.



Source: Observatory for Payment Card Security

▲ Table 7 – **Breakdown by fraud type (domestic transactions, fraud amount)**

Fraud involving the use of appropriated card numbers for fraudulent card-not-present payments has been on the increase since 2005 and is now the most common type of fraud (55.1%, compared with 51.3% in 2008). Fraud involving lost or stolen cards accounted for 38.2% of fraudulent domestic payments. Counterfeit cards accounted for just 2.2% of fraudulent domestic payments. "Other" fraud was stable. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for some 50% of the fraud involving these cards.

	All types of cards		Four-party cards		Three-party cards	
2009	**Amount** (EUR million)	**Share**	**Amount** (EUR million)	**Share**	**Amount** (EUR million)	**Share**
Lost or stolen cards	55.0	38.2%	52.6	39.2%	2.4	25.1%
Intercepted cards	1.7	1.2%	0.8	0.6%	0.9	9.9%
Forged or counterfeit cards	3.2	2.2%	2.2	1.7%	1.0	10.4%
Appropriated numbers	79.4	55.1%	78.8	58.6%	0.6	6.2%
Other	4.6	3.2%	-	-	4.6	48.4%
Total	**144.0**	**100%**	**134.4**	**100%**	**9.6**	**100%**

Source: Observatory for Payment Card Security

▲ Table 8 – **Breakdown of domestic payment fraud by fraud type and by type of card**

Box 6 – Indicators provided by law enforcement agencies

In 2009, law enforcement agencies noted an increase in arrests connected with bank card fraud, reporting 200 arrests, compared with 154 in 2008.

Attacks on automated teller machines (ATMs) were down, with 411 such attacks registered in 2009, compared with 427 in 2008, 391 in 2007, 515 in 2006, 200 in 2005 and 80 in 2004. There was also one attack on a card-operated fuel pump (compared with 3 in 2008), as well as 18 attacks on payment terminals (17 in 2008).

Numerous investigations into these cases were carried out across the country. Police work in this area included the following:

- the arrest of a 13-person ring specialised in capturing card data, counterfeiting and using cards with complicit merchants in France. Losses attributable to the ring are estimated at over EUR 200,000;
- the arrest of a four-person gang specialised in capturing card data from ATMs. Large amounts of card data were compromised on a dozen ATMs, causing total losses in excess of EUR 250,000;
- dismantling a nine-person Franco-Romanian ring specialised in counterfeit cards. Searches resulted in the discovery of a dozen or so such cards, the equipment used and EUR 15,000 in cash.

3 | TECHNOLOGY WATCH

3|1 Monitoring the implementation of contactless payment solutions using cards and mobile phones

In its 2007 report, the Observatory published a study on the security of new methods for initiating card payments[11], which built on an initial analysis published in 2004.

By 2007, payment solutions based on contactless technologies were already widely used in some countries, such as Japan. In France, however, they were still at the pilot project stage. The Observatory therefore issued a number of recommendations dealing with the security of contactless card and mobile phone payments.

The situation has since evolved: contactless cards are now in circulation and mobile phone payments are now the subject of full-scale trials. For this reason, the Observatory decided to conduct work to analyse the current state of play, determine whether issuers and acceptors had followed its 2007 recommendations[12] and assess the appropriateness of its recommendations in the new environment.

Contactless payment solutions: characteristics and security issues

Contactless payment solutions are based on the use of a card or mobile phone. In each case, the device communicates with the payment terminal via an antenna that uses the near field communication (NFC) protocol, which is designed to function at short distances, i.e. a few centimetres. Each device then has specific characteristics of its own.

Contactless cards

With contactless cards, the issuing bank's payment application is embedded in the chip alongside a conventional payment application operating in contact mode. To speed up the payment process, the user does not have to enter a PIN when making contactless payments in the following cases:

- individual transactions below a given threshold, currently around €20-30;
- if combined transactions remain below a given total amount;
- if the number of contactless transactions remains below a pre-determined number.

In all other cases, the card is used in contact mode and the PIN is checked.

Counters managed by the payment application monitor the three types of information mentioned above (individual and combined transaction amounts and number of transactions). To reset the counters, the user must ask for authorisation and enter his/her PIN when making a payment in contact mode.

[11] Cf. 2007 Annual Report, pp. 35-41. The analysis covers contactless card and mobile phone payments.

[12] As with the 2004 and 2007 reports, the study does not deal with prepaid cards, which are examined as part of monitoring work done on issuer and acquirer security policies.

Contactless mobile phone payments

As the current trials stand, two models have emerged as the primary methods for storing the payment application in a secure element[13] on the mobile phone:

- the application can be hosted by the Subscriber Identity Module (SIM) card operated by the phone company[14]. The payment application within the microprocessor then runs the operations needed to initiate payments;
- the application can be put on a secure element that is separate from the SIM card, initiates payment transactions, controls NFC communications and holds digital certificates. This type of architecture makes it possible to develop services independently of the infrastructure operated by telecommunication firms, i.e. without involving SIM cards or associated telephony services.

In both cases, however, the bank that issues the payment application retains control over security for the component on which its application is housed, notably by requiring assessments of host components and payment applications.

As with cards, the payment application manages transaction thresholds that, when reached, require a personal code to be entered on the phone's keypad. This code is not the same as the PIN used to activate the SIM card or any other secure element. The user may choose to require the code to be entered for every payment, no matter how large or small. Counters may be reset remotely when the limits are reached. For this, an authorisation request must be submitted by the phone, and the client must indicate his explicit agreement by entering his personal code either when submitting the request or when making the next transaction.

* * * *

The Observatory's 2007 report identified four types of threats[15] connected with contactless payment solutions. Current developments linked to the gradual deployment of contactless payments increase the need to take account of these threats, which may be combined in some cases.

Capture of exchanged data

Because the payment terminal and the card or mobile phone communicate using radio frequencies, there is a danger that the exchanged information – relating to the card number (PAN)[16], the amount of the transaction and authentication data for the card or secure element – could be captured during payment and then used for fraudulent purposes.

Two systems can prevent captured data from being reused. First, to secure the connection between the contactless device and the terminal, the payment application on the card or phone can be dynamically authenticated whenever a transaction is made. Second, to prevent the PAN from being reused with other acceptance modes if intercepted, a special PAN for contactless

[13] The term "secure element" refers here to the SIM card or any other secure electronic component (SD card, etc.) that can be used to house a payment application.

[14] The Global Platform standard requires SIM cards to have separate security domains so that they can carry different software applications.

[15] Capture of exchanged data, activation of the payment application without the holder's knowledge, theft of the contactless device, attacks against payment applications.

[16] Primary Account Number, which comprises data identifying the issuer and the card number.

payments can be assigned that is different from the PAN when the card is used in contact mode or for card-not-present purchases.

Communication between payment terminals and acquisition and authorisation servers can be protected by reusing the infrastructure already in place for contact payment cards.

Activating the payment application without the holder's knowledge

The use of contactless interfaces makes it possible to enter into dialogue with a card or mobile phone without the holder's consent, potentially with harmful consequences.

Contactless cards

The use of contactless techniques means that transactions can be carried out without the holder's knowledge, particularly if they are below a certain threshold (currently around €20-30) where the PIN is not entered (an attack known as "tele-pickpocketing"). Limiting the distance between the contactless device and the terminal reduces the ability to activate a contactless device using a fraudulent terminal. Even so, by 2007 the Observatory was already recommending introducing processes to activate and deactivate contactless mode, to ensure that holders approve all transactions. Among other things, it recommended protective measures, such as the use of a case to block radio frequencies and prevent access to the payment application outside the short windows when the user takes the card out of the case to make payments.

Contactless mobile phone payments

An activate/deactivate function for the payment application using the phone's built-in keypad is the only way to deliver a level of security equivalent to that described above for contactless cards.

The counter reset process can be made secure by requiring the personal code to be entered to authenticate the holder. Having the bank reset the counters remotely would necessitate a secure channel between the mobile phone and the bank (notably if the information is sent by text message via the phone operator) and strict controls on movements by the bank (checks to verify the validity of resets, limited number of resets for a phone over a set period, etc.).

Theft of the contactless device

Contactless cards and mobile phones are vulnerable to theft insofar as, if the PIN (or personal code) does not have to be entered and the validity of the card (or mobile phone payment application) is not checked online, stolen devices can be used to make small-value purchases.

However, maximum thresholds for contactless payments limit financial losses in the event of fraud. Counters are built into the payment application that calculate the total value of small--value transactions and require the holder to enter the PIN or personal code (if using a mobile phone) to zero the counters.

Furthermore, in the event of theft, the card or phone payment application can be blocked to put a stop to fraudulent use. In the case of mobile phones, the application can be blocked using OTA technology[17], which allows applications to be updated remotely.

Attacks against payment applications

Attacks may be mounted against the payment application, whether it is housed on the card chip or contained in the secure element of a mobile phone. While cards are subject to security certification arrangements, the possibility of attacks against the chips that contain payment applications in mobile phones underlines the need to establish a similar process for chip components, to be conducted by independent third parties, as recommended by the Observatory in 2007.

The resulting level of security should make it possible to guarantee that the payment application and the data that it contains are adequately protected. They should therefore be isolated from the other applications and subject to restricted access (authorised transactions). Security standards, such as those prepared by the Global Platform consortium for SIM cards, can be used to keep applications separate. Furthermore, security assessments conducted within the framework of the national certification scheme[18] ensure a high level of security for these applications and components.

The mobile phone itself can also be exposed to malware (data capture, simulation of payment application for phishing purposes, etc.), which may be spread through Bluetooth, WiFi, GSM and other channels. However, initiatives aimed at securing mobile phone payments consider phones to be "transparent" from a security perspective and seek to protect the payment application and its medium, without relying on the security of the device itself.

Finally, contactless payment applications that use secret information may be compromised during the manufacturing or personalisation of components. For this reason, when it comes to managing secret information, entities operating in the electronic payments industry need to ensure that contactless payments are subject to the same rules as payment cards operating in contact mode.

Contactless payments: a stocktaking

Current initiatives

Contactless payments have been gaining ground in France since 2007, with prototypes leading to pilot projects and even some market launches.

Contactless cards

Société des Paiements Pass (S2P) has led the way in marketing contactless cards. In 2009, it issued 2.5 million Pass cards, which are accepted in Carrefour shops. Moneo, operating through Billettique Monétique Services (BMS), has also been offering electronic purses in the shape of contactless cards since 2006 and has 500,000 cards already in circulation. These cards are accepted by student services organisations, for example.

[17] Over-the-air (OTA) technology is used to remotely access and securely update data held on a SIM card.

[18] ANSSI

Moneo has moreover developed a new mode of contactless payment using a contactless USB key (Smart Object Weneo/Moneo). Trials have been underway in Bordeaux since 2009 and in Toulon since February 2010.

Contactless payment cards by Visa and MasterCard (Pay Wave and PayPass respectively) were launched on a trial basis in Caen and Strasbourg in September 2009. Only 1,000 of these cards have been issued for the time being.

Contactless payments by mobile phone

As of 2010, contactless mobile phone payments are still mainly at the trial rather than marketing stage.

Moneo is testing mobile phone-based electronic purse payment solutions. The *Nice Futur Campus* project is planning to issue 300 mobile phones equipped with NFC technology in 2010. Each phone will be designed to act as a virtual, multi-purpose student card and may be used for small-value payments.

The Pegasus project launched in 2007 was used to define operational specifications for a payment application on a mobile phone SIM card. A joint undertaking by banks, mobile phone operators, terminal manufacturers and international card schemes, Pegasus was tested in Caen and Strasbourg in 2007 and 2008. The project is being pursued and expanded through the "Nice, Territoire d'Innovation" initiative (cf. below).

"Nice, Territoire d'Innovation" Initiative

This initiative is designed as a full-scale test for the future development of contactless technology on cards and mobile phones. Participants include the main mobile phone operators, banks, technical service providers, local authorities and businesses. Some 3,000 phones fitted with NFC technology[19] were issued in the second quarter of 2010 in the Nice Côte d'Azur area. They can be used to carry out face-to-face payments and access other services (transport, tickets, loyalty cards, access control, information). The project is also intended to provide a launchpad for contactless card payments and establish a network of contactless payment terminals in the merchant community.

Impact of recent technological developments

Contactless cards

Most cards currently in issuance are covered by technical specifications that have changed little since the Observatory last issued its recommendations. However, new initiatives have included adding keypads to cards or introducing mechanisms to inform holders when cards have been activated. These projects could enable cards to offer functionalities that were previously restricted to mobile phones. However, they are running up against technical obstacles, mainly linked to issues of charging and range.

[19] Near field communication radio frequency technology designed to function at short distances (a few centimetres).

Contactless mobile phone payments

Growing use of mobile phones and the new functionalities built into smartphones increase the risks of attacks in this segment. However, different measures may be taken to mitigate their impact:

- introduce mobile software signatures[20] to keep the payment application strictly separate from other applications on the mobile;
- filter communications in order to isolate those intended for the payment application;
- research is also being done on secure modes that could be activated when making a mobile payment. These modes would protect the user's interaction with the payment application, notably by checking the integrity of the data entered on the keypad and displayed on the phone's screen.

This payment approach also introduces new participants, known as trusted service managers (TSMs), thereby increasing flows of information as well as the need for specific security measures to ensure the integrity and confidentiality of exchanged data. TSMs provide the link between issuers and mobile phones during the personalisation of payment applications (life cycle) or when counters are reset. They act as trusted third parties and must therefore ensure that a high level of security is maintained throughout these activities.

More generally, the projects and trials currently underway are designed to fine-tune the technical specifications of contactless payments by mobile phone – particularly as regards security aspects – prior to large-scale deployment in France. With this in mind, steps are being taken to bring together the initiatives by AEPM[21] and the international networks (Visa, MasterCard).

Additional recommendations by the Observatory

In 2007, the Observatory concluded that the particular risks associated with contactless payments were linked to the use of radio frequencies to exchange data, and to the fact that payments below certain set amounts were not subject to confirmation, meaning that holders could not be authenticated.

As a result, the Observatory issued two sets of recommendations in this area, on introducing measures to ensure that the holder's consent had been obtained and on guaranteeing a high level of security for components and applications.

As regards contactless cards, issuers have followed the Observatory's 2007 recommendations.

As regards contactless mobile phone payments, current projects and trials include plans to fine-tune the security mechanisms required for a large scale deployment. It will be necessary to ensure that all these measures are implemented when new contactless payment modes are launched on a full-scale basis.

[20] Cardlets for payment applications and midlets for phone/user interfaces. The former are stored in the secure element, the latter in the mobile phone.

[21] Association Européenne Payez Mobile. Created in October 2008, AEPM is an association of banks and telecommunications operators that is introducing contactless mobile phone payment solutions to France. AEPM is taking the Pegasus project forward.

The Observatory also recommends continuing research into and implementation of security practices for contactless cards and mobile phones to ensure high levels of trust in these payment instruments.

These measures include the use of a special PAN for contactless mode that is different from the PAN assigned when the payment card is used in contact mode or for card-not-present payments. This could limit the potential impact if the PAN were reused elsewhere in the event of compromise.

The Observatory recommends the following for mobile phones:

- supply a personal payment code that is different from the SIM card activation PIN, and from the user's payment card PIN. If the user can modify the personal code, the issuing bank should recommend choosing a code that is different from the user's other codes;
- use components whose level of security is at least equal to that of the chips used by cards in contact mode;
- stakeholders should consider the possibility of enhancing protection for holder interaction with the mobile phone payment application;
- entities involved in transactions relating to contactless payments by mobile phone (payments per se, but also personalisation/updating of applications and remote resetting of transaction counters) should implement cryptographic protection measures to ensure the integrity and confidentiality of data exchanged between systems.

Issuers of contactless cards should continue research into simple solutions to activate and deactivate contactless payment mode, similar to the protective cases already in use.

The Observatory will continue to track these innovative payment solutions, monitoring their final specifications and industry developments.

3|2 Security of card-not-present payments by mail and telephone

Strong growth in distance selling in recent years has been accompanied by a substantial increase in card-not-present payments. However, an observation of flows in e-commerce and in mail order/telephone order (MO/TO) sales[22] reveals contrasting trends. In 2008, online card payments continued to grow, while MO/TO card payments were down sharply, surely owing to increased use of the internet in distance selling. In all, 109 million MO/TO card payments were recorded in 2008, worth around EUR 10 billion (approximately 2% of the value of domestic transactions). MO/TO payments address specific needs among consumers and merchants. Mail order coupons, for example, are used for newspaper/magazine subscriptions and for placing orders by mail, particularly by people who do not have an internet connection. Payments are often made over the phone when the transaction is a timely one, such as a hotel, performance or taxi reservation.

The Observatory has noted a much higher fraud rate in card-not-present payments than in face-to-face and UPT payments in recent years. The 2008 report reviewed security measures for online card payments. The purpose of this study is to analyse issues of security for card-not-present payments by mail and phone.

[22] Here, a payment by telephone means a payment made by means of a phone call, rather than by an exchange of data, a trend that is emerging with the arrival of new solutions (mobile payments).

Security measures applied to card-not-present payments by mail and phone

When analysing issues of security in card-not-present payments, it is important to draw a distinction between:

- protection of card data (number, expiry date, CVx2) received through the communication channel, and subsequently used within the environment of the merchant and then within the environment of the bank or of their technical providers. If captured by fraudsters, these data[23] could be used to make fraudulent payments. For this reason, it is vital to protect such data, both when they are exchanged through transmission channels (computer, mail, internet), and also when they are used and, if applicable, stored. There are regulatory recommendations in this area, issued by France's CNIL, as well as professional guidelines, including the PCI DSS standards issued by Visa and MasterCard. This question is addressed by a separate study in this report on the security policies of issuers and acceptors. Accordingly, the following study does not tackle this issue;
- efforts to combat fraudulent card-not-present payments using misappropriated card data, no matter which method is used to obtain the data (theft of the card, data copying/generation techniques, etc.). The Observatory's fraud statistics illustrate the situation: in 2008, the fraud rate for MO/TO card payments increased to 0.280% from 0.201% in the previous year, and for the first time in 2008, the domestic fraud rate for MO/TO payments exceeded the rate for online fraud. The presence of fraudulent MO/TO payments raises questions about what is being done to detect suspicious transactions and make sure that buyers are the rightful cardholders. This study is intended to review the measures implemented in this area.

[23] Which are then said to be compromised.

The following box describes the stages that go into a MO/TO card-not-present payment:

Box 7 – MO/TO card-not-present payment

Channel	✉	☎
Holder	The holder fills out and posts the purchase slip, which includes the name of the holder, the card number, expiry date and CVx2.	The holder calls the number given by the merchant and pays by providing the same information to an operator or a voice mail service.
Merchant **(or service provider)**	The postal service delivers the letter, usually to a service provider that inputs the order and payment data and sends the information to the acquirer. Some data are kept.	An operator or a voice mail service, usually supplied by the merchant's service provider, receives the payment data and sends them to the acquirer. Some data are kept.
Acquirer	The acquirer receives the electronic payment order and sends it to the issuing bank.	
Issuing bank	The issuing bank receives the payment order, conducts the necessary checks, then authorises the transaction.	

Protection of payment data by the merchant is covered by PCI DSS[24] standards and falls outside the scope of this study.

Security solutions

The Technology Watch group examined the solutions used to ensure the authenticity of MO/TO card-not-present payments.

The procedures used by merchants to detect suspicious transactions consist in cross-referencing various pieces of information and parameters relating to the good or service purchased, the buyer, his or her payment data and the shipping address. By combining all the information, the merchant can be more or less sure that the transaction is not likely to have been fraudulently paid for. Such procedures exist for online payments and are adapted to suit the communication channel used in MO/TO card payments. Some established distance selling firms have recognised expertise in implementing this type of procedure and are thus capable of repelling attempts at fraud. But not all merchants use such procedures, notably because they generally require relatively costly human or technical resources. Merchants can use insurance services to protect themselves against fraud. Unless they rely on procedures for detecting suspicious transactions, these types of services are not dealt with here.

[24] These standards are established jointly by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.

Checking the CVx2, which was introduced for four-party cards some years ago[25], is one way to gain better assurance that the buyer has possession of the card whose number and expiry date are used to make payment. Card payment schemes require all merchants in France that accept card-not-present payments to verify the CVx2. While this system has proven its worth, the protection it provides has not eliminated all risk of fraud, given that fraudsters may have captured the CVx2 at the same time as the other data on the card, e.g. if the card is lost or stolen.

The Technology Watch group also looked at random generation of one-time passwords (OTP), since this approach is starting to be used for online card payments. The OTP allows the holder to identify himself or herself to the merchant as the rightful holder of the card. Unlike online payments, which allow computer verifications to be carried out, MO/TO payments might be hard to combine with OTPs. Care would have to be taken to prevent these passwords from being misused, say by an unscrupulous employee. At this stage, it is hard to imagine using this system for MO card payments. TO payments via a voice mail server are carried out in a digital environment and might thus offer a better guarantee of protection. The Technology Watch group nevertheless has reserves about the ability to introduce a solution of this type in a properly secure manner.

The Technology Watch group notes that the existing solutions do enable merchants to prevent some fraud, but cannot by themselves identify buyers as the rightful cardholders. Exposure to fraud could therefore remain high, and the Technology Watch group recommends using this type of payment with care. It proposes formulating advice and good practices for holders and merchants using this payment method.

Conclusion and proposed recommendations

To ensure the security of MO/TO card payments, the Technology Watch group notes the need for merchants and holders alike to take care.

In particular, the Observatory recommends the following good practices for merchants:

- wherever possible in card-not-present sales, merchants should endeavour to have payments made through a computerised channel, such as the internet, rather than over the phone or by mail, so as to be able to authenticate cardholders more effectively;
- merchants that gather payments by mail or phone should pay close attention to the security measures that they apply, particularly if they sell goods or services that are popular among fraudsters. For example, they could pay attention to the consistency of information provided by the buyer (e.g. check the shipping address). Merchants are encouraged to contact their payment service providers and professional associations to obtain the most up-to-date advice on this issue;
- merchants are reminded that they must gather and verify the CVx2 if there is one and the card payment scheme requires it;
- before concluding a sale, notably in the case of large-value transactions, merchants should conduct a number of checks with the holder to ensure that the latter is indeed the person who initiated the order, for example by calling to confirm the order. When the item is delivered or picked up, the merchant could check that the person who takes possession of the good or service is duly authorised to do so;
- merchants are encouraged to refrain from storing sensitive data once they are no longer needed.

[25] See the 2004 Annual Report of the Observatory for Payment Card Security.

The Observatory recommends the following good practices for cardholders:

– before sending card data by mail or phone, cardholders should make sure that they are dealing with a bona fide merchant. In particular, they should be on the watch for scams by fraudsters trying to obtain card data by promising a good or service that will never be delivered;

– before sending card data by mail or phone, cardholders should make sure that they properly understand the contractual terms of payment. In particular, before authorising payment, they should check whether the contract allows the merchant to make repeated debits;

– after payment, cardholders should check their account statement to make sure that the amount debited matches the authorised purchase. Cardholders are protected by law if their card or the data contained on it are used for fraudulent purposes;

– cardholders should never give their PIN out, either by mail or over the phone.

3|3 Security of new "thin" payment terminals

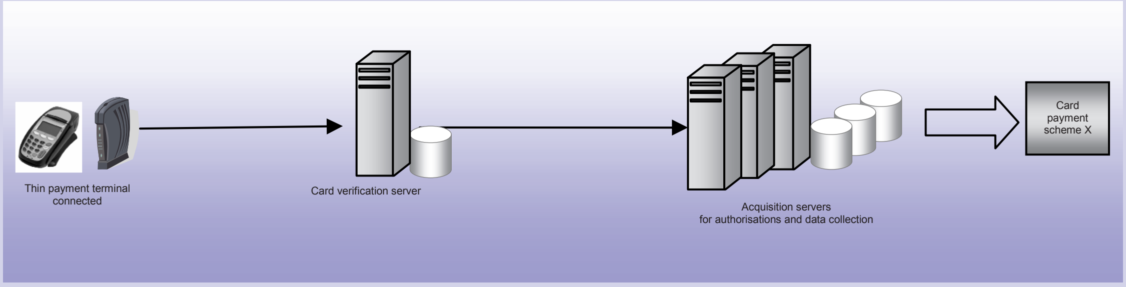
The payment terminals currently in deployment are sophisticated devices that can conduct numerous checks to verify the authenticity of the card and its holder. When they interact with the chip on the payment card, they activate complex cryptographic control mechanisms and indicate whether the card is valid and whether the holder is truly the card's owner. Historically, control functions were developed for these in-store terminals because of the expensive phone communications that would otherwise have been required between terminals and bank data centres. Major growth of phone networks over the last decade and more has gradually shifted the balance in this regard. With high-speed internet now widely available, it is becoming possible for certain controls to be carried out "online" by a remote server, instead of "offline", i.e. on the terminal itself. The idea is to simplify the security functions on the terminal – hence the term "thin" terminal – to cut manufacturing, deployment and even maintenance costs and requirements. Only recently developed, the concept has not actually been put into practice yet, although it is being studied. Some preliminary pilot projects are even underway[26]. With the payment services market opening up to new operators that are liable to offer acquisition services for card payment transactions, the Observatory decided to look at how "thin" terminals might work, to assess the security measures that could be implemented when introducing such terminals.

Security characteristics of "thin" payment terminals

The idea behind a "thin" payment terminal is to have most of the security functions performed not on the terminal, but on a remote server to which it is permanently connected. Compared with a conventional terminal, which is also connected, typically daily, for the collection of accepted transactions and the submission of authorisation requests, the main operational change is that the cryptographic checks needed to verify the authenticity of the card and the holder are carried out remotely. This means that some of the terminal's components can be streamlined, lowering costs. Another advantage is that application upgrades are easier to manage, because they can be centralised, either through server updates or through updates of terminals from the server. The way that applications are distributed also allows remote administration, with parameter management tailored to suit different points of acceptance or the countries in which they are located.

[26] While the Technology Watch group was conducting its work, a number of announcements were made concerning the inclusion of payment card readers on smartphones, to enable these devices to act as payment terminals. This type of device might qualify as a sort of "thin" terminal.

Box 8 – Card payment systems using "thin" terminals


Thin payment terminal connected
Card verification server
Acquisition servers for authorisations and data collection
Card payment scheme X

The in-store "thin" payment terminal is connected via a communication network to a card verification server (located either with the merchant or elsewhere, such as with a service provider), which is generally managed by the supplier of the "thin" payment terminal. It is this server that receives the payment and holder authentication data. Once the payment is validated, the server is the link to the standard systems used for acquisition and authorisation by participants in card payment schemes. The "thin" payment terminal is thus permanently connected to the card verification server.

Security solutions

The conventional payment terminals in use today perform a number of security functions, including offline checks by the terminal itself and online checks in conjunction with banks' authorisation servers. Controls are executed based on risk management rules that depend on the type of card and the size of the transaction:

- a conventional terminal conducts offline checks of the secure elements on the card's chip through a series of cryptographic dialogues. When the card is inserted, an initial series of checks verifies the authenticity of the card. Next, the entry of the PIN on the terminal keypad activates another series of checks, notably of the PIN, by comparing it against the number that is securely held in the card's chip. The terminal also contains lists of blocked card numbers so that it can refuse them;
- once connected to the authorisation server, the terminal can make an authorisation request to obtain validation of the transaction by the issuing bank. The data transmitted concern the transaction (amount, card number, expiry date, CVx2, merchant ID). The transaction is validated based on a check of the card's validity and potentially also on a check to ensure that there are funds on the account. When transactions are validated, the terminal generates a data collection file that is sealed to ensure its integrity when it is transmitted at the end of the day to the acquisition server.

In comparison, a "thin" terminal is designed to carry out the minimum number of controls, with the rest being conducted by the server. Of the controls usually performed offline by a conventional terminal, the card verification server could do the following:

- apply risk management rules governing required card controls;
- check the validity of the card's authentication key. In this instance, data sent over the communication network between the terminal and the card verification server would have to be protected;
- check whether the card is on the list of blocked cards;
- prepare authorisation requests and transaction files sent to acquisition servers.

However, PIN verification would not be moved to the card verification server.

"Thin" terminals are still exposed to the threat of misappropriation (PIN capture, flow takeover, network intrusion). But the sensitivity of the other devices is also changed. The card verification server becomes a sensitive element in the data transmission and processing chain. Because it centralises program updates, it is also directly involved in the remote management and maintenance of terminals. Furthermore, in such a setting, there is a vital need to protect flows of data exchanged initially between the "thin" terminal and the card verification server, and subsequently between that server and the acquisition server.

As a result, a number of security measures are needed to ensure the confidentiality, integrity and availability of data:

- the card verification server and the "thin" terminal must be protected to prevent data compromise or flow takeover. This makes it necessary to check the authenticity and physical and logical integrity of these devices;
- equipment operating systems and installed applications should be kept updated to ensure their security and particularly their integrity;
- data flows between the "thin" terminal and the card verification server should be protected to ensure the authenticity and confidentiality of data exchanged. The measures deployed should be adjusted depending on whether the card verification server is located with the merchant or its service provider. In the latter case, and particularly if networks that are typically open are used[27], it would be advisable to increase security for flows of exchanged data. Furthermore, since the "thin" terminal is to be permanently connected to the card verification server, steps should be taken to ensure that the networks used are configured to guarantee the availability of data exchanged;
- the same applies to data exchanges between the card verification server and the acquisition server. For example, these exchanges could be carried out by encrypting data and by using a virtual private network or SSLv3 or equivalent security protocol[28].

Furthermore, the security requirements of card payment schemes should be adjusted to reflect the architecture of "thin" payment terminals, to avoid weakening current levels of protection for chip/terminal dialogue and for the data processed by these devices.

Since application upgrades can be centralised, it is possible to perform updates very rapidly, enabling swift action to be taken in the event of a security failure.

Conclusion and proposed recommendations

"Thin" terminals are still at the drawing board stage, so it is impossible to say exactly what functionalities they will have. However, the pilot schemes currently being prepared and the existing interest in online terminal management suggest that these new devices are likely to develop over the coming years. Accordingly, the Observatory examined how these "thin" terminals might work and considered potential security measures.

Accordingly, the Observatory notes that it is possible for the majority of controls carried out by a conventional terminal during a card payment to be transferred to a remote card verification server. PIN verification should however continue to be performed by the "thin" terminal, which would thus remain a sensitive element in the payment chain. The card verification server would

[27] Cf. 2006 Annual Report of the Observatory, The Use of Open Networks in the Payment Card Environment, pp. 23 to 28.

[28] Cf. 2006 Annual Report of the Observatory, The Use of Open Networks in the Payment Card Environment, pp. 23 to 28.

also become a sensitive element. Moreover, in such a setting there is a vital need to protect flows of data exchanged between the "thin" terminal and the server.

With this in mind, the Observatory has identified a number of security measures to ensure the confidentiality, integrity and availability of sensitive card payment data. These measures concern, in particular, protecting the card verification server, the "thin" terminal, and the flows of data exchanged between these devices. The Observatory recommends that entities introducing card payment systems employing "thin" terminals make sure to apply measures of this kind. It also recommends adjusting the security requirements of card payment schemes to reflect the architecture of "thin" payment terminals, to maintain the current levels of protection for chip/terminal dialogue and for the data processed by these devices.

3|4 Progress on the migration to EMV

The implementation of the EMV ("Europay, MasterCard, Visa") specifications for chip cards in Europe represents a major issue in the fight against cross-border fraud. It concerns both cards themselves and accepting systems (payment terminals, ATMs, UPTs), which need to migrate to the new specifications in order to achieve a uniform level of protection throughout Europe. As it has done in the past six years, the Observatory again measured progress on EMV migration by collecting statistics on the migration process in France and Europe from the "CB" Bank Card Consortium and the European Payments Council (EPC). These figures show that the migration process is underway throughout Europe. Progress is good in most of the countries, broadly in line with the commitment of European banks within the EPC to complete migration by the end of 2010. The Observatory is nevertheless concerned about the lasting discrepancies in the migration process, which are likely to lead to the persistence of substantial cross-border fraud within Europe.

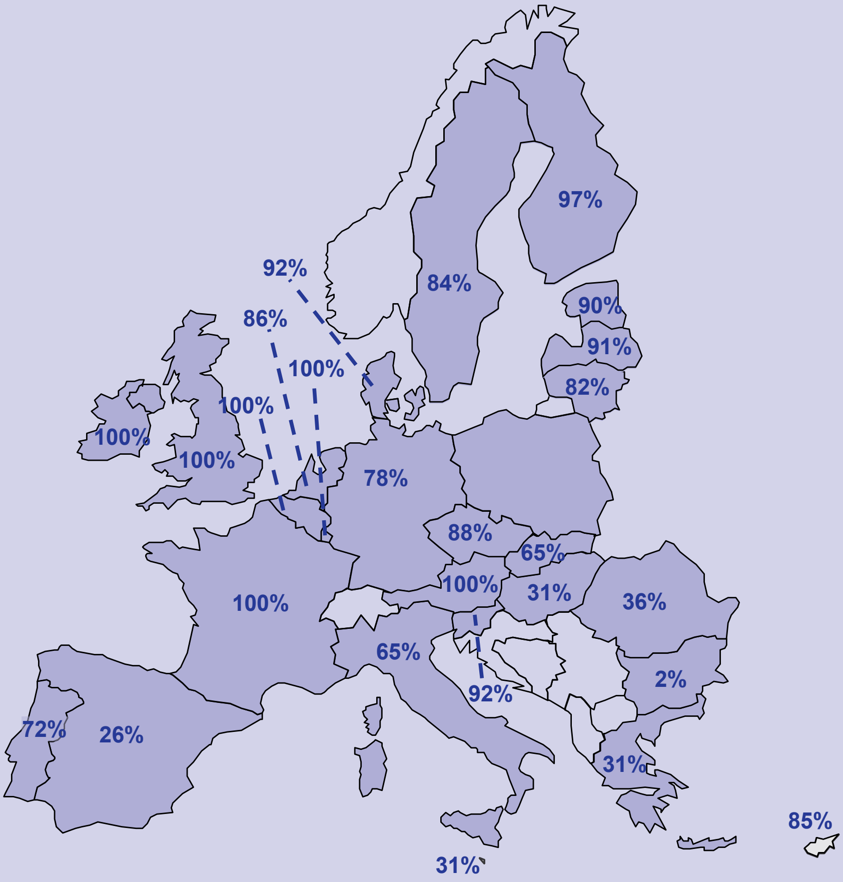
Progress on the migration to EMV in France

Migration to the EMV standard is practically complete in France. By the end of March 2010, according to statistics compiled by the "CB" Bank Card Consortium, 100% of "CB" cards, 99.8% of payment terminals and UPTs, and 100% of ATMs were EMV compliant. The remaining 0.2% of terminals and UPTs, which are not much used, will migrate at the time of their normal replacement.

Progress on the migration to EMV in Europe

In Europe, according to the data provided by the EPC for the period up to the end of March 2010, 69.8% of the four-party cards in use in the 27 countries of the European Union are now EMV compliant. This represents an increase of 2.3 percentage points in comparison with March 2009. The situation varies from one country to another (see Box 9). Whereas compliance with the SEPA interoperability rules began from early 2008 onwards, several countries, such as Bulgaria, have barely begun migrating to EMV, while others, including Spain and Hungary, have made little progress.

Box 9 – Deployment of EMV cards in Europe



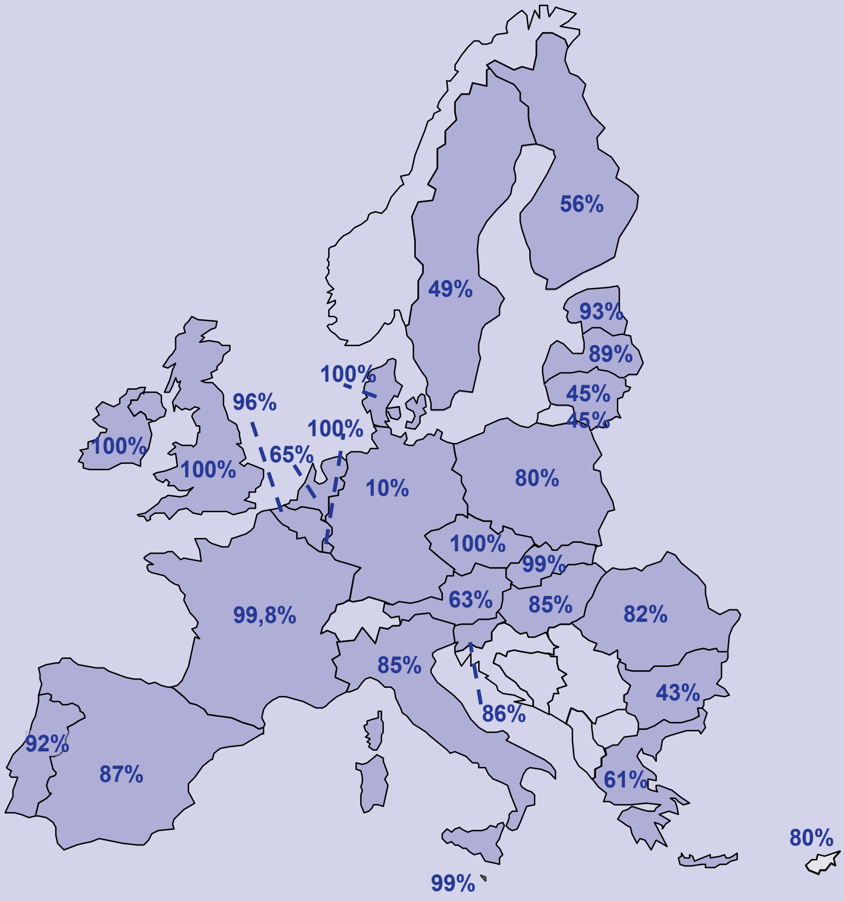
Source: European Payments Council – March 2010

Compared with last year, the map shows overall progress in card migration to the EMV standard. However, several countries, such as Bulgaria and Poland, have barely started migration, and others, like Spain and Hungary, have made little headway.

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

By the end of March 2010, the migration of acquisition systems to EMV had noticeably progressed: 80.0% of payment terminals (see Box 10) and 94.4% of ATMs (see Box 11) were EMV compliant. This represents an increase of 4 percentage points for payment terminals and 2.4 points for ATMs in comparison with March 2009. The situation still varies considerably from one country to the next both in terms of the percentage of compliant equipment and progress from one year to the next.

Box 10 – Deployment of EMV terminals and UPTs in Europe



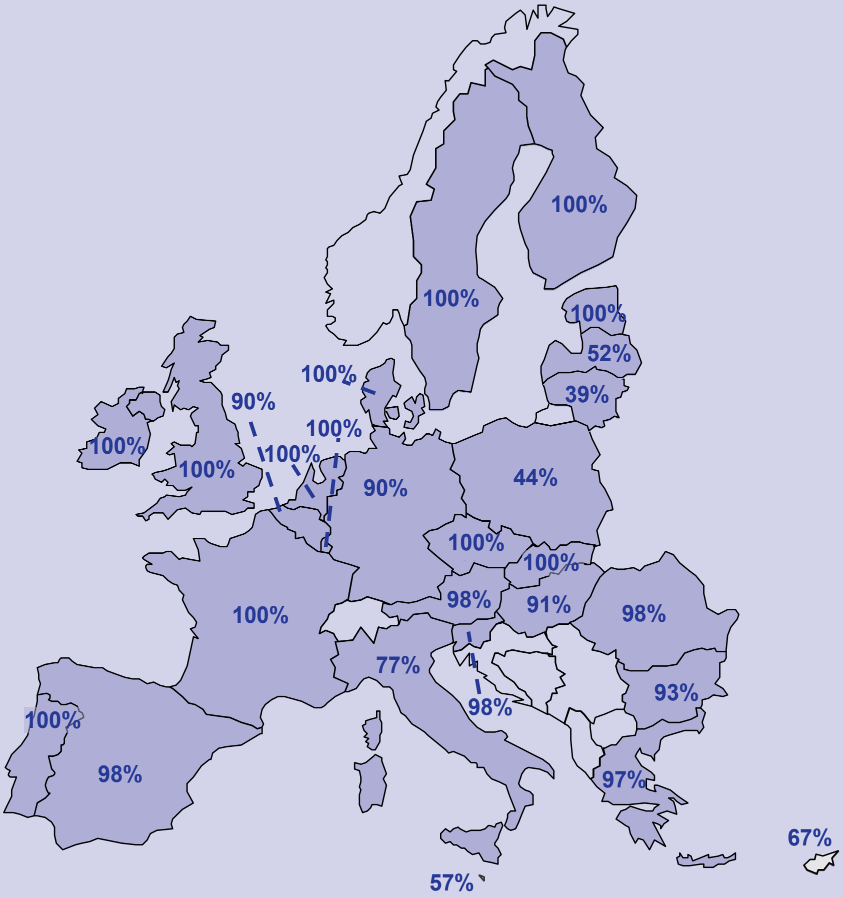
Source: European Payments Council – March 2010

The recorded trend for terminals and UPTs is the opposite of that for card deployment. Overall, the migration of terminals is taking place more rapidly in the countries of Southern Europe, which are the top tourist destinations, where the greatest number of cross-border transactions is likely to be made.

The situation in Germany has changed very little compared with March 2009, with the level of EMV compliant equipment remaining low. By contrast, the map shows progress being made in Sweden and the Netherlands.

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

Box 11 – Deployment of EMV ATMs in Europe



Source: European Payments Council – March 2010

Progress on migration of ATMs has been more uniform in Europe and is generally more advanced than among cards and terminals. However, there are still some disparities. Countries where the migration of ATMs to the EMV standard is still on-going have probably decided to convert the ATMs used by foreign tourists and visitors first. Italy is still slightly behind the other leading countries in terms of deployment, but the proportion of EMV compliant ATMs has improved since March 2009.

4 | CARDHOLDERS' PERCEPTION OF PAYMENT CARD SECURITY

Building on the survey conducted in 2007, the Observatory wanted to update the data collected on cardholders' perception of payment card security. In line with Banque de France recommendations on the security of online transactions, this year's study pays special attention to online payment security and to responses to the use of security solutions.

For this, the Observatory commissioned two surveys carried out by two different polling firms: a quantitative one by CSA and a qualitative one by LH2. The first survey was of a representative sample of 1,010 respondents between the ages of 18 and 74 living in metropolitan France, who were contacted over the phone between 8 and 15 February 2010[29]. The second survey, which concentrated on the perception of security in online payments and responses to five one-time authentication solutions[30], comprised semi-directed individual interviews of 40 people aged between 18 and 65[31].

4|1 The results of the survey of cardholders' perception of payment card security corroborate the trends observed in 2007

The proportion of people with cards is similar, but cards are being used more extensively, particularly for online payments

The vast majority of respondents – nine out of ten – possess at least one payment or ATM card. The main reason given for not holding a card is the lack of need (5% of respondents). Just 1.5% of people cited security concerns as the reason why they did not have a card.

Card usage is widespread in France, with eight holders out of ten using cards whenever or almost whenever possible. Compared with 2007, cards are now being used slightly more for payments at UPTs and in shops.

Meanwhile, the use of cards for online payments has increased fairly substantially since the last study. One person out of every two now makes online purchases using a bank card, compared with 38% in 2007.

As in 2007, some cardholders are still reluctant to use their payment cards abroad: 34% of travellers within Europe and 41% of travellers outside Europe never withdraw cash abroad, and 13% of cardholders travelling abroad never use their cards for withdrawals or payments.

[29] The sample was constructed using quotas relating to gender, age, occupational status and occupation of the respondents, as well as the size of the town or city and region of residence. Qualitative work before the survey involved meetings of several groups of cardholders with similar patterns of card use.

[30] A one-time authentication solution uses one-time codes, i.e. codes that can be used to protect just one transaction, to provide enhanced authentication for the holder or lawful user of the payment instrument.

[31] The main criteria used to structure the sample were as follows: frequency of online payments, use (or not) of security solutions, and parameters to ensure good representativeness in a qualitative study (gender distribution, age brackets, occupational status, internet use, location in Paris/outside Paris). Each interview lasted approximately one and a quarter to one and a half hours.

As in 2007, some cardholders are still reluctant to use their payment cards abroad: 34% of travellers within Europe and 41% of travellers outside Europe never withdraw cash abroad, and 13% of cardholders travelling abroad never use their cards for withdrawals or payments.

Most holders think cards are secure

More than three-quarters of cardholders (77%) still think that cards are safe to use, although this proportion is down slightly compared with 2007 (3 points). One-third of respondents think that payment cards are the least risky way to make purchases.

People who think cards are the safest means of payment are mainly those aged over 65, pensioners, people with secondary education or higher, people who belong to a couple and people who travel in Europe.

Even so, there is a disconnect between the overall opinion that holders express regarding card security and how they feel when actually using cards. Around 46% of French people say that they feel they are taking a risk when they pay by card.

Card payments are deemed to be safer when they are made at a shop in France than online or abroad

Transactions carried out in France are viewed as safest. In particular, paying at a shop in France is thought to be the safest type of transaction, with 94% of respondents expressing this view.

There were more concerns about payments by mail or phone in 2010 than in 2007, because just 25% of holders, compared with 32% in 2007, think that such payments are secure. Similarly, there was an increase in the perception of risk associated with paying a foreign merchant: 51% of holders, compared with 57% in 2007, consider making payments to foreign merchants to be safe.

Online payments are perceived as risky in France and abroad. If the website is French, just one-half of cardholders think online payments are safe. The feeling of risk is far greater when the website is foreign or in a language other than French, with just one cardholder out of every ten viewing such payments as secure.

As in 2007, 44% of card users have already used a means of payment other than their card because they thought they were running a risk. In 37% of cases, this situation arose when making online payments.

Cardholders are adopting good security habits, but they could be better informed about what to do in the event of fraud

Although three-quarters of card users, compared with 66% in 2007, think that financial institutions are best placed to improve card security, 76% of them think that they themselves also have a role to play in preventing fraud. This proportion has increased since 2007 (72%), showing that more and more people are adopting good security habits.

Most cardholders always take precautions to avoid the risks associated with card use. The most widespread practices include checking website security[32], taking care when entering the card's PIN in a shop and checking the amount displayed before approving payment.

However, consumers could be even more watchful if they were better informed about the risks and the steps to take in the event of fraud. Four card users out of ten still lend cards to family members, although this proportion is down compared with 2007, when it was five in ten. Although the proportion of people who think that they are liable in the event that their card is used fraudulently while still in their possession has declined (19% in 2010, compared with 25% in 2007), people are still generally unaware of the time limit for reporting cards lost or stolen: 59% of users think it is ten days or less, and only 4% know that the limit has been extended in certain circumstances, in accordance with provisions set out in the European Payment Services Directive.

Direct or indirect experience of fraud has little impact on user behaviour

The proportion of cardholders who have experienced fraud is more or less the same as in 2007, with 13% saying that they have been the victims of fraud and 18% reporting that they have experienced fraud indirectly. Online payments were the main source of reported fraud (27% of cases).

Experience of fraud has a fairly limited impact on behaviour. However, the effect increased compared with 2007, because almost one-half of fraud victims (45% compared with 37% in 2007) said that they had scaled back their card use as a result.

Fraud victims still trust their cards, however: 63% of people who have had direct experience of fraud say that their card is safe to use, compared with 77% for the general cardholder population. Indirect exposure to fraud has no impact on perceived card security.

[32] Notably by making sure that pages are encrypted when making payments (padlock icon appears to show that this is the case).

Box 12 – Attitudes towards card security

The survey made it possible to identify several types of behaviour and attitude in the cardholder population*:

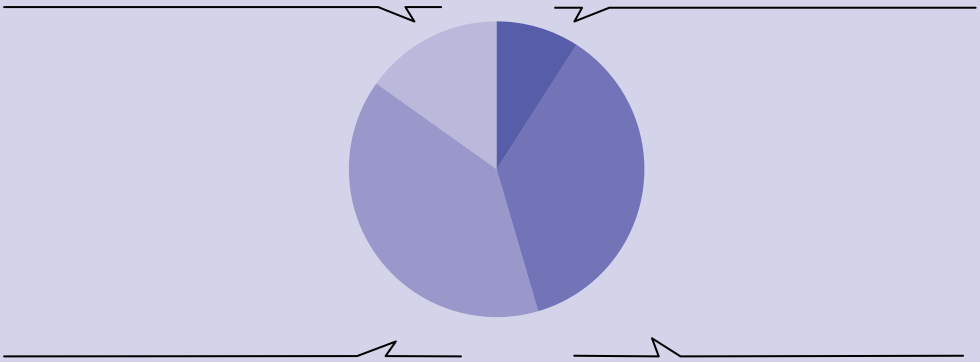
Anxious and vigilant (15%)

People in this group pay with their card as infrequently as possible, a fact that holds across all payment channels. They perceive cards as being generally risky, or even very risky, whatever the channel, and feel as though they are taking a risk when using cards. They do not know much about their card.

Confident (9%)

People in this group pay with their card whenever possible. They think cards are very safe to use and do not believe they are taking risks when using them. They do not take many precautions.

➔ *This group was stable compared with 2007*



Resigned (36%)

People in this group use their cards less frequently than those in other groups, although overall they feel that cards are fairly safe to use. However, they do believe that they are taking a risk every time they use their cards. They take fewer precautions than in 2007.

➔ *This group accounted for 36% of card users, compared with 28% in 2007.*

Informed (39 %)

People in this group pay with their card whenever possible and believe that cards are fairly safe to use. They do not think they are taking a risk when they use their cards. In their view, card security is improving, and they always take precautions to prevent fraud.

➔ *This group accounted for 28% of the population in 2007, and now accounts for 39%.*

* This user classification was prepared using the same method as in 2007. Because of changes to the questionnaire, just four groups could be identified, compared with five in 2007. Three groups are directly comparable to those of 2007: confident users, informed users and resigned users. Prudent users are now grouped with informed or resigned cardholders, while anxious users have become more vigilant.

4|2 People who make online payments have real sensitivity to the risk of fraud and like their bank to be involved in efforts to provide security solutions

The qualitative survey by LH2 highlighted the fact that buyers are genuinely sensitive to the risk of fraud. It also showed that they respond positively when their bank is involved in efforts to enhance security.

Perception of transaction security when making online purchases

Fraud risk is perceived as immaterial

The risk of fraud associated with online payments does not emerge as a major barrier to the growth of online shopping. Concerns about the principle of online buying itself or about how a website looks are far greater obstacles. Indeed, major barriers to online payments are mainly due to fears of not receiving delivery or receiving damaged goods, or the lack of confidence in the merchant’s website.

If online payment fraud does not come immediately to mind, this is chiefly because people perceive the risk of fraud as immaterial. Not knowing exactly how fraud could occur leads people either to distrust computers and the internet in general ("I get the feeling that it's easy to hack into any computer", or "you can do anything through the internet") or to forget about the risk. During online shopping transactions, the padlock icon and the letters "https" that appear on the screen are often the only reminders of the material risk of online payment fraud.

Real but different levels of sensitivity to the risk of fraud

Even so, all cardholders exhibit genuine sensitivity to the risk of fraud, although the perception of risk varies accordingly to respondents' experiences and personality. Three types of people can be identified:

- Nervous: these types of users are found across all age brackets between 25 and 65 and are highly sensitive to the risk of online fraud because of their intellectualised approach to this risk, regardless of whether they have had positive or negative experiences. For them, providing their bank details when making a payment over the internet is a real obstacle to online shopping;
- Cautious: this group talks about online fraud and believes that there is always a risk, but nevertheless makes online purchases – even large-value ones – on a more or less regular basis. This category mainly comprises people between the ages of 35 and 60 who make online payments at home;
- Vigilant: people in this group are aware of the risk of fraud, but for them it is primarily a stage to get through rather than a permanent worry. Once confidence is built up through practice and the experiences of family members, the risk of fraud ceases to be a deterrent to routine online shopping. Most of the people in this group are aged between 20 and 25, and make online payments either at home or when out and about.

Security habits adopted by users

The perception that there is a security risk attached to online transactions leads buyers to adopt a variety of their own security measures. These include paying attention to the reputation of the website and to whether it is a secure site, checking whether a padlock icon and the letters "https" appear, reading the site's security arrangements, not saving bank details on the computer, not buying in response to an email but going through the merchant's official site, and making sure to sign out of the payment page once the payment has gone through.

However, online shoppers sometimes behave inconsistently when it comes to preventing fraud, particularly by failing to systematically apply their security measures. For example, they may apply them to large-value but not small-value purchases. If an attractive price is offered, they may shop on unsecure websites.

In this respect, it would appear that sensitivity to the risk of online fraud sometimes fades over time, provided the user has no negative experiences. Trust in the merchant's website or a previous good experience on a website are viewed as more important than the security measures displayed.

Use of security solutions: helping banks to build strong relationships with customers

Users respond positively when banks are engaged and provide support

Whether they make many or few online payments, buyers always like the online payment security solutions offered by banks. In particular, the involvement of banks in introducing these solutions is seen as a guarantee of effectiveness and security.

Specifically, buyers are particularly receptive to a large-scale, overall approach by banks, which has several effects:

- symbolic: by getting involved, banks help to make online shopping more trustworthy. Users do not think that banks would provide security solutions for unreliable sites;
- psychological: introducing security solutions forms part of building a special relationship between the online shopper and his or her bank. The fact that the bank is working to give customers greater peace of mind and acting in their interests strengthens the ties between the user and his/her bank;
- financial: deploying technical security solutions and insurance mechanisms provides peace of mind that is positively perceived by online shoppers.

Factors of success when introducing security solutions

The study revealed that several factors had a determining impact on success when introducing security solutions for online shopping.

First, solutions have to be specifically tailored to and compatible with different types of behaviour or usage. While solutions have to encourage nervous users to "take the plunge" and make online purchases, they also have to suit cautious users as they get accustomed to shopping online, as well as vigilant users, who are more familiar with online payments and use the solutions more frequently. Proposed security solutions must therefore be tailored to each user type so that people in all categories can use them and get the expected benefits.

Second, banks must provide appropriate communications to support the introduction of these security solutions. Banks' efforts in this area are positively perceived and widely appreciated, provided that users get support when security solutions are deployed.

4|3 Systematically positive responses to using security solutions for online payments

Positive responses

One-time authentication systems

Participants in the qualitative study were asked to assess five one-time authentication solutions[33] on a merchant website.

Four of the solutions generate a one-time password (OTP) that has to be entered online when making payment:

- matrix card with secret path: the OTP is generated by entering codes obtained from the card by means of a path known only to the user;
- token: when a button is pressed, an algorithm contained in a small electronic device generates the OTP;
- OTP sent by text message;
- mini smartcard reader: the OTP is displayed on the screen of the reader after the holder inserts the bank card and enters his PIN.

The fifth solution is based on a USB key with an electronic certificate. The holder has to connect the key to the computer when making payment before entering the key's PIN, which is needed for authentication.

[33] Elca, Vasco and Xiring (now Gemalto) supplied the solutions used in the survey.

Box 13 – One-time authentication systems

Matrix card
with secret path

Token

Mini smartcard reader

OTP sent by
text message

USB key
with electronic certificate

Security solutions welcomed

Introducing security solutions for online transactions is perceived as a way to provide welcome peace of mind. People who make online payments trust banks to put in place reliable mechanisms, insofar as this comes within their responsibilities and seems legitimate. In particular, having to go through the bank's website during authentication always elicits a very positive response.

The fact that paying online takes longer because of the additional authentication step does not appear to be problematic.

Response criteria

Users' positive responses vary according to three characteristics of the solutions proposed in the survey:

– fit with the user's lifestyle and current online payment practices: the solution (reader, card, key, etc.) embodies a risk of fraud that is usually viewed as immaterial. It will be better received if it fits with the holder's lifestyle and sensitivities (e.g. mobile/not mobile) and perception of online payments as highly risky or not very risky;

– familiarity and ease of use: users do not think about the solution in terms of the additional time required; they are more interested in how easy the solution is to use and carry around, as well as the associated risk of error;

– reliability and security: users pay close attention to the risks that the solution might stop working, malfunction or be lost or stolen.

Preferences differ according to profile

While none of the systems is rejected, responses vary depending on experience in online payments.

Buyer profile dictates choices. People who spend most online prefer simple solutions systems that are easy to use on the go, whereas people who spend smaller amounts look for an image of security and a setting that reminds them of paying by card in a shop.

The matrix card has fans across the board, without dominating any particular group. Users see two advantages: the nature of the card makes it reliable, and the secret path provides security. However, users often think the matrix card is too old-fashioned to fit with their lifestyle.

Nervous users

Nervous users, whose high sensitivity to the risk of online fraud is an obstacle to paying over the internet, have a relative preference for the smartcard reader, which reminds them of paying in a shop. It is associated with merchants' payment terminals, which explains the attention placed on the larger of the two models presented.

This familiar object builds confidence because of its ease of use and the security guarantee provided by requiring the PIN to be entered. People do not connect it with their bank card, but imagine it at home, next to the computer. This type of solution offers the closest fit with the payment practices of this user group.

Cautious users

Cautious users are highly sensitive to the risk of fraud, but this does not prevent them from paying online on a more or less routine basis. They prefer the token and text message options because they are easy to use and because they signal the shift to mobile types of use.

Many of the respondents are familiar with, and have tried out, the OTP by text message method. They are comfortable with this approach because the mobile phone is a familiar object that they carry around with them at all times. They also like the text method because it removes the need for another device to generate OTPs.

There is a strong sense of security associated with making payments using this solution, because of the OTP and the personal nature of the device used.

Vigilant users

Vigilant users who routinely make online payments both at home and on the go, and who are therefore less concerned about the risk of fraud, prefer the token and USB key methods, although some users said that they would like these solutions to go virtual.

Because there is no secret code to memorise, the token is extremely easy to use. The OTP is generated by pressing a button. Moreover, users spontaneously associated the token with mobility, which is a characteristic of payment practices in this group. The fact that the token can be carried in a pocket or on a keyring makes it easy to transport. Having to enter a OTP is deemed a sufficient guarantee to ensure the security of online transactions.

The USB key, meanwhile, is viewed as a familiar and modern device. Because they are used to using USB keys, internet users are immediately comfortable with this solution and use it intuitively. Moreover, it is associated with new technology instruments, such as the 3G key.

The key provides a strong sense of security, which stems from the overall solution (electronic certificate, personal nature of the USB key) as well as from the requirement to enter the key's PIN to generate the OTP for online payments. The fact that the key can be used both at home and out and about explains why it fits best with the online payment practices of vigilant users.

Different impacts on payment behaviour

The introduction of security solutions for online payments would affect the payment patterns of all holders, but the impact may vary according to the buyer's profile.

Nervous users are likely to "take the plunge" and start making online payments

Nervous users, whose high sensitivity to the risk of fraud is an obstacle to paying over the internet, most often say that the introduction of security solutions for online transactions is likely to get them started making payments over the internet.

However, this overall response needs to be clarified. Some of these respondents will immediately start paying online because they feel protected by their bank and because they find paying by card more convenient than other methods, such as sending a cheque.

Others, however, are still hesitant. According to their feedback to the survey, they would be reassured by a guarantee of security when paying over the internet, but this might not translate into actual online transactions until several months or years later.

Cautious users are the most sensitive to the support provided by banks

Cautious users, who make online payments despite being highly attuned to the risk of fraud, are the most sensitive to the support provided by banks and approve of efforts to aid and support customers.

While the actual effects are hard to quantify, some respondents state clearly that they might increase the number or size of purchases, as well as the number of sites visited, because of the greater peace of mind procured by the introduction of security solutions.

Others remain prudent and do not imagine that they will rush into anything. Although they do not plan to scale back their current use of online payments, their behaviour will continue to hinge on their confidence in the internet or in the appearance of websites.

Vigilant users expect "greater peace of mind" but also "more constraints"

Vigilant users, who already do a lot of online shopping, like the approach taken by banks, which should provide "greater peace of mind" about transaction security concerns.

Some of them do not think that this will entail significant changes to their online purchasing patterns, perhaps because they already do a lot of shopping on the internet.

For others, however, improved security could mean that they visit a wider range of merchant sites and might also increase the amount of online buying that they do.

A general preference for effectiveness over ease of use

The findings of the quantitative survey clarify and quantify users' perceptions and behaviour in response to the introduction of security measures for online transactions. While the scope of this study is slightly different from that of the qualitative survey (just four solutions are considered: mini card reader, OTP sent by text message, entering a birthdate when making payments and answering a question), it nevertheless quantifies the trends observed during the interviews.

	Ease of use	Perceived effectiveness	Desire to use
Enter birthdate	90%	35%	45%
Answer a question	85%	54%	54%
Enter OTP sent to mobile phone	71%	70%	64%
Enter OTP generated by a mini reader	60%	76%	69%

▲ Table 9 – **Authentication solutions offered by banks: contrasting perceptions**
(% of people making online card payments)

The above figures reveal a general preference for perceived effectiveness over ease of use, with the desire to use one of the four security solutions increasing with the perceived effectiveness of that solution. People appear to be ready to put up with some usage constraints provided that the solution they employ when making online payments seems effective to them.

Box 14 – Security tips for cardholders

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

Be responsible

– Your card is strictly personal: do not lend it to anyone, no matter how close they are to you.

– Keep track of your card, check regularly to see that you still have your card.

– If your card comes with a PIN, keep the code secret. Do not give it to anyone. Memorise it. Avoid writing it down and never keep it with your card.

– Make sure that nobody can see you enter your PIN. In particular, shield the keypad with your other hand.

– Read your statements carefully and regularly.

Be aware

When paying a merchant:

– Watch how the merchant uses your card. Do not let your card out of your sight.

– Make sure to check the amount displayed on the terminal before validating the transaction.

When withdrawing cash from ATMs:

– Check the appearance of the ATM. Try not to use machines that you think have been tampered with.

– Follow the instructions displayed on the ATM screen: do not let strangers distract you, even if they are offering their help.

– If the ATM swallows your card and you cannot retrieve it immediately from the bank branch, report it right away.

When making online payments:

– Protect your card number: do not store it on your computer, never write it in an e-mail message and verify the security features of the merchant's website (padlock in the lower corner of window, URL starting with "https", etc.).

– Make sure you are dealing with a reputable company. Make sure that you are on the right site and read the general terms of sale carefully.

– Protect your computer by running the security updates offered by software editors (usually free) and by installing antivirus software and a firewall.

When travelling to other countries:

– Find out what precautions you need to take and contact the card issuer before leaving to find out about card protection systems that may be implemented.

– Remember to take the international telephone numbers for reporting lost or stolen cards.

Know what to do

If your card is lost or stolen:

– Report it immediately by calling the number provided by the card issuer. Make sure to report all of your lost and stolen cards.

– If your card is stolen, you must also file a complaint with the police as soon as possible.

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

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

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

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

APPENDIX A | PROTECTION FOR CARDHOLDERS IN THE EVENT OF UNAUTHORISED PAYMENTS

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

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

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

Domestic and intra-Community transactions

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

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

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

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

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 the part of the holder, or from a failure to fulfil the terms of safety, use or blockage agreed with the payment service provider, whether with intent or through gross negligence.

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

After submitting notification to block the card

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

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

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

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

Transactions outside Europe

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

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

The payment transactions concerned by these adjustments include transactions made with a payment card whose issuer is located in metropolitan France, in the overseas departments, Saint Martin or Saint Barthelemy, on behalf of a beneficiary whose payment service provider is located in a non-European State[3], 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, Mayotte, 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] that is not part of the EEA agreement (EU + Lichtenstein, Norway and Iceland).

APPENDIX B | MISSIONS AND ORGANISATIONAL STRUCTURE OF THE OBSERVATORY

Decree 2002-709 of 2 May 2002 implementing Article L. 141-4 of the Monetary and Financial Code concerning the Observatory for Payment Card Security, amended by Decree 2009-654 of 9 June 2009, lays down the missions, composition and operating procedures of the Observatory.[1]

Scope

It is generally accepted that a payment card is any card issued by a payment service provider that enables its holder to withdraw or transfer funds[2].

Consequently, the Observatory's remit covers cards issued by credit institutions or other assimilated entities that serve to withdraw or transfer funds. It does not cover the single-purpose cards that, pursuant to Article L. 511-7 I. 5° of the Monetary and Financial Code, benefit from an exemption to banking monopoly. These cards are issued by a single undertaking and accepted as means of payment by said undertaking itself or by a limited number of acceptors that have signed a commercial franchise agreement with it.

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 credit institutions (generally referred to as "three-party" cards),
- a large number of issuing and acquiring credit institutions (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 deposit account and enable their holders to make withdrawals or payments that are debited in accordance with a timeframe set out in the card issuance contract. The debit may be immediate (for withdrawals or payments) or deferred (for payments).
- *Credit cards* are backed by a credit line that carries an interest rate and with a maximum limit negotiated with the customer. These serve to make payments and/or cash withdrawals. They enable holders to pay the issuer at the end of a determined period (over 40 days in France). The acceptor is paid directly by the issuer without delay.
- *National cards* serve to make payments or withdrawals exclusively with acceptors established in France;

[1] The regulatory provisions applicable to the Observatory are laid out in Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the Monetary and Financial Code.

[2] According to Article L. 132-1 of the Monetary and Financial Code as worded prior to 1 November 2009.

- *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 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".

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 General Secretary of the Autorité de Contrôle Prudentiel and his/her representative,
- Ten representatives of payment card issuers, particularly four-party 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 Annex C to this report.

The members of the Observatory, other than those representing the State, the Governor of the Banque de France and the General Secretary of the Autorité de Contrôle Prudentiel, are appointed for a three-year term. Their term can be renewed.

The President is appointed among these 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

Pursuant to the Decree of 2 May 2002 amended by Decree 2009-654 of 9 June 2009[3], the Observatory meets at least twice a year at the invitation of its President. The meetings are held in camera. Measures proposed within the Observatory are adopted by absolute majority. Each member has one vote; the President has the casting vote in the event of a tie. In 2003, the Observatory adopted rules of procedure that delineate its working conditions.

The secretariat of the Observatory, which is ensured by the Banque de France, is responsible for organising and monitoring meetings, centralising the information required for the establishment of payment card fraud statistics, collecting and making available the information required to monitor the security measures adopted and maintain the technology watch in the field of payment cards. The secretariat also drafts the Observatory's annual report that is submitted to the Minister of the Economy and Finance and transmitted to Parliament.

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

Given the sensitivity of the data exchanged, the members of the Observatory and its secretariat are required to maintain the confidentiality of the information that is transmitted to them in the course of their work. To this end, the Observatory's rules of procedure stipulate the members' obligation to undertake to ensure the complete confidentiality of working documents.

[3] The regulatory provisions applicable to the Observatory are laid out in Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the Monetary and Financial Code.

APPENDIX C | MEMBERS OF THE OBSERVATORY

The current members of the Observatory were named by an Order of the Minister of the Economy, Finance and Industry dated 20 April 2006, supplemented by an Order dated 22 June 2006. The list of members was altered in 2007 by two Orders dated 27 June and 25 October 2007, and again in 2009 by an Order dated 29 June 2009.

List of members since 29 June 2009

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Jean-Pierre BRARD
Deputy

Nicole BRICQ
Senator

Representatives of the Secretary General of the Autorité de Contrôle Prudentiel

Jean-Luc MENDA
Banking System Oversight Directorate
Philippe RICHARD
General Secretariat

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

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

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

– The Senior Official for Defence:
Emmanuel SARTORIUS

– The Head of the Treasury or his/her representative:
Henri JOHANET
Alexis ZAJDENWEBER
Marianne CARRUBBA

Nominated on proposition by the Minister of Consumer Affairs:

– The Director of the General Directorate for Competition, Consumer Affairs and the Punishment of Fraud Offences or his/her representative:
Jean-Pierre GERSKOUREZ
Serge DORE

Nominated on proposition by the Minister of Justice:

– The Director for Criminal Affairs and Pardons or his/her representative:
Alexandra VAILLANT
Cédric SAUNIER

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:
Christian AGHROUM
Adeline CHAMPAGNAT

Nominated on proposition by the Minister of Defence:

– The Director General of the Gendarmerie Nationale or his/her representative:
Éric FREYSSINET

Nominated on proposition by the Deputy Minister of Industry:

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

Representatives of payment card issuers

Yves BLAVET
Head of Payment Instruments – Société Générale

Jean-Marc BORNET
Director – Groupement des Cartes Bancaires

Jean-François DUMAS
Vice President – American Express France

Bernard DUTREUIL
Director – Fédération bancaire française

Bernard GOURAUD
Technologies Director –
Banque Populaire – Caisse d'Epargne

François LANGLOIS
Director, Institutional Relations – BNP Paribas Personal Finance

Frédéric MAZURIER
Administrative and Financial Director – Société des Paiements Pass (S2P)

Gérard NEBOUY
CEO – Visa Europe France

Emmanuel PETIT
Chairman and CEO – MasterCard France

Narinda VIGUIER
Director, Interbank Strategy and Coordination – Crédit Agricole SA

Representatives of the Consumer Board of the National Consumers' Council

Régis CREPY
National Confederation – Associations familiales catholiques (CNAFC)

Valérie GERVAIS
General Secretary – Association FO Consommateurs (AFOC)

Christian HUARD
General Secretary – Association de défense d'éducation et d'information du consommateur (ADEIC)

Jean-Pierre JANIS
Representative – Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Representatives of merchants' professional organisations

Philippe JOGUET
Department Head, Regulation and Sustainable Development – Fédération des entreprises du commerce et de la distribution (FCD)

Marc LOLIVIER
General Delegate – Fédération du e-commerce et de la vente à distance (Fevad)

Jean-Jacques MELI
Representative – Chambre de commerce et d'industrie du Val d'Oise

Jean-Marc MOSCONI
General Delegate – Mercatel

Philippe SOLIGNAC
Vice President – Chambre de commerce et d'industrie de Paris/ACFCI

Persons chosen for their expertise

Philippe CAMBRIEL
Executive Vice President – Gemalto

David NACCACHE
Professor – Ecole Normale Supérieure

Sophie NERBONNE
Deputy Head of Legal and International Affairs and Assessments – Commission nationale de l'informatique et des libertés (CNIL)

APPENDIX D | STATISTICS

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

- The 136 members of the "CB" Bank Card Consortium, with international data provided by MasterCard and Visa Europe France;
- Ten three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco;
- Issuers of the electronic purse Moneo.

The Observatory also received statistics collected by the distance selling federation Fevad from a representative sample of its members.

Total number of cards in circulation in 2009: 90.6 million

- 62.4 million four-party cards ("CB", MasterCard and Moneo);
- 28.2 million three-party cards.

Number of cards reported lost or stolen in 2009: around 605,000

Domestic transactions involve a French issuer and a French accepting merchant. There are two types of international transactions: between a French issuer and a foreign merchant, and between a foreign issuer and a French merchant.

The payment card market in France

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
Four-party cards	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**
Face-to-face and UPT payments	6,118.98	271.57	130.92	9.41	149.19	12.14
Card-not-present payments excl. online payments	123.28	11.19	9.06	0.94	7.11	2.40
Card-not-present online payments	245.97	19.08	66.56	3.48	12.84	1.63
Withdrawals	1,492.38	108.73	41.87	4.97	29.72	5.04
Total	**7,980.61**	**410.56**	**248.42**	**18.80**	**198.85**	**21.21**
Three-party cards	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**
Face-to-face and UPT payments	229.20	20.76	8.78	1.60	13.09	2.40
Card-not-present payments excl. online payments	3.98	0.31	0.15	0.02	0.22	0.02
Card-not-present online payments	5.75	0.63	0.32	0.04	0.47	0.06
Withdrawals	9.17	0.86	na	na	na	na
Total	**248,10**	**22.55**	**9.24**	**1.66**	**13.78**	**2.49**
Grand Total	**8,228.72**	**433.11**	**257.67**	**20.46**	**212.63**	**23.70**

Source: Observatory for Payment Card Security

Breakdown of four-party card fraud by type of transaction, type of fraud and geographical zone

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
	Volume (k)	Value (€k)	Volume (k)	Value (€k)	Volume (k)	Value (€k)
Face-to-face and UPT payments	**462.2**	**35,642.0**	**214.2**	**42,660.3**	**338.0**	**68,778.1**
Lost or stolen cards	379.5	33,116.3	74.9	8,784.7	99.1	10,236.2
Intercepted cards	9.6	581.8	1.7	218.9	3.9	525.3
Forged or counterfeit cards	37.1	1,937.4	124.4	31,039.8	75.0	25,947.3
Appropriated numbers	0.0	6.6	6.3	1,832.0	78.3	16,192.4
Other	0.0	0.0	6.9	748.8	81.8	15,849.8
Card-not-present payments excl. online payments	**376.6**	**27,345.9**	**55.1**	**8,604.5**	**na**	**na**
Lost or stolen cards	0.4	31.1	17.5	2,558.3	na	na
Intercepted cards	0.0	1.1	0.1	15.8	na	na
Forged or counterfeit cards	0.0	1.0	13.1	2,250.3	na	na
Appropriated numbers	397.1	27,312.5	17.0	2,221.8	na	na
Other	0.0	0.2	7.4	1,528.2	na	na
Card-not-present online payments	**365.9**	**51,576.1**	**464.6**	**50,594.0**	**na**	**na**
Lost or stolen cards	0.6	109.3	141.7	14,342.8	na	na
Intercepted cards	0.0	0.1	0.4	44.8	na	na
Forged or counterfeit cards	0.0	2.3	104.7	12,041.3	na	na
Appropriated numbers	365.3	51,463.9	151.8	16,446.4	na	na
Other	0.0	0.5	66.0	7,718.8	na	na
Withdrawals	**85.5**	**19,838.3**	**103.2**	**16,467.2**	**9.1**	**2,754.5**
Lost or stolen cards	82.2	19,367.1	11.5	1,933.6	3.0	691.4
Intercepted cards	1.3	172.8	0.1	24.6	0.1	29.1
Forged or counterfeit cards	2.0	298.3	88.8	14,069.3	5.8	2,002.1
Appropriated numbers	0.0	0.0	0.2	24.8	0.1	14.7
Other	0.0	0.0	2.5	414.9	0.1	17.2
Total	**1,275.2**	**134,402.3**	**837.1**	**118,326.0**	**347.2**	**71,532.6**

Source: Observatory for Payment Card Security

Breakdown of three-party card fraud by type of transaction, type of fraud and geographical zone

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
	Volume (k)	Value (€k)	Volume (k)	Value (€k)	Volume (k)	Value (€k)
Face-to-face and UPT payments	**13.96**	**5,376.17**	**8.56**	**2,023.30**	**3.30**	**1,013.51**
Lost or stolen cards	4.87	925.38	1.17	192.97	0.27	54.72
Intercepted cards	3.47	608.37	0.35	139.63	0.05	17.57
Forged or counterfeit cards	0.78	236.21	4.30	911.98	1.07	272.51
Appropriated numbers	0.31	307.45	0.03	13.69	0.01	14.36
Other	4.53	3,298.76	2.71	765.03	1.90	654.35
Card-not-present payments excl. online payments	**7.30**	**2,987.62**	**6.54**	**1,089.87**	**6.52**	**3,585.02**
Lost or stolen cards	1.85	703.22	2.12	112.56	0.84	384.43
Intercepted cards	0.73	209.74	0.05	13.18	0.37	146.35
Forged or counterfeit cards	2.15	761.29	1.60	378.97	3.20	1,682.84
Appropriated numbers	0.32	220.85	0.00	0.00	0.01	1.66
Other	2.26	1,092.52	2.78	585.17	2.11	1,369.74
Card-not-present online payments	**0.83**	**218.12**	**0.91**	**197.98**	**4.90**	**686.67**
Lost or stolen cards	0.10	25.25	0.01	1.31	0.22	48.01
Intercepted cards	0.01	5.06	0.01	2.10	0.04	4.00
Forged or counterfeit cards	0.02	2.56	0.01	7.46	0.23	35.94
Appropriated numbers	0.14	64.18	0.00	0.60	0.00	0.57
Other	0.56	185.07	0.88	168.50	4.40	598.14
Withdrawals	**3.19**	**935.99**	**na**	**na**	**na**	**na**
Lost or stolen cards	2.65	748.97	na	na	na	na
Intercepted cards	0.29	121.25	na	na	na	na
Forged or counterfeit cards	0.00	0.00	na	na	na	na
Appropriated numbers	0.00	0.00	na	na	na	na
Other	0.24	65.77	na	na	na	na
Total	**25.28**	**9,581.90**	**16.01**	**3,295.15**	**14.72**	**5,285.20**

Source: Observatory for Payment Card Security

APPENDIX E | 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:

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

2. 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 and card used in France,
  - French issuer and card used abroad;
- the type of payment card[2], including electronic purses;

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

[1] In the case of the internet, the acceptor may be different from the service provider, or a trusted third party (payments, donations made by internet users wishing to support a web site, cause, etc.).

[2] As defined by Article L. 132-1 of the Monetary and Financial Code as worded prior to 1 November 2009.

Fraud typology

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

The origin of the fraud:

- *Lost or stolen cards:* the fraudster uses a payment card obtained without the knowledge of the lawful cardholder, following card theft or loss;
- *Intercepted cards:* cards intercepted when sent by issuers to lawful cardholders. While this type of origin is similar to theft or loss, it is nonetheless different because it is not easy for a cardholder to ascertain that a fraudster is in possession of a card that belongs to him/her; it also entails risks specific to procedures for sending cards;
- *Forged or counterfeit cards:* an authentic payment card may be falsified by modifying magnetic stripe data, embossing or programming. Creating a counterfeit card means creating an object that appears to be an authentic payment card and/or is capable of deceiving a payment machine or a person. For payments made via UPTs, counterfeit cards incorporate the data required to deceive the system. In face-to-face transactions, counterfeit cards present certain security features found on authentic cards (including visual appearance), incorporate data stored on authentic cards, and are intended to deceive acceptors;
- *Appropriated number:* a cardholder's card number is taken without his knowledge or created through card number generation (see fraud techniques) and used in card-not-present transactions;
- *Unallocated card numbers:* use of a true PAN[3] that has not been attributed to a cardholder, generally in card-not-present transactions;
- *Splitting payments:* splitting up payments so as not to exceed the authorisation limit defined by the issuer.

Fraud techniques:

- *Skimming:* technique that consists in copying the magnetic stripe of a payment card using an illegal card reader known as a skimmer embedded in merchants' payment terminals or automated machines. 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;
- *Opening of a fraudulent account:* opening of an account using false personal data;
- *Usurpation of identity:* fraudulent acts linked to payment cards and involving the use of another person's identity;
- *Wrongful repudiation:* a cardholder, acting in bad faith, disputes a valid payment order that he/she initiated;
- *Hacking automated machines:* techniques that consist in placing card duplication devices in UPTs or ATMs;
- *Hacking automated data systems, servers or networks:* fraudulent intrusion into these systems;
- *Card number generation:* using issuers' own rules to create payment card numbers that are then used in fraudulent transactions.

[3] Personal Account Number

Types of payment:

- *face-to-face payment*, carried out at 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;
- the issuer is established in France and the acquirer abroad;
- the issuer is established abroad and the acquirer in France.

Director of publication	**Robert Ophèle** Director General, Operations Banque de France
Chief editor	**Yvon Lucas** Director, Payment Systems and Market Infrastructures Banque de France

Banque de France Publishing
Press SIMA
Document finalised 15 October 2010
Deposited in October 2010
ISSN 1768-2991

2009 REPORT

The Observatory for Payment Card Security is a French forum meant to promote dialogue and exchange of information between all parties that have an interest in the security and the smooth functioning of card payment systems, in which participate two Members of the French Parliament, representatives of relevant public administrations, card issuers and card users (i.e. merchants and consumers).

Created by virtue of the Everyday Security Act of November 2001, the Observatory monitors the implementation of measures adopted by issuers and merchants to strengthen payment card security, establishes harmonized statistics on plastic card fraud and maintains a technology watch.

The present document reports on the annual activities of the Observatory. Pursuant to the Article L. 141-4 of the French Monetary and Financial Code, it is addressed to the Minister of the Economy and Finance and transmitted to Parliament.

This report has been prepared by the

BANQUE DE FRANCE

EUROSYSTÈME

2010 Issue

BdF - 29598 - Ateliers SIMA - 200325 - 4-10