2006 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

Internal Postcode 11-2323

31, rue Croix-des-Petits-Champs – 75049 Paris Cedex 01

2006

Annual Report of the Observatory for Payment Card Security

addressed to

The Minister of the Economy, Finance 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*) was set up under the Everyday Security Act 2001-1062 of 15 November 2001[1]. The Observatory's tasks are meant to promote information sharing and consultation between all parties concerned by the smooth operation and security of card payment systems[2] (consumers, merchants, issuers and public authorities).

Persuant to the sixth indent of the aforementioned Article L. 141-4, the present document reports on the activities of the Observatory during the year 2006. It is addressed to the Minister of the Economy and Finance and transmitted to Parliament. It includes a study on the protection of payment card data during the card personalisation process in France (Part 1), a presentation of fraud statistics for 2006 (Part 2) and a technology watch summary (Part 3). This report also contains a study on cardholders' perception of payment card security based on a survey by the CSA polling institute (Part 4).

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

2 For the purposes of its work, the Observatory makes a distinction between "four-party cards" and "three-party cards". 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 | PROTECTION OF PAYMENT CARD DATA DURING THE CARD PERSONALISATION PROCESS

1|1 Introduction

As part of its responsibility for monitoring the security policies of card issuers and acquirers, the Observatory already conducted a survey of payment card data protection during the acquisition process. In 2006, it supplemented this survey with an analysis of the security measures implemented by card issuers and card manufacturers during the card "personalisation" process.

Card personalisation consists of taking the cards produced by the manufacturers, which are not useable at this point, and loading the appropriate information on them to enable cardholders to use them. The personalisation information includes the issuer's own authentication data and the cardholder data (name, card number, PIN, expiry date, etc.) The different steps in the personalisation process require major safeguards to ensure that the data loaded onto the card, such as the cardholder's personal data, cannot be stolen or modified by fraudsters.

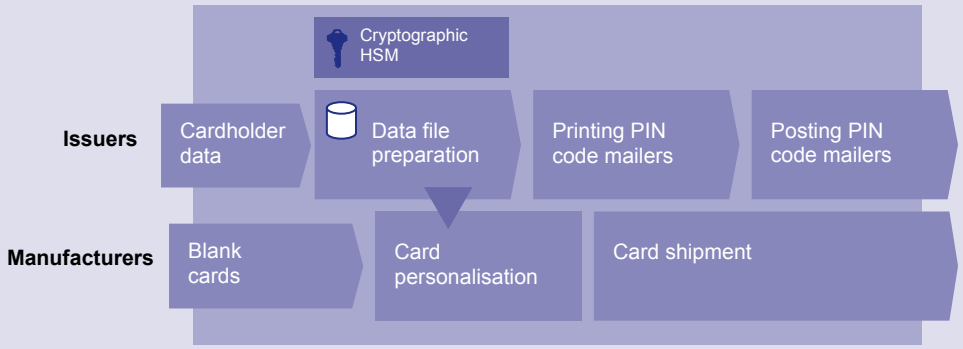
Prior to being loaded onto the cards, the critical data are received and stored in various types of equipment, such as data networks, computers, machine tools and different types of media. The Observatory therefore set itself the task of identifying not only the data that need protection, but also the various types of equipment that are used to load the data onto the cards, so as to arrive at a comprehensive assessment of the relevance and effectiveness of the security measures implemented throughout the card personalisation process.

For this purpose, the Observatory gathered useful information by means of a questionnaire sent to the issuers' representatives[3] and to manufacturers via the AFPC (*Association des Fabricants et Personnalisateurs de Cartes*), the card manufacturing and personalisation industry association.

The survey focused exclusively on the activities carried out in the card personalisation centres, and did not cover operations carried out by issuers (cardholder management) or inside the factories manufacturing the cards (see Box 1).

[3] Banque Accord, American Express, BMS, Cofinoga, Cedicam, Cetelem, CNCE, Diners, Finaref, Groupement des Cartes Bancaires « CB », La Banque Postale, Natixis

Box 1 - Scope of the survey



Scope of survey: **Personalisation centres**

1|2 Card personalisation

Issuers either carry out card personalisation using their own staff, or else they call on specialised providers called “card personalisation centres” or “personalisers”. Issuers hold these centres to strict requirements concerning the security of their operations. As a general rule, the security measures concern all of the data and equipment that are vulnerable to attack from fraudsters. The critical nature of card personalisation requires very strict oversight and control by issuers and the card personalisation centres.

Card personalisation centres

French card personalisation centres generally work for different sectors using cards with chips or magnetic stripes (telephony, retail distribution, banking, etc.) and for customers from different countries. These centres handle some 60 million cards on the French payment card market, of which 85% contain a chip. Half of these 60 million cards are used with a PIN code, which is usually sent to cardholders in a special letter called a “mailer”.

These centres personalise “four-party cards” and “three-party cards”. They are owned by banking groups, manufacturing groups or specialised independent providers.

Their business is a highly complex one because of the variety of quantities of cards to personalise, ranging from one to several hundred thousand cards, the manufacturing processes involved and the security requirements imposed by the critical nature of the operations. Consequently, it requires excellent organisation.

Box 2 – The different steps in card personalisation

There are several steps in the card personalisation process:

1. **Reception, verification and storage of blank cards**

   In most cases, the cards are not manufactured on the same site as the personalisation centre. The cards arriving at the centre are called “blanks”. A blank card bears the issuer’s logo and the chip used for payment applications, if the card contains such a chip.

2. **Reception of the cardholder data from the issuers and preparation of the personalisation data file**

   After receiving the cardholder data, the centre carries out different data processing operations in preparation for personalisation. The issuer’s specific secret codes used to authenticate the card are generated in cryptographic hardware security modules (HSM) using the issuer’s “master keys”. The cardholder data and the issuer data are gathered in a data file. One file is compiled for each type of card in order to simplify the handling of the blank cards by the operators. The loading of data onto the cards can then start.

3. **Processing by card personalisation machine**

   Personalisation may consist of different operations, depending on the type of card: encoding data onto the chip and/or magnetic stripe, embossing the cardholder’s name and the card number and engraving the specific code for card-not-present transactions (“CVx2”). Most programmable machines can carry out all of these operations at once.

4. **Packaging and mailing**

   This final step is usually carried out by hand. Employees make a visual compliance check and prepare the mailing envelop, inserting accompanying documents as required. The envelopes may also be prepared automatically. The cards are then ready to be shipped. They can either be sent directly to the individual cardholders, or sent to the issuer’s branches or distribution centres, which then make them available to cardholders.

5. **Mailing PIN codes**

   For payment cards using a PIN code, the card personalisation centre (or the issuer in some cases), generates the PIN code, prints it onto a secure mailer and posts it to the cardholder.

Data used and produced during card personalisation

The data sent by the issuer include cardholder identification data (name, mailing address) and card identification data (number, type), as well as data about the use of the card (cash withdrawals and/or payments, systematic authorisation, payment and withdrawal limits, etc.) In some cases, the issuer may also choose the PIN code for the card, but this code is usually generated by the card personalisation centre.

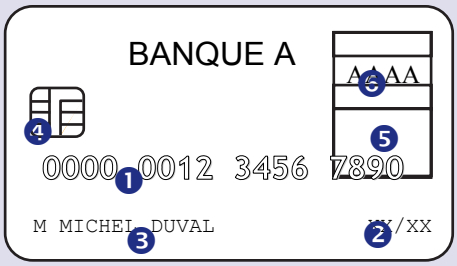
These data are usually linked to administrative data relating to the distribution method for the card, shipping addresses, packaging specifications, etc.

The card personalisation centre supplements the data from the issuer with:

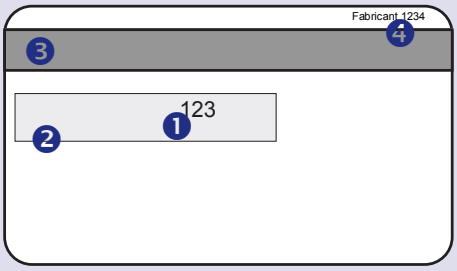
– Secret data (PIN codes, keys and cryptograms) that are generated from the data sent by the issuers for each production run and the secret keys that are specific to each issuer and transmitted at an earlier stage. To protect these data from being stolen or copied in the card personalisation centre, the issuer's secret keys are stored in a cryptographic hardware security module (HSM);

– Administrative data about production (blank card lot number, tracking data, etc.)

Box 3 – Typical four-party card features



1. Card number. The numbers are "embossed", which means they are raised above the card surface.
2. Expiry date
3. Name of cardholder
4. Chip
5. Hologram (location may vary)
6. Network name (location may vary)



1. CVx2 code used for card-not-present payments. This code is generated and engraved during the personalisation phase
2. Signature panel, printed with designs that are specific to each card network
3. The magnetic stripe is made up of 3 ISO tracks (1, 2 and 3), which are encoded during the card personalisation process
4. Reference number of the manufacturer that made the plastic card and inserted the chip

1|3 Security of the card personalisation process

The information and products used in the different steps of the card personalisation process are sensitive elements that could be stolen or copied by fraudsters.

According to the specialists surveyed, the main security measures should be aimed at protecting the data used to personalise cards at every step in the process: storage, production and shipping. The specialists also think that steps should be taken to protect blank or personalised cards, and the associated mailers, from being stolen during production or shipping.

Issuers require card personalisation centres to apply strict security policies in the following areas.

Selection and approval of card personalisation centres

Card networks and issuers have very strict security requirements for card personalisation centres. The "CB" Bank Card Consortium, as well as Visa and MasterCard, impose very strict requirements on card personalisation centres. These requirements must be met to earn approval. The requirements include a set of physical and logical security specifications, as well as organisational requirements that are monitored periodically by independent assessors

appointed by the card networks and credit institutions. “Three-party card” issuers that do not personalise their own cards generally choose card personalisation centres that have already been approved by the "CB" Bank Card Consortium, Visa or MasterCard.

Credit institutions are also required to submit a report to the supervisory authorities each year on how they and their providers manage the risks incurred in their main activities.

Card personalisation centres

Card personalisation centres are required to have a series of security systems to protect critical goods during their handling and processing. The physical security of the centres relies on physical access control (turnstiles, etc.), permanent and comprehensive surveillance of the premises (video surveillance, security guards) and vaults for storing cards. Logical access to information systems must be controlled and restricted to authorised personnel. The cryptographic hardware security modules that issuers provide to the centres contain the root cryptographic keys and these are kept in special high-security areas.

These physical and logical security measures seem to be connected to a set of organisational best practices. These usually include appointing a security manager, who is independent from the production unit to verify compliance with the procedures. In the same vein, the different functions of the centre are physically separated. For example, the PIN mailers are printed in a separate area and by different staff from those who personalise cards. The different categories of employees have access only to the areas and information that are strictly necessary for their jobs. A double count of the items used or produced is organised at every step in the personalisation process. In most card personalisation centres, a computerised production tracking system can be used to consolidate and audit all of the events related to a production lot of cards at any time. These systems can also be used to ensure proper synchronisation of the personalisation operations (combining the cardholder data with the card issuer data).

Data and files

Personalisation requires the use of highly sensitive data and files. The card personalisation centres implement the following practices to protect these data and files:

- Using dedicated computer platforms for secure data transfers between the issuer and the card personalisation centre;
- Encrypting and sealing data files for transport;
- Issuing a logical receipt to validate transfers and reception;
- Encrypting data files during the card personalisation phase and for archiving in historical data files, if appropriate;
- Logging and auditing of all events by the security staff, especially access to critical data files.

Cryptographic hardware security modules and keys

Cryptographic hardware security modules containing the issuer’s keys needed to generate the personalisation data are kept under special surveillance, especially during maintenance operations. The cryptographic keys must be loaded into the hardware security modules following very strict procedures under the supervision of persons who are independent of the card personalisation centre. The hardware security modules are equipped with systems to protect them from logical attacks or physical tampering.

Cards

The security requirements call for highly protected transportation of blank cards between industrial sites. As soon as they arrive, the cards are counted and stored in vaults. Access to the vaults is restricted to authorised personnel only. The cards to be personalised are supplied to the card personalisation staff as needed. Rejects and supplies that could reveal card data, such as ink ribbons, are counted and destroyed. Each production lot of cards is fully accounted for at each stage of the personalisation process so that the cards produced or rejected can all be traced. Rejected cards are systematically destroyed.

Shipping personalised cards

Personalised cards are either posted directly to cardholders, by registered mail in most cases, or sent in lots to the issuers' distribution centres. Returned mail (invalid address) is normally given special treatment to prevent possible theft.

The mailer used for the PIN code cannot be read by holding it up to the light and it cannot be resealed once it has been opened. The mailer is sent in such a way as to prevent a fraudster from coming into possession of both the card and the PIN code.

In addition, many issuers block the card number when it is generated and then activate the card when it is first used by the cardholder (in an ATM for example), or by means of a remote activation procedure, over the telephone, for example.

1|4 Conclusion

Card personalisation is an activity in which security is critical. It is the production step where the cards themselves and sensitive data, including those identifying and authenticating the card and the cardholder, come together.

The risk of theft or copying of these various elements, which are present in huge quantities at this step in the manufacture of the cards, calls for stiff security requirements with regard to physical and logical protection.

The answers to the survey that the Observatory conducted show that card issuers and card systems hold their usual providers to strict requirements. They approve providers on the basis of these requirements and periodically verify that security measures are properly implemented. The professional reputation of France's card personalisation centres testifies to the precautions taken by all of them. They are constantly innovating to back up the issuers' security requirements with best practices, as needed.

The card issuers and the representatives of the card personalisation centres surveyed did not report any incidents affecting the security of their card personalisation operations.

2 | FRAUD STATISTICS FOR 2006

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[4]. A summary of the statistics for 2006 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 C to this report presents a series of detailed fraud indicators.

Box 4 - Fraud statistics - respondents

In order to ensure the quality and representativeness of its fraud statistics, the Observatory relies on a diversified sample of respondents encompassing the issuers and merchants that are most representative of four-party card payment systems and three-party card payment systems. In 2006, a new issuer, Franfinance, was added to the sample.

Issuers provided the Observatory with data on:

– EUR 346.4 billion in transactions in France and in other countries made with 53.6 million four-party cards issued in France, including just under a million electronic purses,

– EUR 26.1 billion in transactions primarily in France with 25 million three-party cards[5],

– EUR 22.58 billion in transactions in France with foreign three-party and four-party cards.

Card issuers

Data were gathered from:

– Nine three-party card issuers: American Express, Banque Accord, Cetelem, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco;

– The 150 members of the "CB" Bank Card Consortium. The data were collected through the Consortium, and international data were obtained from Europay France and the Carte Bleue Group;

– Issuers of the electronic purse Moneo, with the data gathered through BMS (Billettique Monétique Services).

Merchants

The data collected came from six merchants accepting payment cards: Carrefour, the Casino group, Décathlon, France Loisirs, Monoprix, and the French railways (SNCF). In 2006, the data collected also included statistics gathered by the e-commerce and distance selling federation (FEVAD) from a representative sample of 29 distance selling firms.

---

4 See 2003 Report, Part 3.

5 The decline in the number of such cards between 2005 and 2006 (27.2 million three-party cards were in circulation at the end of 2005) stems from the implementation of Act 2005-67 of 28 January 2005 *to enhance consumer confidence and protection*, called the "Chatel Act". This legislation requires automatic termination of any credit contracts that have not been used for three years in a row. Some three-party card issuers had to cancel the cards associated with the contracts covered by the new legislation.

2|1 Overview

Total fraudulent payments and withdrawals recorded by the French systems came to an estimated EUR 252.6 million in 2006, as opposed to EUR 235.9 million in 2005. After declining between 2003 and 2005 (see Table 1), fraud posted a small increase of 6.6%. The average amount of a fraudulent transaction was up slightly to EUR 117, as opposed to EUR 111 in 2005.

However, the sustained growth in the number and value of card transactions (see Annex C) means that the increase in the amount of fraud has had no impact on the overall fraud rate, which has remained stable. It stood at 0.064% in 2005 and in 2006, as opposed to 0.070% in 2004.

The amount of issuer fraud, which is the total of fraudulent payments and withdrawals made in France and in other countries with cards issued in France, came to EUR 186.1 million in 2006. This is an increase from the figure of EUR 161.9 million for 2005. However, as a percentage of the transaction amount, the issuer fraud rate for 2006 stood at 0.050%, which is slightly higher than the 0.046% rate for 2005, but equivalent to the figure of 0.049% for 2004.

The amount of acquirer fraud, which is the total of fraudulent payments and withdrawals made in France with all French and foreign cards, came to EUR 176.2 million in 2006, versus EUR 171.8 million in 2005. As a percentage of the transaction amount, the acquirer fraud rate stood at 0.047%, down slightly from 0.048% in 2005.

Annex C to this report contains detailed tables on the numbers and amounts of transactions and the numbers and amounts of frauds by card type, geographical area, transaction type and fraud type.

2|2 Breakdown of fraud by card type

Fraud amounts, EUR millions
(Fraud rate)

	2002	2003	2004	2005	2006
Four-party cards	232.1 (0.082%)	259.2 (0.086%)	224.1 (0.069%)	218.8 (0.064%)	**237.0 (0.065%)**
Three-party cards	13.1 (0.078%)	14.4 (0.082%)	17.5 (0.082%)	17.1 (0.067%)	**15.6 (0.052%)**
Total	245.2 (0.082%)	273.6 (0.086%)	241.6 (0.070%)	235.9 (0.064%)	**252.6 (0.064%)**

Source: Observatory for Payment Card Security

Table 1 **– Fraud amounts and rates**

The total amount of fraud involving four-party cards was up slightly from EUR 218.8 million in 2005 to EUR 237 million in 2006. As a percentage of the transaction amount, this works out to a fraud rate of 0.065%, which is not significantly higher than the rate of 0.064% in 2005.

The issuer and acquirer fraud rates for this type of card stood at 0.050% and 0.047% respectively in 2006, compared to 0.046% and 0.048% in 2005. The average fraudulent transaction amount was EUR 112, as opposed to EUR 110 in 2005.

The total amount of fraud involving three-party cards stood at EUR 15.6 million in 2006, which works out to a fraud rate of 0.052%. This rate was substantially lower than the rate of 0.067% recorded in 2005. The issuer and acquirer fraud rates for this type of card stood at 0.045% and 0.046% respectively in 2006, compared to 0.049% and 0.061% in 2005. The average fraudulent transaction amount stood at EUR 430 in 2006[6].

2|3 Geographical breakdown of fraud

	Fraud amounts, EUR millions **(Fraud rate)**				
	2002	**2003**	**2004**	**2005**	**2006**
Domestic transactions	**89.5 (0.033%)**	**88.3 (0.031%)**	**103.9 (0.033%)**	**97.8 (0.029%)**	**109.6 (0.031%)**
International transactions	**155.7 (0.531%)**	**185.3 (0.648%)**	**137.7 (0.417%)**	**138.1 (0.408%)**	**143.0 (0.362%)**
(o/w French issuer / foreign acquirer)	51.9 (0.558%)	79.3 (0.690%)	55.2 (0.463%)	64.1 (0.458%)	76.4 (0.453%)
(o/w foreign issuer / French acquirer)	103.8 (0.519%)	106 (0.620%)	82.5 (0.391%)	74.1 (0.373%)	66.5 (0.295%)
Total	**245.2 (0.082%)**	**273.7 (0.086%)**	**241.6 (0.070%)**	**235.9 (0.064%)**	**252.6 (0.064%)**

Source: Observatory for Payment Card Security

Table 2 – **Geographical breakdown of fraud**

The geographical breakdown of fraud still shows a discrepancy between domestic and international transactions. International transactions account for 60% of the fraud, even though they make up only about 10% of the value of card payments handled by the French systems.

As domestic transaction amounts showed sustained growth of 6.29%, the fraud rate of such transactions was up only slightly, rising from 0.029% in 2005 to 0.031% in 2006, which is still a very low level.

The amount of fraud involving international transactions was up in 2006, but the fraud rate was down. This general trend reflects two developments:

– On the one hand, the amount of fraud involving foreign cards in France fell from EUR 74.1 million in 2005 to EUR 66.5 million in 2006, while the associated fraud rate fell from 0.373% in 2005 to 0.295% in 2006. This improvement was probably due to the rapid migration of French acquiring systems to EMV, which provides more secure handling of payments made with foreign cards;

– On the other hand, the amount of fraud involving French cards in other countries increased from EUR 64.1 million in 2005 to EUR 76.4 million in 2006, while the associated fraud rate showed a slight decline from 0.458% in 2005 to 0.453% in 2006.

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

[6] The substantial increase from the figures for the previous year (EUR 188 in 2005) stems from the improvement in the statistical tools of several three-party card issuers.

sale or at petrol pumps, ticket machines, etc. from card-not-present payments online, by post, by telephone, by fax, etc., and withdrawals.

With regard to domestic payments (see Table 3) the figures show that:

– Face-to-face transactions, unattended payment terminal sales and automated teller machine (ATM) withdrawals accounted for nearly 70% of the fraudulent payments that the Observatory recorded in 2006. The trend for this percentage shows a decrease: From 76% in 2005 and 83% in 2004;

– The fraud rate for face-to-face payments and unattended payment terminal sales is much lower than the fraud rate for card-not-present payments. The fraud rate for such payments 0.024% in 2006, as opposed to a rate of 0.199% for card-not-present payments. This trend for this rate is also downwards: it stood at 0.025% in 2005 and at 0.029% in 2004;

– Fraud involving card-not-present payments came to EUR 33.2 million in 2006, which is a substantial increase from the figure of EUR 23.6 million recorded in 2005. However, the strong growth in the number and value of such payments, with a 38.9% increase in the amount between 2005 and 2006, means that the increase in the fraud rate involving such payments was very slight, rising from 0.196% in 2005 to 0.199% in 2006.

– After decreasing between 2004 and 2005, fraud involving cash withdrawals was up slightly in 2006 to EUR 17.4 million, as opposed to EUR 15.0 million in 2005.

	Fraud amounts*, EUR millions **(Fraud rates)**		
Domestic transactions	**2004**	**2005**	**2006**
Payments	**81.2 (0.036%)**	**82.8 (0.033%)**	**92.3 (0.035%)**
- o/w face-to-face and unattended payment terminal payments	63.5 (0.029%)	59.2 (0.025%)	59.1 (0.024%)
- o/w card-not-present payments	17.7 (0.177%)	23.6 (0.196%)	33.2 (0.199%)
- o/w by post / telephone	na	na	19.8 (0.194%)
- o/w online	na	na	13.4 (0.208%)
Withdrawals	**22.7 (0.027%)**	**15.0 (0.017%)**	**17.4 (0.019%)**
Total	**103.9 (0.033%)**	**97.8 (0.029%)**	**109.6 (0.031%)**

** All types of cards* *Source: Observatory for Payment Card Security*

Table 3 – **Breakdown of domestic payment fraud by transaction type**

The Observatory's work to improve its statistical information system means that it now has fraud rates for the different types of card-not-present payments made with any type of card. For example, the figures show that the fraud rate for card-not-present online payments is slightly higher than the fraud rates for other card-not-present payment channels, such as the mail or the telephone. Furthermore, this is confirmed by the FEVAD estimates[7], which show that the fraud rate does seem to vary from sector to sector and is estimated to be higher in the sale of services than it is in the sale of products.

[7] Based on a survey of a sample of e-commerce businesses and websites belonging to FEVAD that are representative of the main e-commerce and distance selling sectors.

However, the fraud rate for card-not-present payments, as measured by the FEVAD's sample, is lower than that found by the Observatory[8]. The discrepancy suggests that the fraud rate is lower in the case of e-commerce specialists, which may stem from the fact that these specialists have implemented specific security measures for this type of transaction.

The Observatory would like to stress the importance of compliance with the security measures recommended by issuers, especially systematic use of the CVx2 code for card-not-present payments and verification of the buyers' identity by merchants[9].

In the case of international transactions (see Table 4), the Observatory does not have a detailed breakdown of fraud by transaction type, except for 2006, and then only for French cards used to make payments in other countries. The figures show, as they do in the case of domestic transactions, that:

– The fraud rate of 0.288% for face-to-face payments and unattended payment terminal sales is much lower than the fraud rate of 0.840% for card-not-present payments;

– The fraud rate of 0.898% for card-not-present payments is higher for payments made online than the fraud rate of 0.684% for other types of card-not-present payments.

	Fraud amounts EUR millions **(Fraud rates)**
French issuer / foreign acquirer	**2006**
Payments	**54.0** **(0.421%)**
- o/w face-to-face and unattended payment terminal payments	28.1 (0.288%)
- o/w card-not-present payments	26.0 (0.840%)
- o/w by post / telephone	5.7 (0.684%)
- o/w online	20.3 (0.898%)
Withdrawals	**22.4** **(0.555%)**
Total	**76.4** **(0.453%)**
Foreign issuer / French acquirer	**2006**
Payments	**61.5** **(0.344%)**
Withdrawals	**5.0** **(0.107%)**
Total	**66.5** **(0.295%)**

Source: Observatory for Payment Card Security

Table 4 – **Breakdown of international payment fraud by transaction type**

8 FEVAD estimates fraud involving four-party cards used for domestic card-not-present payments at 0.130%.

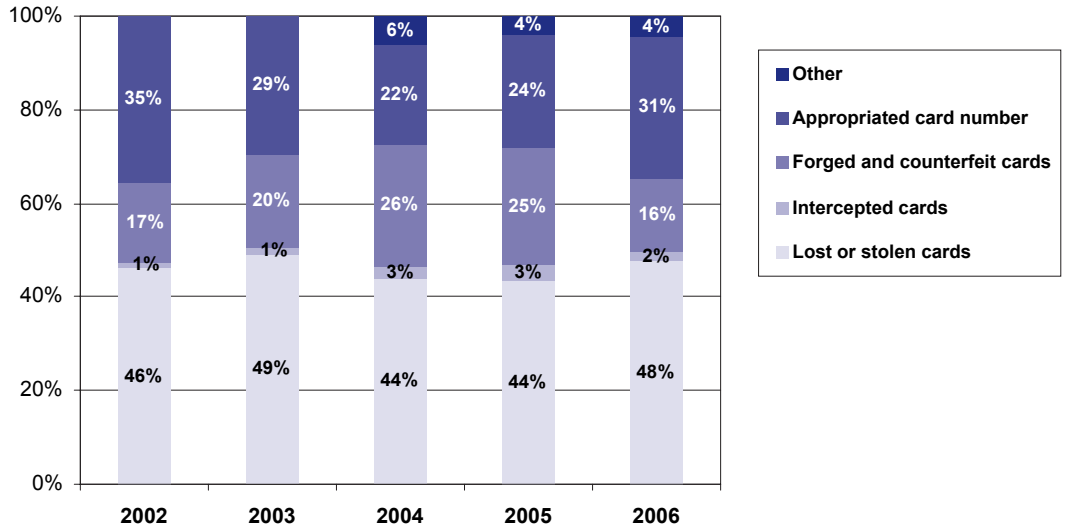
9 See the first chapter of the Observatory's 2004 annual report for an overview of security policies in this area.

2|5 Breakdown by fraud type

The Observatory breaks fraud down 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 that use programs to generate random card numbers and then uses the numbers for card-not-present transactions.
- "Other" fraud, which covers, particularly for three-party cards, the fraud resulting from the fraudulent opening of accounts with a false identity.

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



Source: Observatory for Payment Card Security

Table 5 - **Breakdown by fraud type (domestic transactions, fraud amounts)**

By far, the most common type of fraud involves lost or stolen cards. Such fraud increased in 2006 and accounted for nearly 48% of fraudulent domestic payments in 2006. Counterfeit cards accounted for 16% of fraudulent domestic payments in 2006, which represented a substantial decrease. On the other hand, fraud involving the use of appropriated card numbers for card-not-present payments accounted for slightly more than 31% of fraudulent payments, showing an increase in 2005 and in 2006, after declining for three years in a row. "Other" fraud was stable. This category of fraud is often used by three-party card systems 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	
2006	**Amounts** (EUR millions)	**Shares**	**Amounts** (EUR millions)	**Shares**	**Amounts** (EUR millions)	**Shares**
Lost or stolen cards	52.5	47.9%	50.0	49.8%	2.5	27.5%
Intercepted cards	1.8	1.6%	0.7	0.7%	1.1	11.7%
Forged or counterfeit cards	17.4	15.9%	17.1	17.0%	0.3	3.1%
Appropriated numbers	33.5	30.5%	32.7	32.5%	0.8	8.3%
Other	4.4	4.1%	-	-	4.4	49.4%
Total	**109.6**	**100%**	**100.5**	**100%**	**9.1**	**100%**

Source: Observatory for Payment Card Security

Table 6 - **Breakdown of domestic payment fraud by fraud type and by type of card**

Box 5 – Highlights of the year for law enforcement agencies

In 2006, law enforcement agencies noted a general increase in the number of payment card fraud cases.

In 53,755 cases of counterfeiting cards, 3,496 individuals were charged and 1,642 suspects were detained.

Attacks on ATMs were up sharply, with 515 such attacks registered in 2006, as opposed to 200 in 2005 and 80 in 2004. Many investigations of such attacks were carried out throughout France in 2006. Police work in this area included:

- The arrest of three ring leaders of a gang pirating ATMs. These arrests helped put a stop to the activities of three criminals with police records for organised crime who specialised in such attacks and worked in conjunction with some Romanians based in the Netherlands;
- An investigation of the hacking of about 20 payment terminals belonging to restaurant chains, which led to more than EUR 2 million in losses and compromised some 3,000 payment cards. The investigation led to the arrests of five individuals in Spain and three others in France.

In 2006, cooperation between French law enforcement agencies and their opposite numbers in Eastern Europe was reinforced to respond to the cross-border dimension of this type of crime and the origin of the criminal gangs involved. This cooperation will be continued in the coming years.

3 | TECHNOLOGY WATCH

As part of its technology watch, the Observatory conducted two studies in 2006. The first dealt with the impact of the use of open networks in the payment card environment and the second dealt with unattended payment terminals and automated teller machines. The Observatory examined the security issues raised by each of these topics and came up with a set of recommendations. The Observatory also updated the information gathered in previous years on the migration to the EMV standard for cards and terminals in different European countries.

3|1 The use of open networks in the payment card environment

Up until recently, the risks associated with the networks used for payment card transactions were kept mostly under control. This was because the networks were administered by the legacy operator and the technology in use was more familiar to hardware manufacturers than to potential hackers. Furthermore, the connections were only made as needed to download information or transmit authorisation requests. The use of technologies like X.25[10] ensured that a barrier was available, even in the event of an accidental connection to other networks, such as the Internet, without any need for filters[11].

New telecommunication technologies, commonly called “open networks”, have brought about sweeping changes to the threat level facing future payment systems. The widespread use of the IP (Internet Protocol) standard communication protocol that the Internet is built on, and the telecoms operators’ new range of services are leading inevitably to the use of common networks carrying multiple flows of data and voice. The emergence of such technologies as ADSL[12] and GPRS[13] means that connecting card payment acceptance equipment provides such benefits as always-on high-speed connections, which make new functions possible (more frequent uploading of updates, faster authorisation requests, etc.), a reasonable flat fee, and the ability to use the same line for several connections.

The widespread use of open networks facilitates interconnection and gives rise to threats that are not new, but on a different scale as a result of the broad dissemination of the most recent telecommunications technology. Where each payment terminal or network equipment manufacturer once developed its own X.25 communication system, IP development is based primarily on external software tools that are easy to obtain. This means that the skill levels are now reversed: familiarity with communication protocols is no longer the preserve of payment terminal providers. In addition, networks are now much more accessible as wi-fi becomes widespread, providing scattered access points in many different countries. The security levels vary, depending entirely on the network operator's own choices, whereas the legacy operator

---

10 X.25 is a communication protocol that the CCITT standardised in 1976. It is used by Transpac in France.

11 Software or hardware components that enforce the network security policy, which defines which types of communications are allowed or prohibited.

12 Asymmetric Digital Subscriber Line. Development of the use of ordinary telephone lines to establish an always-on broadband Internet connection that does not disrupt the use of the conventional phone service.

13 *General Packet Radio Service* or GPRS is a mobile telephone standard derived from GSM that can be used for faster data transmission. It is often referred to as 2.5G. The G stands for generation and the 2.5 means that the technology is halfway between GSM (2nd generation) and UMTS (3rd generation).

had provided a uniform level of security. The always-on network connection also means that the time of exposure to threats has increased.

What follows are a description of the various players concerned in the payment card system, a risk analysis of the use of open networks, security measures implemented, and the Observatory's recommendations.

Players and networks involved

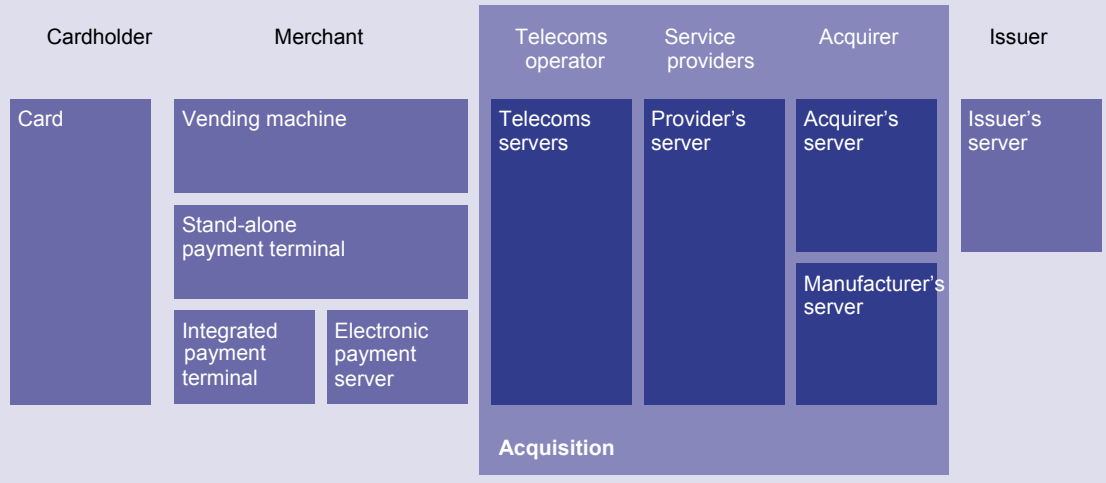
A payment card system handles different flows of information:

– Operational flows, associated with transaction management, such as:

  - The transaction stage, which includes the initiation, validation and transmission of the payment order. This stage involves the cardholder and his card, the merchant and its acceptance system. Validation of a card payment requires the implementation of several functions, such as cardholder authentication, authentication of the card and the transaction authorisation, which may be accomplished off-line (without consulting the card issuer) or on-line. Completed payments are stored in the merchant's accepting terminal. They are then transmitted to the acquiring bank (remote data collection).
  - The settlement stage is where the payment is completed by the exchange and settlement of payment orders between the cardholder's and the merchant's financial intermediaries.

– Maintenance data flows carried by acceptance systems, such as remote parameterisation and uploading of updates, which also involve the manufacturers of the card accepting equipment.

Box 6 – Players and networks



Exchanges between acquirers and issuers are handled by tightly controlled bank networks. The network for "CB" bank cards is called e-RSB (Réseau de Services aux Banques). The network is based on IP technology, but it is totally private and there is no interconnection with the Internet.

On the other hand, more and more telecoms operators are offering links between merchants and acquiring banks using ADSL and GPRS. Merchants' own links between cash registers,

concentrators, and base terminals are could migrate to more vulnerable technologies, such as wi-fi[14] wireless connections, Bluetooth[15], DECT[16], and local IP networks.

Impact of the use of open networks

The use of open networks may lead to increased risks in terms of down-time, data confidentiality, intrusion and hacking.

The use of secure protocols is critical for controlling such risks and protecting the data flows between the various players in the payment system. Yet logical integrity of equipment is also critical for preventing intrusions.

Security of data flows

The links between the various pieces of equipment in the payment card system handle sensitive data flows that need to be protected against intrusion and manipulation. Therefore, these data should be protected by systems that ensure confidentiality, integrity and authentication.

The electronic payment exchange protocol does not cover all of these security services, which means that they must rely on the systems provided by the communication protocols associated with the new networks. Communications between the acceptance system and the acquisition server of the acquirer or the acquirer's service provider need to be authenticated and their integrity and confidentiality need to be protected by robust encryption algorithms. The same holds true for the communication networks between an acceptance system concentrator and the various points of sale or cash registers.

As new technology makes the communications networks used more accessible, supervision of the authorised flows handled by the network also becomes absolutely necessary. This calls for systems that block any communication other than the rightful communications necessary for the smooth operation of the system. Such systems primarily consist of filtering based on firewalls or filtering routers, which supervise data flows at a central point. A supplementary technique consists of compartmentalisation. This means designing the network so that it has separate security zones, with supervision of data flows between zones, which limit a hacker's chances even if he has gained access to one of the zones.

The use of these techniques also provides protection against denial-of-service attacks. This means that the only attacks possible must be launched from identifiable equipment, which can then easily be disabled.

---

14 Wi-fi is a wireless network technology that can be used to operate as an internal network or to provide broadband Internet access. It is based on the IEEE 802.11 standard (ISO/CEI 8802-11).

15 Bluetooth is a short-range radio technology aimed at simplifying connections between electronic machines. It was designed to replace the wires between computers and peripheral equipment, such as printers and scanners.

16 Digital Enhanced Cordless Telephone.

Box 7 – Secure protocols

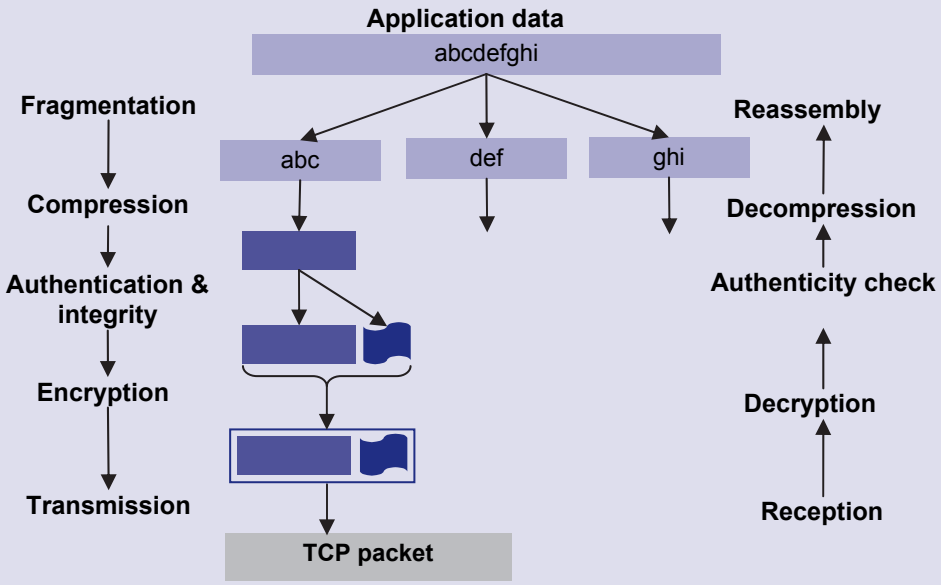
A secure protocol provides a set of data protection services: confidentiality, integrity and authentication.

Confidentiality is a security service that ensures that only authorised persons shall be able to see a set of data. The device that usually provides this service is data encryption using a cryptographic algorithm.

Integrity is a security service that ensures that only authorised persons shall be able to modify a set of data. In the context of communications, this service makes it possible to detect any alteration of data during transmission.

Authentication is a security service that ensures that the data received were actually transmitted by the expected transmitter.

The following example shows how the SSL (Secure Socket Layer) protocol protects data generated by applications, before they are transmitted using the TCP communication protocol:



Equipment security

Attacks may concern flows of data, but they can also involve fraudulent attempts to gain access to one of the pieces of equipment making up the payment system. Such an attack could enable a fraudster to obtain sensitive data, but it could also be an attempt to manipulate the system for gain. Attackers may also try to make the system unavailable.

Logical attacks via the telecoms network are increasingly an issue to be dealt with, as technology changes.

Payment terminals and servers should be specified, designed and supervised to withstand, detect or counter such attacks. This requires an enhancement of operating system security for hardware, supervision of access and authentication of players, as well as monitoring of work done on the hardware, especially with regard to maintenance operations. In the case of acceptance systems, this specifically means a strengthening of the supervision systems for remote parameterisation operations and downloading.

Box 8 – Enhancing system security

Enhancing the security of a system means aiming to optimise security within the context of its use. Manufacturers generally provide hardware with a set of functions and a default configuration that is supposed to suit the majority of users, but which may have shortcomings with regard to security.

Enhancing the security of the system requires the elimination or deactivation of unused software components and functions, which could make the hackers' task easier or result in security problems.

The default configuration is usually very basic in terms of security. It also needs to be adapted so that it only allows what is strictly necessary. Any default passwords must also be changed.

In order to enhance hardware security further, it is often possible to activate supplementary security systems or supervision, or to provide tools for closer surveillance of the system.

In addition, system security enhancement often involves updates with the latest security patches, followed by verification using supervision tools.

Review of security measures

Card payment system players must implement measures to circumscribe the risks stemming from the use of open networks.

In 2004, for example, the "CB" Bank Card Consortium set out its "*Security requirements for communications with payment acceptance systems*". These requirements deal with traceability of maintenance operations, the integrity of electronic payment systems, protection of internal and external links to merchants, restriction of communications, hardening of operating systems and authentication of servers. The requirements are designed to ensure the security of electronic payment data flows and hardware in terms of integrity, confidentiality and availability when using open networks. The requirements have been binding on the various players in the "CB" system since 2005, including acquirers, merchants, telecoms operators and equipment manufacturers.

In the case of three-party cards, measures to ensure the security of transactions are more often a matter for each issuer to decide. Three-party card systems are closed systems at present, which means that they are under the issuers' control and less concerned by the use of open networks for the time being. However, even though three-party card systems use their own applications and networks, they still share some hardware with the "CB" system, including merchants' payment terminals, since most merchants use one terminal to accept payments from different cards. This means that three-party card issuers could benefit from the security measures developed by manufacturers for the "CB" system.

The measures currently implemented by French issuers are the result of their own security analysis and not the result of European or international initiatives. The only existing measures, which are the "Payment Card Industry (PCI) Data Security Standard" of the PCI Security Standards Council, deal with only some of the problems. These standards require encryption of transmissions over open networks, but they concern only protection of the card data. The Common Approval Scheme (CAS) group has launched a European initiative to develop security requirements for the protection of payment terminals and the associated transmissions over all types of networks, including open networks. Once the European Payments Council (EPC) imposes these requirements on European payment card systems, the level of protection for data transmission will be equivalent to that now available in France.

Recommendations

The Observatory urges all French players concerned to comply with the "*Security requirements for communications with payment acceptance systems*" defined by the "CB" Bank Card Consortium.

The application of these recent requirements should keep pace with the replacement of hardware, as the X.25 protocol is replaced by the IP protocol in the medium term. Compliance with security requirements is necessary to cope with the attacks that are made possible by the increasing use of open networks. This joint document would have the advantage of making the security measures for the system as a whole more uniform and providing effective protection for all of the players.

The impact of the use of open networks for card payment systems seems to be properly dealt with in France, but there are no standards in this regard at the European level. Yet, the introduction of the Single European Payments Area (SEPA) will mean that the networks extend beyond national borders. In this respect, the Observatory feels that common rules will be indispensable and that they should be at least as rigorous as the French requirements are. It would be desirable for the EPC's coordination efforts with regard to standards to incorporate security requirements, such as those formulated by the Common Approval Scheme group.

3|2 Security of unattended payment terminals and automated teller machines

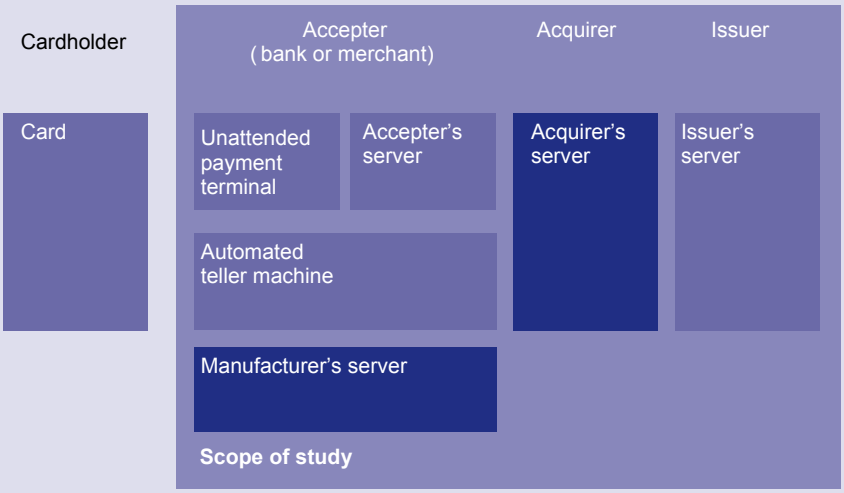
Scope of the survey

As part of its technology watch task, the Observatory studied the security of stand-alone payment terminals in 2005. In 2006, it continued its study of security for acceptance systems by reviewing the specific systems to protect unattended payment terminals (UPTs), such as card-operated petrol pumps, and automated teller machines (ATMs) used for cash withdrawals.

There are some 180,000 machines of both types in France today (see Table 7), and their security is an important issue. Their isolated locations can make them a favourite target for fraudsters seeking card data to help them make fraudulent transactions. Such machines usually accept four-party cards, as well as certain three-party cards.

The Observatory studied the most commonly used security measures and systems for such machines, including those for the transactions between this type of equipment and the electronic payment servers that they are linked to (see Box 9).

Box 9 – Scope of the study



After a brief description of the how the machines work, the risks that they are vulnerable to and the related security issues are discussed. This is followed by a presentation of the protection measures implemented and the outlook for changes in this area. In conclusion, the Observatory puts forward its recommendations based on its analysis.

How the machines work

The machines can be used by cardholders around the clock every day of the week and, with the exception of payphones, more and more are being installed in France. In addition to four-party cards that operate with a chip, the machines frequently accept three-party cards and foreign bankcards with a magnetic stripe that are not compliant with the EMV standard.

Automated teller machines (ATMs) accept four-party cards and are usually operated by banks. The "CB" Bank Card Consortium has defined the security requirements for such machines. For EMV compliant four-party cards, the transactions use the chip in the card, not the magnetic stripe. As of the middle of 2007, all ATMs in France accept EMV-compliant chip cards. These cards still have a magnetic stripe so that they will work in ATMs in other countries. The magnetic stripe on an EMV-compliant card is often still used to open the door to an ATM lobby that does not have direct access from the street. The ATM sends an authorisation request to the issuer of any card by transmitting the data read on the stripe and the PIN to the issuer as securely as possible. In countries that have not yet migrated to the EMV standard, ATMs treat EMV-compliant cards in the same way as cards with magnetic stripes.

Merchants install **unattended payment terminals (UPTs)** to meet very specific automated distribution needs (petrol, DVDs, transport tickets, drinks, etc.). Such vending machines accept four-party cards and many three-party cards. The configuration of UPTs varies greatly, depending on the types of products and services sold, the age of the machine and the characteristics of certain transactions (motorway tolls, for example). Machines that are compliant with the "CB" Bank Card Consortium standards handle the transaction in EMV mode, using the chip and offline verification of the PIN, and transmitting an authorisation request if necessary. If the UTP only uses the magnetic stripe, the PIN verification, which is transmitted to the acquirer's server in encrypted form, is usually conducted online at the same time as the authorisation request.

Security issues

The number of UPTs and ATMs in France has been increasing steadily. With the exception of payphones, where the number of card-operated models has decreased in recent years through declining use as a result of the popularity of mobile telephones, the number of UPTs has increased in all sectors. Overall, UPTs account for 12% of the payment terminals installed in France.

	Number of machines in **2000**	Number of machines in **2006**	**Change** %
Automated Teller Machines (ATM)	33,000	48,000	+45%
Card-operated petrol pumps	10,000	18,000	+80%
Transport ticket vending machines	4,000	8,000	+100%
Parking paystations	3,000	4,000	+33%
Goods and services (groceries, photos, etc.)	4,000	6,000	+50%
DVD rentals and sales, ski lift tickets, hotel rooms, etc.	7,000	8,000	+14%
Sub-total (excluding payphones)	**61,000**	**92,000**	**+51%**
Payphones	220,000	90,000	-59%
Total	**281,000**	**182,000**	**-35%**

Source: Observatory for Payment Card Security

Table 7 – **Changes in the installed base of card-operated machines**

Changing risks

According to the banking community, the number of cases of machines tampered with to skim card data would have doubled between 2005 and 2006 (500 machines, including 450 ATMs, representing 0.3% of the installed base). Law enforcement agencies have arrested fraudsters on several occasions and seized their equipment. These agencies highlight the increasing technical sophistication of the fraudulent systems.

The Observatory does not have any data available to assess the scale of transactions made using data skimmed from cards used in a UPT or an ATM. Nor does the Observatory have data about fraud perpetrated specifically on UPTs.

On the other hand, it does have data on the amount of fraud involving French cards, primarily four-party cards, being used for cash withdrawals:

– From French ATMs, which handle transactions using the chip in the card. This type of fraud almost exclusively involves the use of lost and stolen cards. In 2006, this type of fraud came to EUR 17.4 million, or 0.019% of withdrawals made in France using French cards;

– On ATMs in other countries, 80% of the fraud involves transactions made using the magnetic stripe on the card and primarily concerns counterfeit cards. In 2006, this type of

fraud came to EUR 22.4 million, or 0.556% of withdrawals made in other countries using French cards.

Some 80% of the fraud involving ATMs in other countries occurs in Europe, with Italy being the most likely place, accounting for EUR 10 million in fraud or 30% of total fraud involving ATMs in other countries. However, in view of liability shift measures, most of the losses incurred from this type of fraud are borne by Italian banks.

Some 40,000 French cards were used for fraudulent withdrawals from foreign ATMs in 2006. The average loss for the use of a fraudulent card to withdraw cash from ATMs is EUR 600, taken in three transactions.

Fraud targets

UPTs and ATMs are targeted by two types of attacks aimed at:

- Obtaining the card data that the lawful cardholder enters into the machine (skimming). These data can then be used to make counterfeit cards with magnetic stripes. Some systems even enable fraudsters to steal the card itself. Fraudsters also seek to obtain the corresponding PIN at the same time so that they can use the stolen card in a greater number of UPTs, ATMs and payment terminals;
- The use of counterfeit cards, stolen cards or tampering with UPTs to obtain the goods and services fraudulently.

Types of attacks

The main types of attacks involving UPTs and ATMs are aimed at:

- Stealing the card: A device is mounted on the card slot to block it. The lawful cardholder thinks that the machine has malfunctioned. After the cardholder leaves, the fraudster can remove the card. However, this method relies on the fraudster's being able to see the cardholder enter the PIN in order to make use of the stolen card.
- Obtaining the confidential data from the card, including the PIN: several devices have been seen for skimming the data from the magnetic stripe using a card skimmer mounted on the machine or else copying the card identification data and the PIN using devices mounted inside or on the front of the machine;
- Changing the software and parameters of the machine to take control of it or modify its operations. This type of attack is very rare and relies on malicious software. In one case in another country, the fraudster managed to use the administrator's code for a machine that had been set at the factory and that the machine owner had not changed. By this means the ATM was made to dispense larger amounts of cash than the amounts entered.

Cases of fraud seen

The protection of payments made using magnetic stripes is not as good as that of payments made using chips.

Stolen magnetic stripe and chip cards can be used with their PIN code to make payments and cash withdrawals in France and other countries until they are reported missing. Even if some of these fraudulent transactions can be made using the magnetic stripe or for card-not-present transactions, they do not stem from tampering with UPTs or ATMs. In France, the

cardholder is liable for the losses from this type of fraud until the card is reported missing, subject to a limit set by law.

Counterfeit cards, with the corresponding PIN can be used for magnetic-stripe-based transactions in the following specific cases:

– Fraudsters can use counterfeit French cards to make payments and cash withdrawals in countries where acceptance devices still use magnetic stripes and have not migrated to the EMV standard. However, such fraud is only possible until the card is reported missing, since this type of transaction usually involves an authorisation request to the French issuer. In all these cases, the losses are not borne by the cardholders;

– Counterfeit foreign cards, with or without a chip, can be used for payments in France in exceptional circumstances where certain types of card-operated UPTs only read the magnetic stripe. However, such fraud is limited by authorisation requirements, which are often as low as one euro, and by automatically checking the card against the list of lost and stolen cards uploaded to the machine. The ongoing migration to the EMV standard will restrict the opportunities for such fraud to foreign cards with no chips;

– Foreign cards without chips, which are issued in countries that have not yet migrated to the EMV standard, can be used to make cash withdrawals in France and other countries, provided that the fraudster also has the PIN. Transactions made with foreign cards require authorisation, which is requested over the international networks, and this means that fraudsters can only use these cards until they are reported missing. The resulting losses are usually borne by the foreign issuers.

The Primary Account Number (PAN) and the expiry date, which are recorded in the magnetic stripe, can also be used for card-not-present transactions. Such fraud is only possible before the card is reported missing and only if the merchant fails to ask for the CVx2 code engraved on the back of the card, which means that a fraudster would have to have had possession of the card. In France, most issuers of four-party and three-party cards require this code for card-not-present payments (see Box 2, page 12 in the 2005 report).

Existing protection measures

In light of the types of attacks, protection for UPTs and ATMs should be approached from three angles:

– Verifications carried out during and after the transactions;

– Protection against pirate devices mounted on or inside machines;

– Protection against devices mounted on communication lines or the use of spyware and malware.

Verifications carried out during and after the transactions

The protection measures are not exactly the same, depending on whether the transaction uses the stripe data or the EMV chip data. The deployment of EMV-compliant chip cards in Europe will greatly reduce the use of magnetic stripes and will reduce fraud involving data skimmed from the stripes.

Common measures to prevent fraud on UPTs and ATMs include authorisation requests, which may be systematic for certain types of operations, checking lists of stolen cards, and offline or online PIN verification. For greater effectiveness, some measures are frequently targeted to specific areas, depending on the type of machine to protect.

Analysis of transaction files and fraud after the fact makes it possible to identify compromised machines and stolen cards. This information can be used for investigations and for compiling statistics in order to identify risky transactions when authorisation requests are received (see "Fraud detection systems", page 36 in the Observatory's 2003 Annual Report).

Protection against skimmers mounted inside machines

Protection against spying devices mounted inside machines starts with restricting access to the inside of the machines. Manufacturers provide robust equipment with effective locking systems that are sometimes equipped with alarms. Access to the sales function (or dispensing of banknotes) and the payment function is often recorded and usually carried out separately. This makes it possible to restrict access to card readers to authorised operators only, thus limiting the opportunities for installing spying devices. A second level of protection is used for the payment function proper, with end-to-end encryption of the PIN from the keypad to the transaction processing system. The physical security of the keypad and the electronic controls prevents any possibility of obtaining the PIN and data entered.

Protection against skimmers mounted outside machines

The front of the machine is designed to provide protection against the installation of external spying devices. On some machines, the normal aspect of the machine is displayed on the screen so that users can identify any alterations. Other increasingly frequent protection measures include hoods to shield the PIN keypad and video surveillance of machines.

Since 2005, the "CB" Bank Card Consortium has imposed Anti-Fishing, Anti-Skimming security requirements (AFAS) for UPTs and ATMs. These requirements deal with maintenance procedures and protection of the machines and PIN codes. The requirements are now incorporated into the manufacturing process and manufacturers are making very sophisticated machines offering various types of protection. For several months now, compliance with these requirements is a prerequisite for obtaining the "CB" Bank Card Consortium’s certificate of approval for UPTs.

Protection of data transmissions

UPTs that accept "CB" cards are subject to the same rules as payment terminals. The previous section contains a detailed description of the principles applied to protect these transmissions. ATMs are connected to servers that provide real-time surveillance of their operations around the clock. All of the data transmitted are encrypted.

Protection against eavesdropping and malicious software

The increasingly widespread use of commercial operating systems, such as Windows and Linux, in the computers controlling UPTs and ATMs creates new threats from computer viruses and malicious software, such as Trojan horses. In many cases, manufacturers “harden” operating systems by limiting them to useful functions only and preventing the installation of unknown software. These systems are protected in accordance with the latest computer protection recommendations, including firewalls.

When software applications installed in UPTs and ATMs can be uploaded, it is important for uploads to be fully secure. For this reason, software applications are often signed by the manufacturer or the software publisher using a cryptographic device to prevent any software

that might not be authentic from being installed. Such uploads may also only be possible from each manufacturer's own server.

User information

These measures are backed up by information campaigns aimed at:

– Cardholders, information presented by banks on the ATMs themselves ("Do not allow others to see you enter your PIN", "Do not let strangers distract you"). This information is often backed up by consumer associations' information campaigns. This year, the Observatory has put forward some tips for secure use of payment cards (see Chapter 4);

– Operators of ATMs located in bank branches (organised by the French Banking Federation) and merchants operating UPTs (organised by merchants' associations), to detect any current or past anomalies on the front of the machines.

Outlook

Visa, MasterCard and JCB, under the joint label PCI, defined specific security requirements for UPTs called PCI-UPT. These requirements are similar to those in effect for payment terminals (see Box 3 page 14 in the Observatory's 2005 Annual Report). The requirements deal with the physical and logical protection of the electronic components in UPTs, including keypads, electronic controls and screens. The requirements are based on an analysis of risks incurred primarily by international systems that still use magnetic stripe cards, and which may seem pointlessly cumbersome for machines that use chip cards[17], as is the case in France.

Furthermore, some of the PCI-UPT security requirements restrict sales functions to protect the payment function. For example, screens can only be used for the payment function; and not to engage in a sales dialogue with the customer. In some cases, the use of three-party cards will be impossible, which will limit UPT sales considerably. This explains why merchants have opposed the implementation of the requirements until PCI has dealt with these problems. The "CB" Bank Card Consortium's requirements, which cover some of the risks dealt with by the PCI-UPT requirements, are designed to be applied pending adaptation of the PCI-UPT requirements to the European context.

In the meantime, the European Common Approval Scheme group has defined security requirements for cards, payment terminals, UPTs and ATMs that supplement those developed by the international networks. The group is studying the assessment methods for this equipment and is developing a security certification scheme based on mutual recognition of certificates issued in the various SEPA countries. This work has been recognised by the EPC, which is in charge of coordinating the various initiatives to develop European standards.

Recommendations

The Observatory notes that the high level of protection for the data recorded in the chip means that fraudsters' attempts to steal the data focus primarily on reading the magnetic stripe. Yet, many machines still read both magnetic strips and chips in order to accept international cards and three-party cards or, even if this is not the case, because of industrial standardisation.

[17] The PCI requirements do not apply to transactions using French three-party cards with magnetic strips made online in a very closed environment, as is the case with store cards used in the store itself.

Therefore, when UPTs do not need to accept cards with magnetic stripes, the Observatory recommends that manufacturers should design them without a magnetic stripe reader, which is often only included because of industrial standardisation.

The presence of a magnetic stripe reader needlessly creates a risk of data being skimmed from the stripe when chip cards are used in such machines. The decision to eliminate the magnetic stripe reader must obviously be made in close consultation with the issuers of three-party cards so as not to decrease the services available to their cardholders.

In addition, when machines have to be able to read both the magnetic stripe and the chip, the chip reader and magnetic stripe reader should be separated, as is already the case in payment terminals, in order to counter the risk of skimming the stripe during a chip-based transaction. This type of measure is especially worthwhile for machines incurring high risks because of their purpose or their isolation. However, the Observatory notes that this would entail significant changes in the configuration of the machines, with consequences in terms of replacement costs and user-friendliness. Therefore, the Observatory thinks it would be helpful for the machine operators to conduct feasibility studies and ensure that implementing this measure would not make them vulnerable to fraud of another nature.

At the same time, the ongoing improvement of physical protection systems for UPTs and ATMs, such as systems to prevent the installation of spying equipment, or systems that enable the user to verify the appearance of the machine (AFAS measures) should be incorporated when replacing machines or when machines are compromised by fraudsters.

The Observatory reminds manufacturers of the need to take all threats into account systematically in the design stage, especially threats to the software loaded onto the machines.

The Observatory also urges card issuers and merchants to conduct information campaigns aimed at cardholders to make them take proper precautions when using UPTs and ATMs. The information campaign that the French Banking Federation aimed at bank branches operating ATMs seems to have been very helpful in identifying compromised machines as soon as possible.

In any event, the security issues surrounding UPTs and ATMs call for a convergence of efforts to develop European security standards involving all of the stakeholders: manufacturers, merchants and banks. The Observatory welcomes the various initiatives and urges the different stakeholders to participate in them in an active and coordinated manner.

3|3 Progress on the migration to EMV

The implementation of the EMV (Europay, MasterCard, Visa) specifications for chip cards in Europe marks a major step forward in the fight against cross-border fraud. It concerns both cards themselves and the accepting systems, including payment terminals, UPTs and ATMs, 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 three years, the Observatory measured progress on EMV migration by collecting statistics on the migration in France and Europe from the “CB” Bankcard Consortium and the European Payments Council (EPC). The data still show that progress in Europe is patchy. Some countries, including France, have nearly completed the migration, while others are lagging behind seriously. The Observatory is once again concerned about the disparities, which are likely to lead to the persistence of substantial cross-border fraud within Europe. With the SEPA project for payment cards slated to be implemented in early 2008,

these delays could mean that the adaptations will not be fully completed in 2008, thus facilitating cross-border payment fraud.

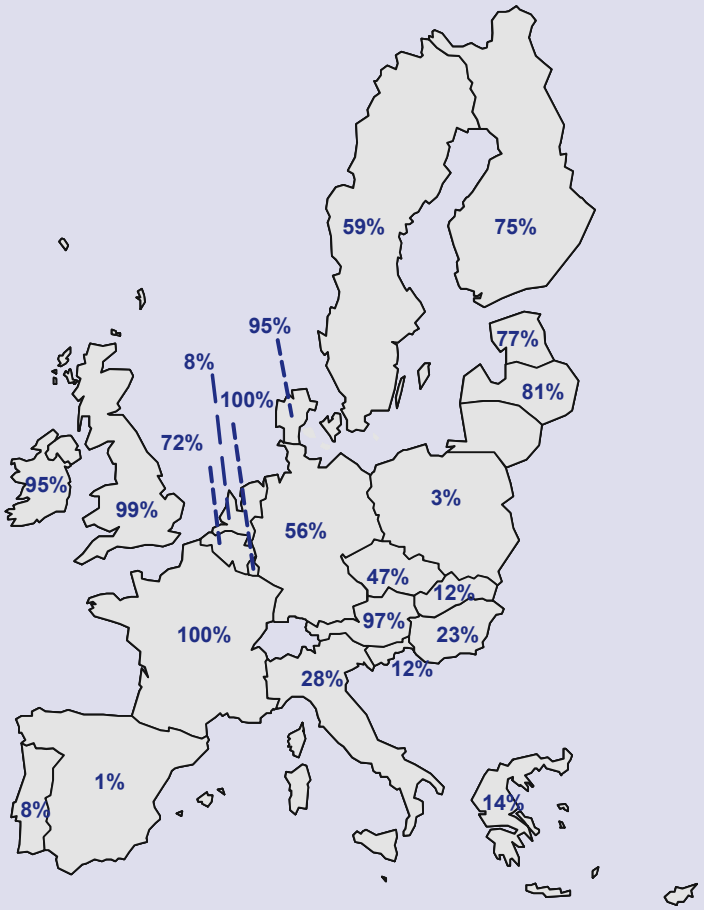
Progress on the migration to EMV in France

In France, migration to the EMV standard is practically complete. By the end of March 2007, according to statistics compiled by the "CB" Bank Card Consortium, 100% of CB cards, 95% of payment terminals and UPTs, and 100% of ATMs were EMV compliant.

Progress on the migration to EMV in Europe

In Europe, according to the data provided by the European Payments Council for the period up to the end of March 2007, 53.8% of the four-party cards in use in the 27 countries of the European Union are now EMV compliant. This represents an increase of six percentage points. The situation varies greatly from one country to the next (see Box 10). With the SEPA project only months away, several leading countries have barely started the migration, including Spain, Poland, Portugal and the Netherlands, or have made so little progress that their installed base is unlikely to be completely converted in 2008, such as Germany, Italy and Sweden.

Box 10 – Deployment of EMV cards in Europe



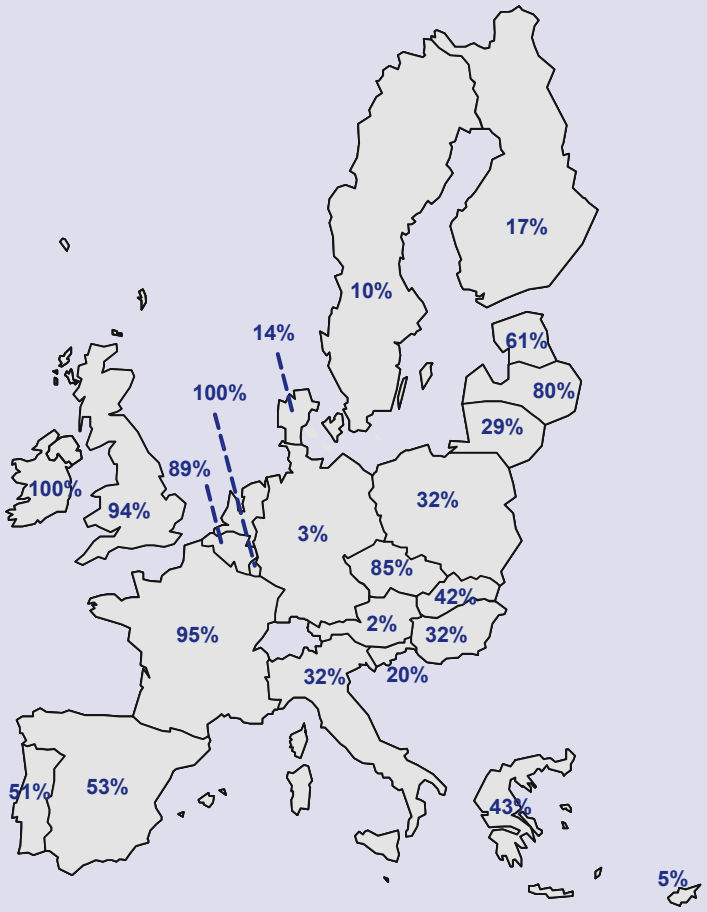
Source: European Payments Council – March 2007

As was the case in 2006, several leading countries have barely started migration, including Spain, Italy and Poland.

The map shows that, once again, EMV card deployment has made more progress in the countries of Northern Europe.

At the end of March 2007, migration of acquisition systems to EMV had progressed by 14 percentage points: 51.7% of payment terminals (see Box 11) and 66.1% of ATMs (see Box 12) were EMV compliant. The situation still varies greatly from one country to the next both in terms of percentages of compliant equipment and progress from one year to the next. There has been very little progress in Germany and Austria since March 2006, with very low percentages of compliant equipment. Yet, all of the EU countries have now started the migration process.

Box 11 – Deployment of EMV terminals and UPTs in Europe

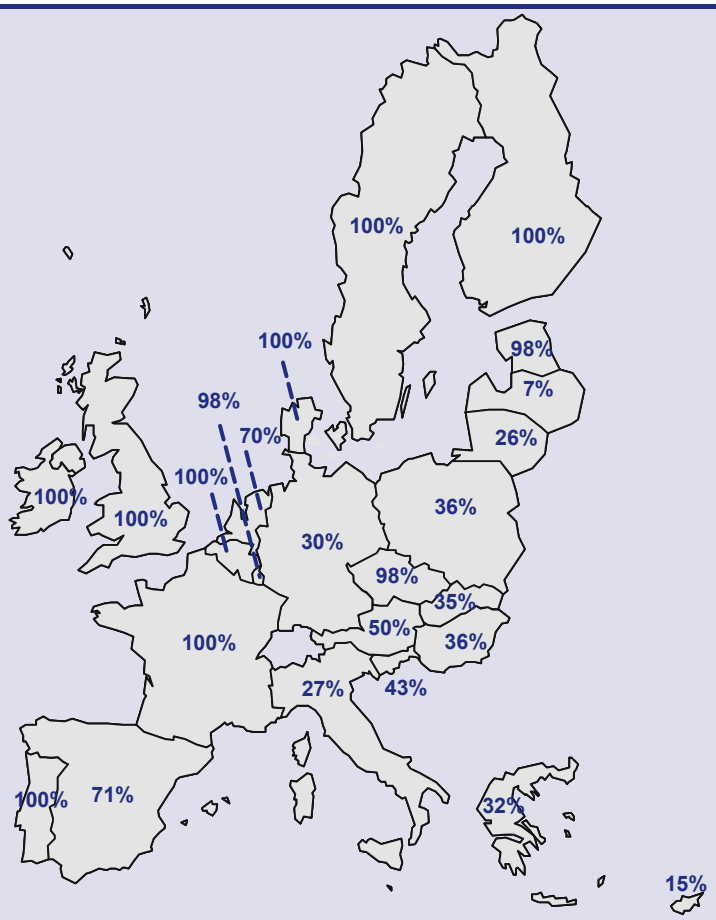


Source: European Payments Council – March 2007

The map shows that the pattern is the opposite of that for EMV-compliant card deployment. The migration of terminals is taking place more rapidly in the countries of Southern Europe on the whole. This pattern corresponds to the top tourist destinations, where the greatest number of cross-border transactions is likely to be made.

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

Box 12 – Deployment of EMV ATMs in Europe



Source: European Payments Council – March 2007

Progress on migration of ATMs has been more uniform in Europe, but there are still marked 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. However, deployment in Germany and Italy is still lagging behind the other leading countries.

4 | CARDHOLDERS' PERCEPTIONS OF PAYMENT CARD SECURITY

The statistics that the Observatory publishes have been used to measure the level of card payment fraud, how it changes and which payment methods are the least secure. Up until now, however, the Observatory did not have any information about cardholders' perceptions of the security of card payments or the impact of these perceptions on their use of payment cards.

Therefore, in early 2007, the Observatory commissioned a survey of French cardholders. The survey was conducted by CSA on a representative sample of 1,005 respondents between the ages of 18 and 74 living in metropolitan France[18], who were contacted by telephone on 5 and 6 February 2007.

The findings of the survey are presented below. By comparing these findings to its statistics, the Observatory attempted to learn if the cardholders' responses were in line with the main trends shown in the statistics. An analysis of the findings also shows the persistence of risky behaviour patterns on the part of cardholders and ignorance of the systems for blocking cards and disputing payments that are intended to protect cardholders. With this in mind, the Observatory, working with the support of its member bodies representing consumers, merchants and card issuers, drew up a list of security tips for the general public.

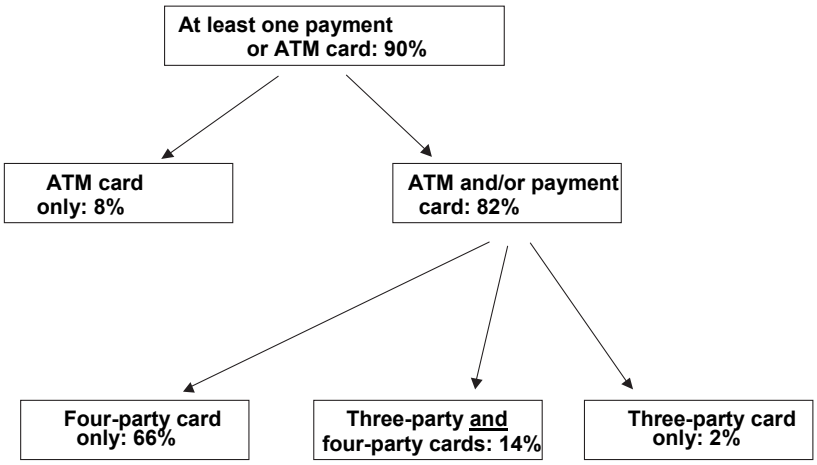
4|1 Payment card possession and use

Payment card possession

The vast majority of the respondents, 9 out of 10, possess at least one payment or ATM card. More specifically, 8% have only an ATM card for cash withdrawals, whereas 80% have at least one bank card and 16% have at least one three-party card[19].

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

[19] It should be noted that the distinctions between the different types of cards used for the purposes of the survey are not the same as the ones the Observatory usually uses. Four-party payment and ATM cards include all CB, Visa, MasterCard, American Express and Diners cards, whereas three-party and store cards include cards issued by credit organisations, such as Cetelem, Cofinoga, Sofinco, Finaref and Franfinance. Cards in the latter category are sometimes marketed directly by merchants under their own logo.

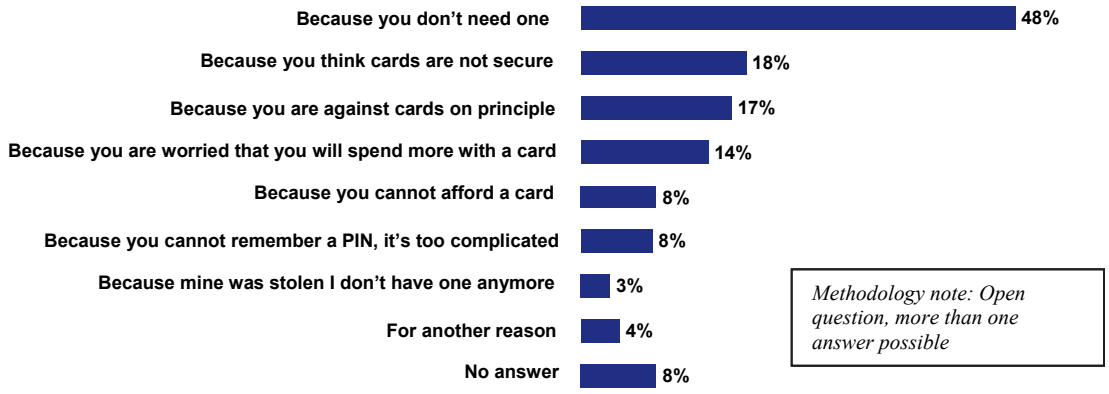


There are many reasons for choosing not to possess specific cards (see chart below). The first reason given is the lack of need. The lack of security is the second most commonly cited reason (18%), but this means that only 2% of the aggregate population aged between 18 and 74 does not have a card because of security concerns.

The other reasons cited by respondents are mainly a refusal to have a card on principle or their lack of financial resources, whether they are worried about spending more with a card or they find the fee charged for the card is beyond their means.

Reasons for not having a card:

(base: non-cardholders or 10% of respondents)



Segmentation of cards as perceived by cardholders

The French payment card market features many types of cards associated with different uses and target customers. The qualitative analysis has shown that, for cardholders, the cards available fall into four broad categories described below. These findings have been confirmed by the quantitative analysis.

“Ordinary everyday cards”
(held by 61% of the population aged 18 to 74)

This category covers the most common “four-party” cards in the Observatory’s usual classification. "Ordinary everyday cards” are the most frequently used and the most common for all types of uses: paying for ordinary purchases, cash withdrawals, payments in other countries or online payments.

These cards are an integral part of payment habits and their use is widespread, even though they are still in competition with cheques occasionally, particularly in the lowest socio-economic categories of the population.

“Selective cards”
(held by 17% of the population aged 18 to 74)

This category includes international three-party cards as per the usual definition given by the Observatory (American Express or Diners Club), but for some cardholders, it also includes some high-end four-party cards. Cardholders are uncertain about the position of such cards, since they are similar to the “ordinary everyday cards” by virtue of their widespread use.

"Selective cards” enjoy an image of prestige, especially for those who do not have them. For those who do have them, they are often associated with special expenses, such as major purchases, travel, and high status spending. They are also perceived to be more secure than other cards because of the various services and guarantees provided with such cards, such as assistance.

“Restricted cards”
(held by 8% of the population aged 18 to 74)

This category covers cards that require systematic authorisation of payments and ATM cards. They enjoy little status and are associated with young people who are still inexperienced with account management or low-income groups. They are perceived as more secure than ordinary cards, because of the restrictions on their use.

“Store cards”
(held by 18% of the population aged 18 to 74)

This category covers all other types of three-party cards. They are issued by consumer credit institutions, and some of them are perceived by cardholders to be issued by chain stores. The attraction of these cards lies directly in the pre-approved credit, even though loyalty-building actions can also be a factor in their popularity in some situations. As in the case of the restricted cards, the limited use of store cards makes holders feel that they are more secure.

Payment card use

Respondents showed strong attachment to their cards, with which they spontaneously associate such qualities as modernity and ease of use. Cards are accepted by virtually all merchants for any amount. They are suitable for many very different types of transactions, such as purchases, credit and cash withdrawals, and cardholders use them with great ease. This attachment largely overrides any concerns about fraud.

Widespread use in France

In France, payment card use is completely familiar for the vast majority of cardholders. Nearly 8 out of 10 cardholders report that they use their card often or always to pay for purchases and a comparable proportion report that they use their cards in a shop at least once a week. Only a small minority of cardholders use their card less than once a month.

The biggest users are urban males aged 45 to 54 in higher social and occupational categories with high income. Frequent use of cards is also strongly linked to interest in new technology.

Nearly all cardholders (95%) also use their cards for cash withdrawals from ATMs and half make such withdrawals at least once a week. On the other hand, patterns of use for UPTs for motorway tolls, train tickets, etc. are more contrasted. The proportion of cardholders who use their card in UPTs is smaller (approximately 3 out of 4), the frequency of the payments made by those who do use UPTs is fairly high (more than 5 times a month).

There is still reluctance about card-not-present payments and payments in other countries

Use of cards for card-not-present payments is natural for many cardholders. Some 30% use their card for payments by telephone at least 3 times a year and 47% of cardholders with access to the Internet make online payments with the same frequency. However, a certain proportion of cardholders are still reluctant to use their cards for card-not-present payments. Some 33% of cardholders never use their cards for payments by telephone, by post or online.

Whereas 51% of cardholders with international payment cards use their cards often or always to make payments and cash withdrawals when travelling, there are 33% who do not use their cards for cash withdrawals in other countries and a similar proportion that never use their cards to make payments, or use them as little as possible.

4|2 Judgments about payment card security

Cards are deemed to be more secure than other means of payment

Today, payment cards seem to be the most secure means of payment from the consumer's point of view. They are perceived to be safer than cash, credit transfers, direct debits and cheques.

Means of payment deemed to be the most secure:

(Base: aggregate French population aged 18 to 74)

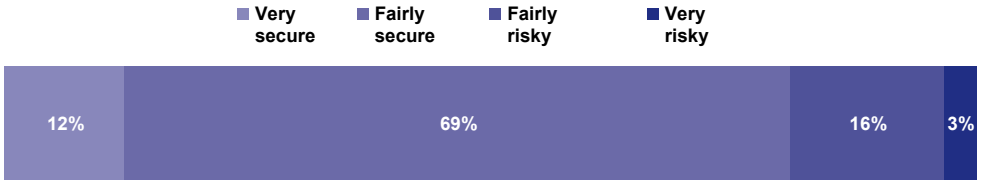
The ranking varies considerably, depending on the segment of the population: payment cards are deemed most secure by 45-to-64-year-olds, but the youngest respondents (18 to 24 years old) rated cash most secure, whereas the oldest (65 and over) rated cheques most secure.

Cards seen as a secure means of payment

The vast majority of cardholders consider that the use of cards is now secure on the whole: 12% consider that it is “very secure” and 68% “fairly secure”. Only 19% consider that the use of cards is “risky”, of which 3% think it is “very risky”. In addition, a large proportion of cardholders consider that payment card security is either constant (49%) or improving (43%).

Overall perception of payment card security:

(Base: All cardholders aged 18 to 74)



Furthermore, security concerns cannot be seen as a potential obstacle to the use of payment cards, since only 13% of cardholders report being bothered by the perceived risks in their use of them.

In line with the profile of the most frequent card users, the respondents most likely to consider cards a secure means of payment are employed men in higher social and occupational categories who are interested in new technology.

On the other hand, opinions about payment card security are more mixed in the oldest age groups and the lower social and occupational categories (65 and over, manual and non-manual workers, with primary or vocational education who are resistant to new technology).

Persistent concerns about card-not-present payments and payments in other countries

There is still a discrepancy between the overall opinion that cardholders express about payment card security and their feelings when using their cards. Virtually all of the 12% of cardholders who think that the use of payment cards is "very secure" also think that they are not taking any risks at all when they use their cards. But only 68% of those who think that the use of payment cards is “fairly secure” show the same confidence when they use their cards.

In contrast, 29% of the cardholders who think that the use of payment cards is risky in general terms report that they do not feel that they are taking a risk when they use their cards.

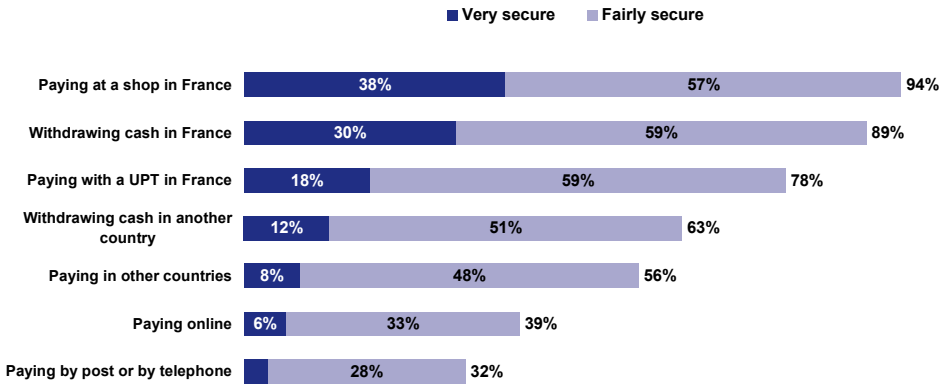
In all categories, however, the feeling of insecurity is limited: only 2% of cardholders feel that they are taking a large risk when they pay with their cards, and only 5% do so when they withdraw cash with their cards.

It should be noted that these feelings are more common among women, the most elderly respondents and those who are resistant to new technology.

The perception of security when using cards varies greatly, however, depending on the type of use.

Perception of payment card security in different situations:

(Base: all cardholders aged 18 to 74)



Virtually all cardholders think that using payment cards to make payments and cash withdrawals in France is secure, or even very secure for a third of respondents. However, the use of cards is seen as risky in other countries and even more so for payments online, by telephone or by post.

This means that nearly 4 out of 10 cardholders think that using payment cards in other countries is risky. The proportion is 6 out of 10 for online payments and 7 out of 10 for payments by post or by telephone, which are considered to be the two riskiest channels for card payments.

Payments by telephone or by post are distinctive because even the cardholders using these payment channels think that they are engaging in risky behaviour. This is not the case for the other types of payment, such as online payments (where 71% of respondents making online payments think that paying online is secure) and payments in other countries (where 76% of respondents making such payments think that they are secure).

Some cardholders report that they choose another means of payment than their card if they think that they are running a risk: 43% of cardholders have already done so once, and 31% several times. In three quarters of these cases, the payments concerned were payments online, by post or by telephone, or else payments made in other countries. The main means of payment substituted for a card in nearly two thirds of these cases is a cheque and, in a quarter of the cases, card payments are replaced by cash payments.

4|3 Dealing with security issues: proper reflexes, but lacking awareness of rights and terms of use

Financial institutions and the Banque de France at the forefront for the improvement of payment card security

According to cardholders, financial institutions and the Banque de France should be responsible for improving payment card security, even though they are not seen as liable for the risks associated with payment cards. Financial institutions are mentioned first or second by 66% of respondents, and the Banque de France is cited either first or second by 63% of the

respondents. The government is mentioned by 28% of respondents, followed by the police (18%), then consumer associations (11%) and, finally, merchants (9%).

Cardholders tend to think fraud is a global phenomenon that affects everyone, but that nobody is directly responsible for it. This means that the feel strongly involved in the security of their own cards: three quarters of them feel that they have a role to play in preventing fraud. It is noteworthy that the cardholders feeling most involved in security are those who feel that using their card is very secure or fairly secure.

Sound precautionary reflexes

On the whole, cardholders are aware of and appreciate the measures taken to ensure payment card security and the safeguards recommended by banks. Cardholders seem familiar with the issuers' recommendations regarding due care when using cards. They no longer perceive any particular message on the topic and the majority report that they comply with the various recommendations naturally[20].

These recommendations are seen as helpful, or even indispensable in many cases, and the vast majority of cardholders report that they follow them each time they make a payment. Yet, there are still 5% who report that they do not comply with any of the issuers' recommendations.

User information can still be improved

User information for cardholders can still be improved with regard to ways of improving payment card security or the terms of use for cards:

- More than one out of two cardholders report that they lend their cards to family members (their spouse in most cases);
- Means of securing online payments are still largely unfamiliar (68% of those making online purchases are unable to cite a single such means spontaneously);
- Insurance is reassuring for cardholders, but they are not actually familiar with the terms or coverage and cannot distinguish between personal assistance insurance and protection for the use of their card;
- The majority of cardholders feel instinctively that they are not financially liable in the event of fraud, without making any particular distinction between counterfeiting and other types of fraud;
- Cardholders seriously underestimate the time limit for reporting fraud, with 68% thinking it is 10 days or less;
- More than 80% of cardholders whose cards were lost or stolen reported it the same day, nearly 20% waited at least one day and 5% waited more than a week. And 3% never even reported their lost or stolen cards.

[20] The survey related to the following safeguards: checking the amount displayed when entering the PIN, not letting the card out of sight when paying, keeping payment and withdrawal receipts, checking account statements, finding out about safeguards when using cards in other countries, only using cards on the websites of reputable firms, installing antivirus software and a firewall on computers. There was also a question about how carefully account statements are checked.

4|4 Direct or indirect experience of fraud has little impact on behaviour

Vast direct and indirect experience of fraud

Even though fraud is an objectively limited phenomenon, it paradoxically affects a significant proportion of cardholders:

– 8% of cardholders report that their cards were used fraudulently;

– 18% of cardholders have also had an indirect experience of fraud, meaning that they know someone whose card was used fraudulently, even though they have no personal experience of fraud.

All in all, 1 out of 4 cardholders has ultimately had a direct or indirect experience of fraud. According to the cardholders concerned, fraud followed theft or loss of their cards in 21% of the cases, and online payments were the source of fraud in 20% of the cases. Cash withdrawals and payments in France, which represent the bulk of transactions, account for only 1 case of fraud in 4.

The profile of fraud victims matches that of the most frequent card users. In most cases they are men in higher social and occupational categories, as well as persons with an interest in new technology.

But the experience of fraud has only a limited impact on behaviour and the perception of payment card security

The experience of fraud does have an impact on its direct victims, but it is limited. Only 37% of fraud victims report that they have reduced their use of their cards, preferring cheques (22% of fraud victims) or cash (12%), while some 63% report no change in their behaviour.

The use of payment cards is also perceived as slightly more risky by cardholders who have been fraud victims (27% of fraud victims think that using cards is risky, as opposed to only 19% of all cardholders). On the other hand, indirect experience of fraud seems to have only a minor impact on the perception of payment card security.

Box 13 – Attitudes towards payment card security

The survey made it possible to identify five types of behaviour and attitudes in the cardholder population:

The anxious (15%)

Anxious about using cards, which they regard as very risky, they rarely pay with their cards.

The confident (8%)

Feeling that using cards is very secure, they use their cards frequently, in all situations, without any worries about the risks.

The prudent (21%)

Feeling that the use of their cards is not totally secure, they perceive a risk when they use their cards and take many precautions.

The vigilant (28%)

They feel that the use of their cards is fairly secure and use them without concern, while being aware of the inherent risks and remaining vigilant.

The resigned (28%)

They feel that the use of their cards is fairly secure, but they still feel that they are taking a risk every time that they use their cards. This is not really a major obstacle to using their cards.

4|5 Comparison of the main survey findings with the Observatory's own findings

The cardholders' generally positive perception regarding the use and security of payment cards is consistent with the figures that the Observatory has published in recent years. The number of cards held by the French, according to the Observatory's figures, is high at 78.6 million four-party and three-party cards. At the same time, fraud losses logged by French card systems stood at 0.064% of transaction amounts and the trend was declining compared to earlier years.

The different levels of perceived risk in different payment situations are in line with the fraud rates measured by the Observatory on the whole:

– Cardholders' strong confidence in face-to-face payments, which 94% think are secure, corresponds to a very low fraud rate of 0.024% of transaction amounts;

– Cardholders have less confidence in cash withdrawals from ATMs than in face-to-face payments (89% think they are secure), but the fraud rate logged by the Observatory is only 0.019%. The difference may stem from the precautions that cardholders take when carrying cash;

– Payments and cash withdrawals in other countries are perceived as relatively riskier on the whole. This perception is consistent with the Observatory's figures. In 2006, the fraud rate for all payments made with French cards in other countries stood at 0.421%, as opposed to 0.035% for French cards in France. Meanwhile, the fraud rate for cash withdrawals with French cards in other countries stood at 0.555%, as opposed to 0.019% in France. However, the cardholders' perceptions vary quite substantially if we look only at those who actually travel to other countries. Only 56% of cardholders feel that payments in other countries are secure, but this figure is 76% for cardholders who actually travel to other countries. The proportions are 63% versus 82% in the case of cash withdrawals in other countries;

– Card-not-present payments raise the greatest concern, both for online payments, which only 39% of cardholders feel are secure, and for payments by post or by telephone (32%). This is in contrast to the Observatory's estimates: the fraud rate for domestic card-not-present payments is estimated at 0.199%, which is eight times higher than the fraud rate for face-to-face payments and UPT payments. However, regular users of online payments show a higher level of confidence, with 71% thinking that online payments are secure. This is not the case for payments by post or by telephone;

– Payments with UPTs are considered secure by 78% of the cardholders. The Observatory does not have the data to assess the specific fraud rate for such payments, but the qualitative study seems to show that media coverage of attacks on certain types of machines has made cardholders more careful.

Ultimately, fraud affects a larger proportion of the French population than that measured by the Observatory

The survey shows that 8% of cardholders report that they have been a direct victim of fraud at least once in their life, and a further 18% report that at least one person close to them has been a fraud victim. Only a direct experience of fraud seems to have an impact on cardholders' perceptions, however: 27% of cardholders with a direct experience of fraud think that using a payment card is risky, as opposed to 18% of cardholders with no experience of fraud and 19% of cardholders with an indirect experience of fraud.

Nevertheless, negative perceptions stemming from direct experience of fraud seem to last for several years: The seemingly high proportion of cardholders affected by fraud stems from the accumulation of cases over several years, or even several decades in some cases.

By comparing data on behaviour, perceptions and experiences of fraud, the CSA polling institute was able to identify two very different groups of cardholders. The first group, representing about 15% of the population, CSA qualifies as "anxious", meaning those who think that using cards is very risky and who, consequently, rarely use their cards to make payments. The second group of cardholders, representing about 8% of the population, are qualified as "confident", meaning that they think that using cards is very secure and they use their cards frequently in all types of situations, without worrying about risk.

The Observatory does not have the right data to estimate the number of cardholders affected by fraud each year. However, it does publish the number of fraudulent transactions logged by the French card systems, which can be used to set the maximum number of people affected. In 2006, 1.7 million cases of fraud involving French cardholders were logged. Therefore in 2006, at the most, fraud affects 2.2% of the cards in circulation.

The recommended safeguards are familiar and complied with, but they have not eliminated all types of risky behaviour

Recommended safeguards for cardholders making payments with their cards have been disseminated to the public for several years now, amongst others, by issuers and the consumer associations that are members of the Observatory. Consequently, the Observatory has not yet communicated on all of these safeguards. The Observatory's previous reports dealt only with certain security solutions, particularly for card-not-present payments.

The findings of this survey show that cardholders are very involved in the security of their cards. Nearly three quarters (72%) of holders feel that they have a personal role to play in preventing fraud. They also confirm that the safeguards are familiar and followed by the vast majority of cardholders.

A small but significant proportion of cardholders (5%) report that they never follow any of these safeguards, and some of them think that these safeguards do nothing to improve the security of card payments.

Furthermore, familiarity with these safeguards does not eliminate all types of risky behaviour. Despite the recommendations of most issuers, 53% of cardholders report that they have lent their cards to others, primarily their spouse or their children. Most cardholders (82%) state that they reported lost or stolen cards the same day, but a minority did not report lost or stolen cards for several days after they went missing.

In the specific case of online payments, 58% of cardholders feel that requiring the purchaser to provide the CVx2 code is an effective safeguard. Nevertheless, it is noteworthy that other secure online payment solutions are not very familiar. Nearly 70% of respondents making online purchases were able to cite any, despite their perception of higher risks.

The terms of use for payment cards are not familiar enough

The Observatory reported on the legal framework applying to payment cards in France in its 2003 annual report. It focused on two provisions protecting cardholders: the liability cap of EUR 150 before reporting a lost or stolen card (Article L. 132-3 of the Monetary and Financial Code) and the exemption from liability in the event of fraudulent card-not-present payments (Article L. 132-4).

However, these provisions do not seem to be very familiar to cardholders. Many of them (70%) think that they are not financially liable for fraud of any type (lost or stolen cards, forged or counterfeit cards). The legal time limit for disputing transactions is also greatly underestimated, probably because it is often confused with the time limit for reporting lost or stolen cards.

Furthermore, the qualitative study showed that the majority of cardholders did not have a clear understanding of the content and coverage provided by the insurance that comes with most cards, especially four-party cards. This finding was confirmed by the quantitative survey.

Security tips for cardholders

For the various reasons mentioned above, the Observatory has drawn up a series of security tips for cardholders. These tips were drafted in collaboration with representatives of consumers,

merchants and issuers so that each group can reuse the list of tips for their own audience, as appropriate to their own circumstances.

The following list has been deliberately written in plain language and is limited to the main security measures. The Observatory will post this list of tips to its website and urge the media and the public authorities to give these recommendations wide distribution.

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 it.
– If your card comes with a PIN code, 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. Avoid machines that you think have been altered if possible.
– 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 with 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.

Your bank may require you to report lost or stolen cards within a given time limit, which must be at least two full days. If you report a lost or stolen card within this time limit, you will only be liable for the first EUR 150 of fraudulent payments made with your card before you report it missing. On the other hand, if you fail to report a lost or stolen card within this time limit, you will be liable for all fraudulent payments made before you report it missing. Once you have reported a lost or stolen card, you are no longer liable for the next fraudulent payments.

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

Unless 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 make a written claim as soon as possible. The time limit set by law is 70 days after the date of the disputed transaction. The card issuer may extend this limit, but it cannot be more than 120 days. You will not be liable. The disputed amounts must be reimbursed at no charge and within one month of receiving the claim.

ANNEX A | MISSIONS AND ORGANISATIONAL STRUCTURE OF THE OBSERVATORY

The Decree 2002-709 of 2 May 2002 implementing Article L. 141-4 of the Monetary and Financial Code lays down the missions, composition and operating procedures of the Observatory.

Scope

Article L. 132-1 of the French Monetary and Financial Code defines a payment card as "any card issued by a credit institution or an institution referred to in Article L. 518-1, which enables its holder to withdraw or transfer funds".

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, 5° of the Monetary and Financial Code, benefit from an exemption to banking monopoly. These cards are issued by an undertaking and accepted as means of payment by said undertaking itself or by a limited number of acceptors that have financial and commercial ties with the issuer.

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 differed (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.
– *International cards* serve to make payments and withdrawals at all national or international acquiring points managed by national acquirers or by foreign partner acquirers.

– *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 the aforementioned Article L. 141-4 of the Monetary and Financial Code and the Decree of 2 May 2002, 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 addition, 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 the aforementioned Decree of 2 May 2002. The Observatory is made up of:

– A Deputy and a Senator,
– Eight general government representatives:
  - a representative of the general secretariat for National Defence,
  - two representatives of the Minister of the Economy and Finance,
  - a representative of the Minister of Justice,
  - a representative of the Minister of the Interior,
  - a representative of the Minister of Defence,
  - a representative of the Minister for Consumer Affairs,
  - a representative of the Minister of Industry.
– The Governor of the Banque de France or his/her representative,
– The General Secretary of the Banking Commission 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 an annex 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 Banking Commission, are appointed for a three-year term. Their term can be renewed twice. The President is appointed among these members by the Minister of the Economy and Finance. He has a three-year term of office, renewable twice. 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, 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 maintaining 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.

ANNEX B | 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.

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Jean-Pierre BRARD
Deputy

Nicole BRICQ
Senator

Representative of the General Secretary of the Banking Commission

Jean-Luc MENDA
Deputy Director of General Surveillance of the Banking System

Representatives of public administrations

Nominated on proposition by the General Secretary for National Defence:

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

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

- The Senior Official for Defence or his/her representative:
  Emmanuel SARTORIUS
  Alain ROCCA
- The Head of the Treasury and Economic Policy or his/her representative: **Maya ATIG**
  Audrey SUDARA-BOYER

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
  Virginie BEAUMENIER
  Jean-Pierre GERSKOUREZ

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons
  or his/her representative:
  Pauline FLAUSS
  Vincent MONTRIEUX

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

Nominated on proposition by the Minister of Defence:

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

Nominated on proposition by the Deputy Minister of Industry:

- The Director General of Business or his/her representative:
  Mireille CAMPANA

Representatives of payment card issuers

Brigitte CHARLIER
Head of Electronic Payments (CEDICAM)

Patrice COUFFIGNAL
Director (Europay France)

Armand de MILLEVILLE
Executive Vice President (American Express France)

Jean-Marie DRAGON
Electronic Payments Expert (La Banque Postale)

Bernard DUTREUIL
Director (Fédération Bancaire Française)

Hervé DUCHARNE
Audit Manager and Research (Groupe Carte Bleue)

Alain GOLDBERG
Risk and Compliance Director (Natexis Paiements)

Dominique JOLIVET
Head of Risk Management and Electronic Payment Security Department (Caisse Nationale des Caisses d'Épargne)

Cédric SARAZIN
Business and Strategy Manager (Groupement des cartes bancaires)

Gérard JOUVE
Institutional Relations Manager (CETELEM)

Representatives of the Consumer Board of the National Consumers' Council

Michèle DAUPHIN
Representative and technical adviser (Familles de France)

Valérie GERVAIS
General Secretary of Association FO Consommateurs (AFOC)

Jean-Pierre JANIS
National Adviser, Associations Familiales Laïques (CNAFAL)

Christian HUARD
General Secretary, Association d'éducation et d'information du consommateur de l'Éducation nationale – ADEIC

Frédérique PFRUNDER
Special adviser to Confédération du logement et du cadre de vie – CLCV

Representatives of merchants' professional organisations

Richard BOUTET
Means of Payment Adviser (Fédération des entreprises du commerce et de la distribution)

Marc LOLIVIER
General Delegate, Fédération des entreprises de vente à distance (FEVAD)

Jean-Marc MOSCONI
General Delegate (MERCATEL)

Philippe SOLIGNAC
Vice-President (Chambre de commerce et d'industrie de Paris)

Guillaume VANOVERSCHELDE
Chief Administrative Officer and Chief Financial Officer (DECATHLON)

Persons chosen for their expertise

Philippe CAMBRIEL
Executive Vice-President (Gemalto)

Jacques STERN
Head of the Information Technology Department, École normale supérieure (ENS)

Sophie VULLIET-TAVERNIER
Head of Legal Affairs, Commission nationale de l'informatique et des libertés – CNIL

ANNEX C | STATISTICS

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

- The 150 members of the "CB" Bank Card Consortium and international data from Europay France and the Carte Bleue Group;
- Nine three-party card issuers: American Express, Banque Accord, Cetelem, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco;
- Issuers of the electronic purse Moneo, through BMS (Billettique Monétique Services);

The data collected came from six merchants accepting payment cards: Carrefour, the Casino group, Décathlon, France Loisirs, Monoprix, and the French railways (SNCF). For the first time, the Observatory also received statistics collected by the distance selling federation FEVAD from a representative sample of its members in 2006.

Changes in the sample and some of the computation procedures mean that not all of the data provided here are comparable with data that the Observatory has previously published. Readers should refer to Part 2 of this report for analysis and interpretation of the data.

Total number of cards in circulation in 2006: 78.6 million, including:

- 53.6 million four-party cards ("CB" and Moneo);
- 25 million three-party cards.

Number of cards reported lost or stolen in 2006: approximately 400,000

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

Cross-border transactions represent a tiny share of transactions. In 2006, only 3.3% of French cardholders' transactions took place outside of France, as opposed to 2.5% in 2005.

The payment card market in France

	French issuer / French acquirer		French issuer / Foreign acquirer		Foreign issuer / French acquirer	
Four-party cards	**Volume (millions)**	**Value (EUR bn)**	**Volume (millions)**	**Value (EUR bn)**	**Volume (millions)**	**Value (EUR bn)**
Face-to-face and UPT payments	5,172.59	226.63	101.13	8.09	131.75	12.24
Card-not-present payments, excluding online payments	na	9.98	5.38	0.79	5.38	1.30
Online payments	84.89	6.31	34.62	2.23	7.17	0.72
Withdrawals	1,295.90	88.35	33.97	4.03	27.85	4.72
Total	**6,553.38**	**331.27**	**175.11**	**15.14**	**172.15**	**18.97**
Three-party cards	**Volume (millions)**	**Value (EUR bn)**	**Volume (millions)**	**Value (EUR bn)**	**Volume (millions)**	**Value (EUR bn)**
Face-to-face and UPT payments	196.65	22.95	7.77	1.64	15.12	3.36
Card-not-present payments, excluding online payments	0.95	0.23	0.22	0.05	0.54	0.20
Online payments	0.67	0.14	0.14	0.03	0.26	0.05
Withdrawals	11.32	1.03	na	na	na	na
Total	**209.58**	**24.34**	**8.12**	**1.72**	**15.91**	**3.61**
Grand total	**6,762.97**	**355.61**	**183.23**	**16.86**	**188.06**	**22.58**

Source: Observatory for Payment Card Security

Breakdown of four-party card fraud by type of transaction, origin 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	**843.9**	**51,923.7**	**184.2**	**26,825.5**	**376.4**	**57,685.1**[1]
Lost or stolen cards	522.5	34,448.9	111.4	9,295.6	167.4	11,830.0
Intercepted cards	13.4	614.8	3.3	535.6	4.9	479.1
Forged or counterfeit cards	308.0	16,860.1	62.1	15,182.1	96.9	23,249.9
Appropriated card numbers	0.0	0.0	4.1	733.4	10.4	801.1
Other	0.0	0.0	3.2	1,081.7	96.8	21,325.0
Card-not-present payments, excluding online payments	**213.0**	**19,475.7**	**25.4**	**4,567.0**	**na**	**na**
Lost or stolen cards	0.0	0.0	8.5	1,566.5	na	na
Intercepted cards	0.0	0.0	0.1	16.2	na	na
Forged or counterfeit cards	0.0	0.0	6.0	1,296.8	na	na
Appropriated card numbers	213.0	19,475.7	1.0	82.8	na	na
Other	0.0	0.0	9.9	1,604.7	na	na
Online payments	**96.6**	**13,214.0**	**168.4**	**20,051.7**	**na**	**na**
Lost or stolen cards	0.0	0.0	48.4	5,862.2	na	na
Intercepted cards	0.0	0.0	0.2	23.2	na	na
Forged or counterfeit cards	0.0	0.0	40.9	5,131.2	na	na
Appropriated card numbers	96.6	13,214.0	2.2	252.2	na	na
Other	0.0	0.0	76.7	8,782.9	na	na
Withdrawals	**72.8**	**15,862.0**	**115.9**	**22,388.3**	**21.1**	**5,047.1**
Lost or stolen cards	70.8	15,530.4	16.8	2,927.9	3.4	773.4
Intercepted cards	0.5	93.8	0.1	19.7	0.1	19.1
Forged or counterfeit cards	1.5	237.8	98.4	19,298.3	16.5	4,049.6
Appropriated card numbers	0.0	0.0	0.6	131.0	0.1	23.1
Other	0.0	0.0	0.1	11.4	1.0	181.9
Total	**1,226.3**	**100,475.4**	**493.9**	**73,835.5**	**397.5**	**62,732.2**

Source: Observatory for Payment Card Security

[1] Foreign card issuers cannot distinguish face-to-face and UPT payments from card-not-present payments. This means that the only relevant distinction is that between payments and withdrawals. Therefore, the figures given for "Foreign issuer, French acquirer" fraud correspond to all payments, meaning the sum of card-not-present payments, face-to-face payments and UPT payments.

Breakdown of three-party card fraud by type of transaction, origin 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	**15.89**	**7,142.51**	**4.38**	**1,248.25**	**2.67**	**1,654.69**
Lost or stolen cards	7.31	1,574.74	0.74	246.64	0.92	574.99
Intercepted cards	3.47	820.75	0.44	167.81	0.03	4.41
Forged or counterfeit cards	0.66	278.11	2.90	777.35	1.57	911.85
Appropriated card numbers	0.38	364.26	0.05	19.33	0.08	48.98
Other	4.07	4,104.65	0.24	37.12	0.07	114.46
Card-not-present payments, excluding online payments	**0.71**	**306.59**	**3.09**	**1,126.43**	**2.56**	**1,718.84**
Lost or stolen cards	0.10	17.77	0.08	22.39	0.13	36.64
Intercepted cards	0.07	4.50	0.06	31.22	0.01	4.41
Forged or counterfeit cards	0.07	7.36	0.22	68.06	0.41	192.10
Appropriated card numbers	0.38	255.92	2.66	983.72	1.93	1,389.45
Other	0.08	21.04	0.07	21.03	0.08	96.24
Online payments	**0.28**	**205.70**	**0.95**	**219.23**	**1.24**	**441.20**
Lost or stolen cards	0.05	56.97	0.01	2.13	0.03	4.53
Intercepted cards	0.00	0.00	0.01	0.55	0.01	0.50
Forged or counterfeit cards	0.00	0.00	0.02	3.55	0.08	26.30
Appropriated card numbers	0.21	142.73	0.90	211.76	1.11	407.96
Other	0.02	6.00	0.01	1.24	0.02	1.90
Withdrawals	**4.45**	**1,492.39**	**0.00**	**0.00**	**0.00**	**0.00**
Lost or stolen cards	3.61	863.70	0.00	0.00	0.00	0.00
Intercepted cards	0.42	244.33	0.00	0.00	0.00	0.00
Forged or counterfeit cards	0.00	0.00	0.00	0.00	0.00	0.00
Appropriated card numbers	0.00	0.00	0.00	0.00	0.00	0.00
Other	0.42	384.36	0.00	0.00	0.00	0.00
Total	**21.33**	**9,147.18**	**8.42**	**2,593.91**	**6.47**	**3,814.73**

Source: Observatory for Payment Card Security

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 19 octobre 2007