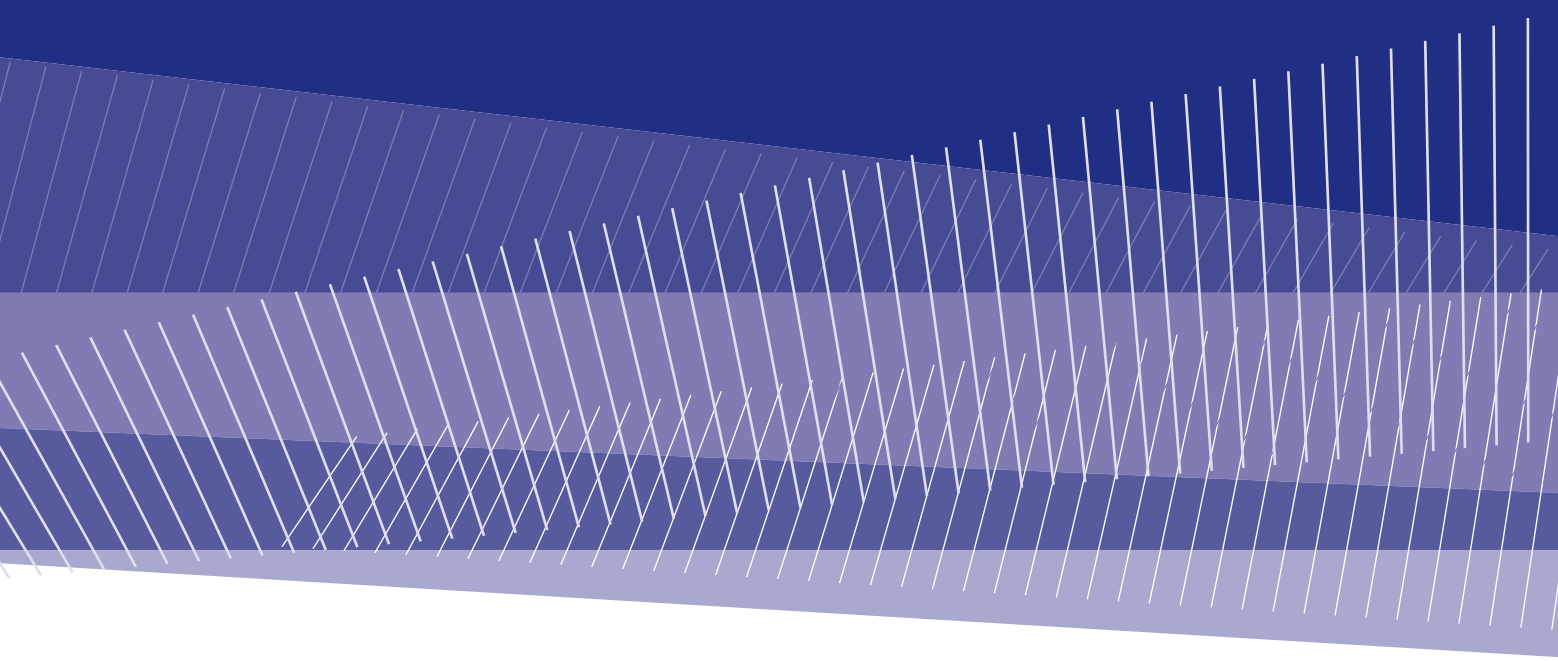
2008 ANNUAL REPORT

OF THE OBSERVATORY FOR PAYMENT CARD SECURITY



Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

2008 ANNUAL REPORT

OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

bservatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr

Observatoire
de la sécurité
des cartes de paiement

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

2008

Annual Report of the Observatory for Payment Card Security

addressed to

The Minister of the Economy, Industry and Employment,
The President of the Senate,
The President of the National Assembly

by

Christian Noyer,

Governor of the Banque de France,
President of the Observatory for Payment Card Security

CONTENTS

PRESIDENT'S MESSAGE

As the second mandate of the members of the Observatory for Payment Card Security draws to a close, let me emphasise that the security issues facing payment card professionals and users truly are at the heart of the work done by this institution.

European questions have been front and centre in our agenda, reflecting developments linked to the Single Euro Payments Area (SEPA) and the creation of a harmonised legal framework by the Payment Services Directive. The Observatory has often been a step ahead of European discussions, drawing attention over the last few years to the challenges of harmonising payment instruments in Europe and issuing recommendations to promote a high level of security for card payments in Europe. This year's report stresses the importance of implementing harmonised certification procedures for card security in Europe.

One of our core tasks is to monitor fraud and its developments. The annual statistics published have been regularly expanded and provide a valuable reference source for market players, giving them a clearer understanding of how fraud is evolving, so that security and protective measures can be adapted accordingly.

The 2008 statistics show that fraud has increased by more than the overall growth in card payments and withdrawals. Fraud was up most obviously in card-not-present domestic payments, but also increased markedly among foreign transactions using French cards. However, the rules on the distribution of fraud mean that consumers, who are protected by law, have not had to sustain any loss from fraud. The Observatory monitored this increase closely and carried out an analysis of security for card-not-present payments. It found that cardholder authentication requirements should be tightened wherever possible to bring the security of card-not-present payments up to the same level as that of face-to-face payments.

The report also covers studies by the Observatory in a number of topical areas for payment card professionals and users, including the emergence of instant issuing systems for payment cards at the point of sale, the rise of card co-branding, and security measures for unattended payment terminals connected to open networks.

The Observatory's diverse projects are a precious source of information and recommendations that will surely, as in years past, help to guide efforts to maintain the security of card payments.

Christian NOYER

FOREWORD

The Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement – hereinafter the Observatory*) was created by virtue of the Everyday Security Act 2001-1062 of 15 November 2001[1]. The Observatory is meant to promote information sharing and consultation between all parties concerned by the smooth operation and security of card payment schemes (consumers, merchants, issuers and public authorities)[2].

Pursuant to the sixth indent of Article L. 141-4 of the French Monetary and Financial Code, the present document reports on the activities of the Observatory. It is addressed to the Minister of the Economy and Finance and transmitted to Parliament. Part 1 consists of a study on the security measures applied to in-branch and in-store instant issuing systems. Part 2 details the 2008 fraud statistics. Part 3 is a summary of the Observatory's technology watch activities, while Part 4 contains a study on the security certification of cards and terminals.

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

2 For the purpose of its work, the Observatory makes a distinction between "four-party" and "three-party" card payment schemes. Four-party cards are issued and acquired by a large number of credit institutions. Three-party cards are issued and acquired by a small number of credit institutions.

1 | SECURITY MEASURES APPLIED TO INSTANT ISSUING SYSTEMS

As part of its task of monitoring the security policies applied by issuers and acceptors, the Observatory decided to supplement its 2006 study on the protection of card data during the card personalisation process by conducting an analysis of the security of in-branch and in-store instant issuing systems.

The personalisation process consists in loading information onto blank cards to render them useable by holders. It is usually performed by personalisation centres, which handle industrial quantities of card data and media. The 2006 study showed that these centres deploy security measures to provide physical and logical protection for these sensitive items. But to be able to respond more swiftly to customer needs, some issuers are using instant issuing techniques, where cards are personalised at the time when they are made available to holders. Establishing a contractual relationship right at the point of sale may, for example, allow the customer to instantly take advantage of a promotional offer or obtain credit for a purchase.

Issuers of three-party cards in France have made wide use of this type of solution in recent years. For some of them, instant issuing accounts for a large proportion of new card issuance. The technique is gaining ground among issuers of four-party cards in the international networks (MasterCard, Visa). In response to demand from members, the “CB” Bank Card Consortium is also working on special rules to enable the secure implementation of instant issuing systems. Furthermore, with the rise of co-branding[3], the personalisation process may be carried out at the premises of a commercial partner, rather than by the issuer.

The Observatory therefore decided to carry out a study to see whether the level of security of instant issuing systems was on a par with security at personalisation centres. To do this, it gathered information by sending out a questionnaire to representatives of issuing institutions[4], card manufacturers and personalisation centres[5], and technical providers[6] involved in the personalisation process.

The study looks at the risks associated with instant issuing, plus the security measures put in place to prevent these risks at the different stages of this area of activity.

---

3 Co-branding consists in associating the card with the brand of the credit institution issuing the card along with one or more brands of other commercial partners.

4 Banque Accord, BNP Paribas Personal Finance (formerly Cetelem), Cofinoga-Laser, Finaref, “CB” Bank Card Consortium, S2P.

5 Association des Fabricants et Personnalisateurs de Cartes (AFPC), Giesecke & Devrient.

6 ATOS, Monext.

1 | 1 Instant issuing systems

Main stages

Instant issuing of payment cards usually comprises the following stages:

– **gather customer data**: a customer who wants to take up the offer of a payment card, whether in a bank branch or at the store of one of the issuer's commercial partners, provides the personal information needed to issue the card;

– **prepare card data**: once the application has been approved, the card data, i.e. card number, security code, cryptographic keys and PIN, are generated based on the cardholder's information, then sent to the instant issuing server, which prepares the data contained on the stripe and/or chip;

– **personalise card and issue it to the customer**: the prepared data are sent to a personalisation device in the branch or store. Once the card has been personalised, it is activated by the issuer and given to the holder, who may then use it at once.

These stages entail a number of tasks and exchanges of information involving several environments, namely the in-branch or in-store customer service area, the issuer's card management system and the instant issuing server, which may be housed by the issuer or by a technical provider. The various tasks are carried out on a number of devices that operate in a network, including PCs, servers and personalisation devices (see Box 1).

Data processed and produced as part of the instant issuing process

The data gathered and processed at the customer service area include the cardholder's ID (first and family names, address), and potentially the PIN, which the holder may be allowed to select, as well as information about the required card (card type, visual aspects, where applicable) and arrangements for using the card (withdrawal and/or payment, systematic authorisation, maximum amounts, etc.).

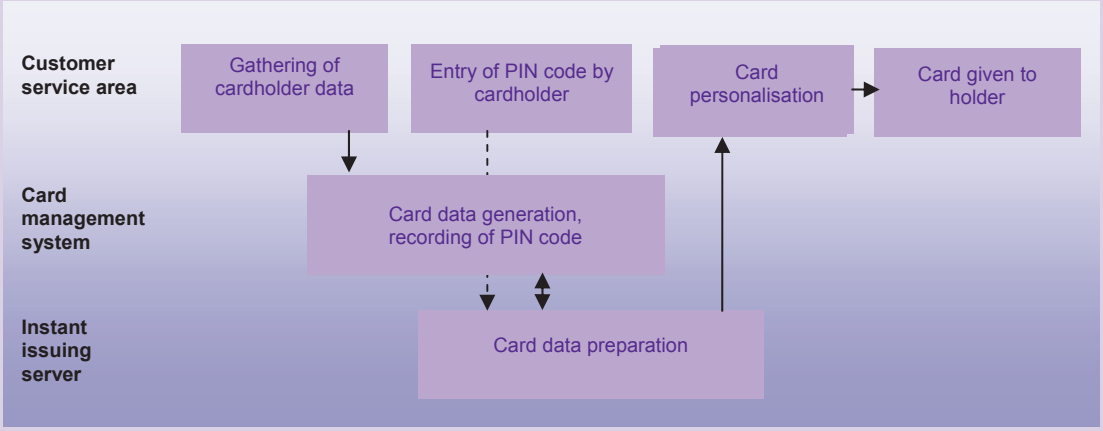
The issuer's information system generates a card number and an expiry date, which it sends to the issuer's card management system.

Based on this information, the issuer's card management system and the instant issuing server process and generate a set of supplementary data, including:

– sensitive data (encoding data for the magnetic stripe and/or preparation of EMV data with associated keys and security codes): these data, which are required for all card personalisations, are generated using the issuer's keys in cryptographic modules;

– data used for administrative management and supervision of equipment and actions (management of authorisations and system access, orders sent to in-branch personalisation devices, traceability data, etc.).

Box 1 – Description of the instant issuing process



Instant card issuance usually comprises the following stages:

– The customer comes to the customer service area of a bank branch or at the premises of one of the issuer's commercial partners. A customer service representative helps him or her to complete a payment card application, potentially as part of a credit arrangement. As part of this process, the customer service representative enters personal information provided by the holder.

– These data are sent to the issuer's information system, which approves the application and assigns a card number.

– Once the application has been approved, the representative begins the instant issuing process using an application connected to the dedicated instant issuing server housed by the issuer or a technical provider.

– The personal data gathered in the branch or at the store are sent to the issuer's card management system.

– If applicable, the customer may be asked to select and then enter a PIN at the branch or store.

– The card management system generates the card data and sends them to the instant issuing server, which prepares the card personalisation data.

– The instant issuing server sends the prepared data (stripe and/or chip) to a personalisation device with blank cards located in the branch or store.

– The card is personalised with the customer's data, activated by the issuer and then given to the holder in the branch or store, where it can be used immediately. If the personalisation process is centralised, the customer has to wait for the card to be sent to him or her.

1|2 Security of instant issuing systems

As with centralised card personalisation systems, the various stages of the instant issuing process involve sensitive information, equipment and products that, if misappropriated or copied, could be used to make fraudulent payments.

Accordingly, issuers and their technical providers should deploy security solutions that provide a level of data protection equivalent to that achieved by personalisation centres.

However, given the nature of the instant issuing process, where several sensitive steps are carried out in an open area for customers that is harder to make safe and supervise than a personalisation centre, specialists who were questioned on this issue said that special protective measures needed to be put in place, particularly to prevent the risks of compromise:

- in the customer service area, i.e. theft and/or misappropriation of data processed by personalisation devices and applications, theft of cards or supplies used in the personalisation process;
- in the channels of communication connecting the point of sale to the issuer's or technical provider's instant issuing server, i.e. interception of data on networks, unavailability of equipment and systems;
- during the transportation and use of blank and rejected cards, as well as new and used supplies.

The following areas are therefore covered by special security measures.

Customer service area

A set of security measures is generally implemented for the customer service area to prevent personalisation devices from being compromised. Physical protection measures, such as entry controls and continuous surveillance of the premises (videosurveillance, alarms, security staff), are typically in place for these devices, which themselves may also be the subject of special protection arrangements, e.g. they may be sealed or locked away. There are also procedures to prevent the misappropriation of sensitive items, such as blank or rejected cards or supplies such as embossing ribbons or print ribbons for security codes, during maintenance of these devices.

To protect access to the applications used to approve requests to issue and manufacture instant issuing cards, authentication mechanisms are generally in place to prevent anyone from posing as a customer service representative. Assigning restricted rights to these applications also prevents certain types of fraud, including the creation of counterfeit cards (that do not draw on a customer's account) or duplicate cards (that do draw on a customer's account). The risk of interception of customer data, notably the PIN when it is entered at the point of sale, may also be subject to special measures, e.g. secure terminals connected to the representative's workstation may be used. Furthermore, application servers usually have back-up systems in case applications are unavailable.

Physical and logical security measures at locations where cards are issued on an instant basis may additionally be covered by audit clauses in contracts between issuers and their commercial partners.

Communication channels

To prevent data from being intercepted on the networks that link customer service areas to the servers operated by issuers or their technical providers, secure links such as Virtual Private Networks (VPNs)[7] or application encryption solutions based on the Secure Socket Layer version 3 (SSLv3) protocol[8] are typically deployed. End-to-end encryption is usually provided for highly sensitive data (e.g. PINs). Filtering solutions are also often in place to protect access to networked application servers and so foil efforts to take control of devices from a remote location.

Cards and supplies

Like customer service areas, cards and supplies are covered by special provisions and procedures. These are designed to prevent them from being stolen or misappropriated during their transportation to and from the customer service area. For example, these items may be delivered by special transporters (cash transit companies) or carried by secure courier services.

In addition, physical protection measures are usually used to safeguard batches of blank or rejected cards, such as a secure box or enclosure attached directly to the personalisation device at the point of sale. The same is true for supplies, such as embossing ribbons or print ribbons for security codes.

Rejected cards and used supplies are destroyed in a secure manner, for example by following a procedure involving only authorised members of staff.

Traceability systems (automated in information systems and affected equipment, or built into operational procedures) ensure end-to-end control of all sensitive operations.

Issuer's environment

All the physical and logical security measures for the customer service area, communication channels and cards and supplies are covered by recommendations that the international networks (Visa, MasterCard) apply to issuers and their technical providers. The "CB" Bank Card Consortium is also working on security requirements for instant issuing.

The networks' security and organisation recommendations draw heavily on the arrangements at personalisation centres (protection of sensitive data, traceability, etc.) and have been adjusted to suit instant issuing (need to secure remote personalisation devices, access controls for these devices, protection of communication networks, etc.). These recommendations and requirements will of course be modified to reflect market practices and needs.

---

7 A VPN consists in setting up a network that is isolated through a logical process, using a technique known as tunnelling.

8 The SSLv3 protocol is used to provide security for applications.

1|3 Conclusion

The different stages of the personalisation process, which are highly sensitive, are inherently harder to protect when they are performed at numerous, widely accessible points of sale (branches and shops), than when they are carried out in personalisation centres, which handle industrial volumes and have access to significant security resources.

According to information gathered by the Observatory from representatives of issuers, card manufacturers, personalisation centres and technical providers, the physical and logical security measures put in place during the different stages of instant issuing provide satisfactory coverage of the risks associated with these activities. These measures will have to change further to reflect the rise of instant issuing among four-party cards, in order to take into account the special requirements associated with protecting sensitive data contained on card chips.

To date, no instances of compromise involving instant issuing systems have been detected, according to feedback from specialists. However, the Observatory urges those concerned to continue to pay close attention to the security of these systems and to constantly adjust security levels to reflect changing risks.

2 | FRAUD STATISTICS FOR 2008

The Observatory for Payment Card Security has compiled fraud statistics for three-party and four-party cards since 2003, using data collected from issuers and merchants. The statistics use harmonised definitions and typologies that were established in the Observatory's first year of operation and that are provided in Annex D to this report. A summary of the 2008 statistics is presented below. It includes an overview of the different fraud trends for three-party cards and four-party cards, fraud trends for domestic, international, face-to-face and card-not-present transactions, as well as payment and withdrawal transactions, and fraud trends involving lost or stolen cards, intercepted cards, forged or counterfeit cards, and appropriated card numbers. In addition, Annex C to this report presents a series of detailed fraud indicators.

Box 2 – Fraud statistics: respondents

In order to ensure the quality and representativeness of its fraud statistics, the Observatory gathers data from all issuers of four-party and three-party cards. It supplements these data with statistics compiled by France's e-commerce and distance selling federation (Fevad) from a sample of 33 companies that account for 38% of revenues in distance selling to retail customers.

The statistics calculated by the Observatory thus cover:

– EUR 412.9 billion in transactions in France and in other countries made with 58.2 million four-party cards issued in France (including 1.3 million electronic purses);

– EUR 26.8 billion in transactions primarily in France with 27.2 million three-party cards issued in France;

– EUR 24.4 billion in transactions in France with foreign three-party and four-party cards.

Data were gathered from:

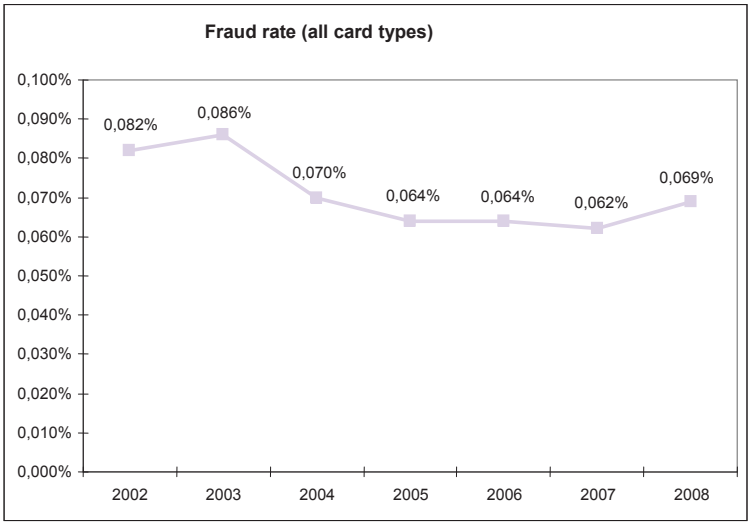
– Ten three-party card issuers: American Express, Banque Accord, BNP Paribas Personal Finance, Cofidis, Cofinoga, Diners Club, Finaref, Franfinance, S2P and Sofinco;

– The 146 members of the "CB" Bank Card Consortium. The data were collected through the consortium, and international data were obtained from MasterCard and the Carte Bleue Group;

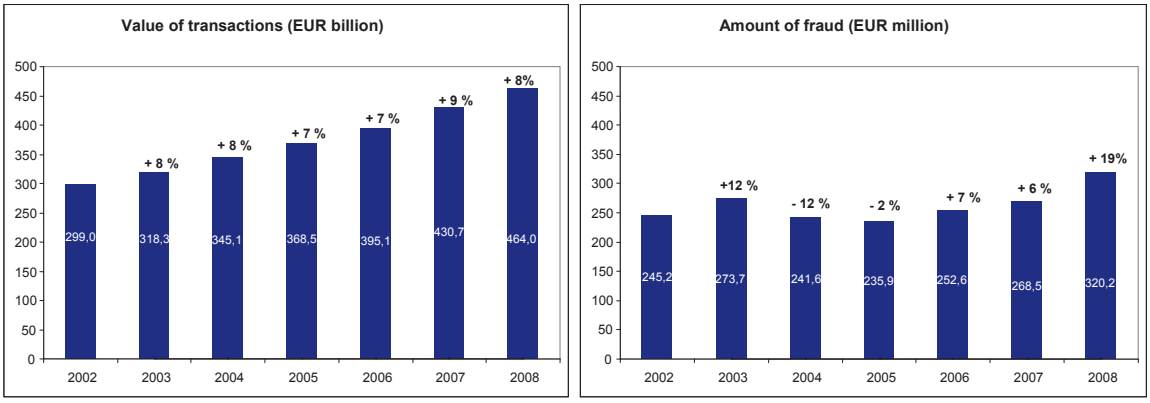
– Issuers of Moneo, an electronic purse.

2|1 Overview

The overall fraud rate for card payments and withdrawals recorded by French card schemes in 2008 stood at 0.069%, an increase on previous years (0.062% in 2007 and 0.064% in 2006 and 2005 – see Table 1). This was because the overall increase in the amount of fraud (19.3%, from EUR 268.5 million in 2007 to EUR 320.2 million in 2008) exceeded growth in the value of transactions, which climbed 7.7% from EUR 430.7 billion in 2007 to EUR 464.0 billion in 2008 (see Table 2). The average amount of a fraudulent transaction was stable, at EUR 131 compared with EUR 130 in 2007.



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



Source: Observatory for Payment Card Security

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

The rate of issuer fraud, which is the total of fraudulent payments and withdrawals made in France and in other countries with cards issued in France, increased to 0.057% in 2008, up from 0.049% in 2007. Issuer fraud thus totalled EUR 249.2 million, compared with EUR 199.8 million in 2007.

The rate of acquirer fraud, which is the total of fraudulent payments and withdrawals made in France with all French and foreign cards, rose slightly to 0.045% in 2008 (corresponding to a value of EUR 201.9 million) from 0.044% in 2007 (EUR 183.2 million).

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

2|2 Breakdown of fraud by card type

	Fraud rate (Fraud amount, EUR million)				
	2004	**2005**	**2006**	**2007**	**2008**
Four-party cards	0.069% (224.1)	0.064% (218.8)	0.065% (237.0)	**0.063%** (253.6)	**0.070%** (304.3)
Three-party cards	0.082% (17.5)	0.067% (17.1)	0.052% (15.6)	**0.052%** (15.0)	**0.054%** (16.0)
Total	0.070% (241.6)	0.064% (235.9)	0.064% (252.6)	**0.062%** (268.5)	**0.069%** (320.2)

Source: Observatory for Payment Card Security

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

The fraud rate for four-party cards was up in 2008, climbing to 0.070%, which corresponds to fraud of EUR 304.3 million, compared with 0.063% in 2007 (EUR 253.6 million). Issuer and acquirer fraud rates for this type of card stood at 0.057% and 0.046% respectively, compared with 0.049% and 0.044% respectively in 2007. The average value of a fraudulent transaction was EUR 127, compared with EUR 125 in 2007.

The fraud rate for three-party cards increased slightly to 0.054% (corresponding to fraud of EUR 16.0 million) from 0.052% in 2007 (EUR 15 million). Issuer and acquirer fraud rates for this type of card were 0.046% and 0.042% respectively, compared with 0.044% and 0.046% respectively in 2007. The average value of a fraudulent transaction was EUR 357 in 2008, compared with EUR 432 in 2007.

2|3 Geographical breakdown of fraud

	Fraud rate (Fraud amount, EUR million)				
	2004	**2005**	**2006**	**2007**	**2008**
Domestic transactions	**0.033%** **(103.9)**	**0.029%** **(97.8)**	**0.031%** **(109.6)**	**0.029%** **(114.5)**	**0.031%** **(130.9)**
International transactions	**0.417%** **(137.7)**	**0.408%** **(138.1)**	**0.362%** **(143.0)**	**0.368%** **(154.0)**	**0.427%** **(189.4)**
o/w French issuer and foreign acquirer	0.463% (55.2)	0.458% (64.1)	0.453% (76.4)	0.476% (85.3)	0.594% (118.3)
o/w foreign issuer and French acquirer	0.391% (82.5)	0.373% (74.1)	0.295% (66.5)	0.288% (68.7)	0.291% (71.0)
Total	**0.070%** **(241.6)**	**0.064%** **(235.9)**	**0.064%** **(252.6)**	**0.062%** **(268.5)**	**0.069%** **(320.2)**

Source: Observatory for Payment Card Security

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

The geographical breakdown of fraud still shows a discrepancy between domestic and international transactions. The latter account for 59% of fraud, even though they make up barely 10% of the value of card payments handled by the French schemes.

As domestic transaction amounts showed sustained growth of 7.9%, the fraud rate for such transactions increased slightly to 0.031% in 2008 from 0.029% in 2007, thus remaining at a very low level.

The rate and amount of fraud involving international transactions both increased in 2008. The fraud rate for foreign transactions using cards issued in France increased sharply, reaching 0.594% (corresponding to fraud of EUR 118.3 million), compared with 0.476% (EUR 85.3 million) in 2007. The fraud rate for transactions in France using cards issued in other countries rose slightly to 0.291% (corresponding to fraud of EUR 71.0 million), compared with 0.288% (EUR 68.7 million) in 2007.

Box 3 – Breakdown of losses from fraud

In 2008, as in 2007, the Observatory estimated indicators for the distribution of losses from fraud between cardholders, merchants and banks. These overall indicators cover all three-party and four-party schemes. It is important to note that they apply only to the losses themselves, not to the total processing and insurance costs generated by fraud. The indicators show a trend, but remain theoretical and reflect only the direct breakdown of losses between participants, because they are constructed to refer to the legal and regulatory provisions governing the procedures for blocking lost or stolen cards and for disputing fraudulent card payments. In addition, they cannot capture all the commercial practices of issuers and acquirers.

Taking all schemes into account, losses from fraud in domestic transactions were distributed as follows in 2008: 2.6% for cardholders, 43.9% for issuers and acquirers, and 53.5% for merchants, mainly in distance selling. The portion borne by merchants increased significantly (from 46% in 2007) owing to growth in fraud involving card-not-present payments, an area where merchants bear most of the losses.

Furthermore, out of the EUR 320.2 million in fraud recorded by the French schemes in 2008, it is estimated that foreign schemes bore EUR 96.0 million, or 30%. This is attributable to the application of international liability-sharing rules as part of the implementation of the EMV standard and the 3D-Secure authentication mechanism for card-not-present payments.

2|4 Breakdown of fraud by transaction type

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

Domestic transactions

	Fraud rate (Fraud amount, EUR million)				
Domestic transactions	**2004**	**2005**	**2006**	**2007**	**2008**
Payments	**0.036% (81.2)**	**0.033% (82.8)**	**0.035% (92.3)**	**0.032% (95.6)**	**0.036% (111.7)**
- o/w face-to-face and UPT	0.029% (63.5)	0.025% (59.2)	0.024% (59.1)	0.017% (45.4)	0.015% (44.5)
- o/w card-not-present	0.177% (17.7)	0.196% (23.6)	0.199% (33.2)	0.236% (50.1)	0.252% (67.2)
- o/w by post / phone	na	na	0.194% (19.8)	0.201% (23.8)	0.280% (28.5)
- o/w online	na	na	0.208% (13.4)	0.281% (26.4)	0.235% (38.8)
Withdrawals	**0.027% (22.7)**	**0.017% (15.0)**	**0.019% (17.4)**	**0.020% (19.0)**	**0.018% (19.1)**
Total	**0.033% (103.9)**	**0.029% (97.8)**	**0.031% (109.6)**	**0.029% (114.5)**	**0.031% (130.9)**

Source: Observatory for Payment Card Security

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

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

– the fraud rate for face-to-face and UPT payments continued to fall, declining to 0.015% (corresponding to fraud of EUR 44.5 million), compared with 0.017% (EUR 45.4 million) in 2007, reflecting efforts over recent years to strengthen cryptographic systems. Face-to-face and UPT payments accounted for 69% of domestic transactions, and 34% of fraud in value terms.

– the fraud rate for card-not-present payments rose in 2008 to 0.252% (corresponding to fraud of EUR 67.2 million), compared with 0.236% in 2007 (EUR 50.1 million). Card-not-present payments thus accounted for 6% of the value of domestic transactions but for 51% of fraud in value terms. This increase needs to be seen in the context of substantial growth in the volume and value of card-not-present payments (25.6% between 2007 and 2008).

  A comparative analysis of payments by post or phone compared with online payments shows that the trend in fraud rates for these two channels has reversed. Fraud increased by more among online payments than among post/phone payments (47.0% compared with 19.7%), but the fraud rate for post/phone transactions was higher because of the sharp decline in the amount of such payments (-14.0%). Since the increase in the amount of online payments exceeded the increase in fraud, the fraud rate for such transactions fell to 0.235% (down from 0.281% in 2007).

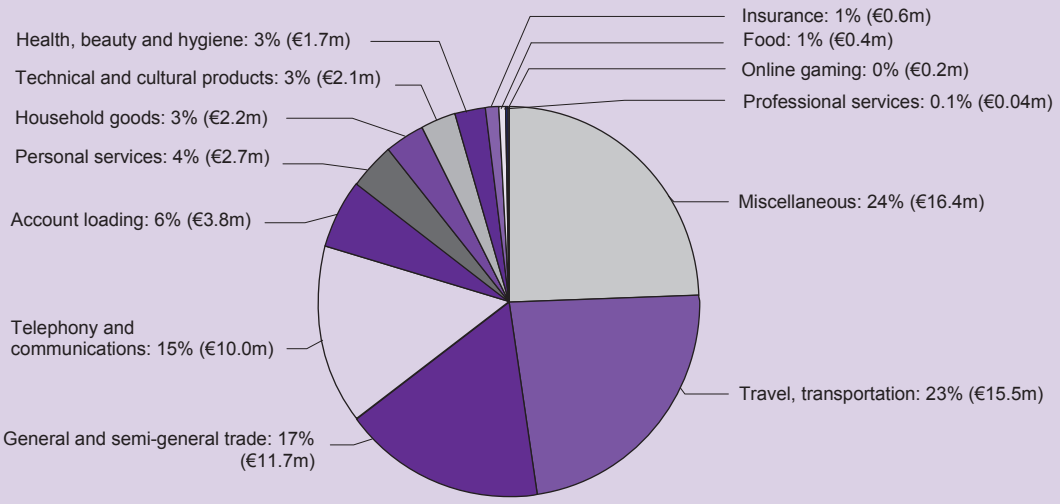
  Fevad's statistical analyses corroborate data gathered by the "CB" Bank Card Consortium on this point.

  The Observatory pays close attention to developments in fraud relating to card-not-present payments. Chapter 3 of this report includes a study of security solutions.

– the fraud rate for cash withdrawals fell to just 0.018% (corresponding to fraud of EUR 19.1 million), after 0.020% (EUR 19.0 million) in 2007. Withdrawals represent 25% of domestic transactions and account for 15% of the total fraud amount.

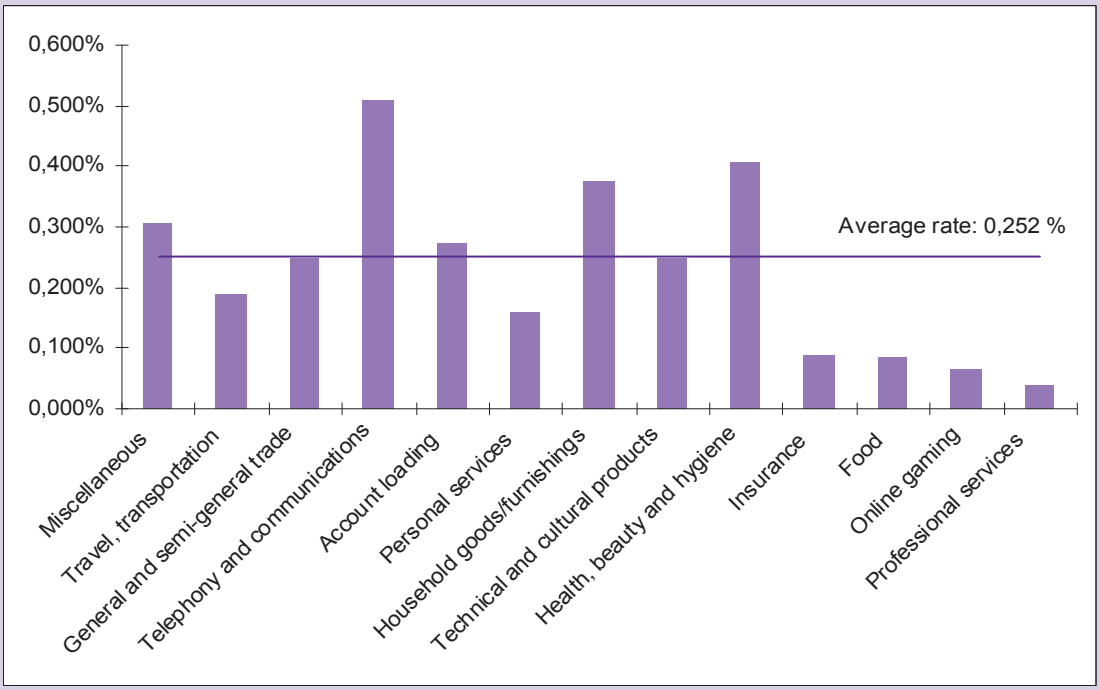
Box 4 – Domestic fraud in distance selling, by sector of activity

For the first time this year, the Observatory has gathered data that provide information about the distribution of fraud in card-not-present payments by sector of activity. These data cover domestic transactions only.



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

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



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

Source: Observatory for Payment Card Security

International transactions

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

Source: Observatory for Payment Card Security

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

In the case of international transactions, the Observatory has a detailed breakdown of fraud by transaction type only for transactions by French cards in other countries. The main finding regarding such transactions is that fraud for card-not-present payments increased sharply (91.5%, corresponding to fraud of EUR 67.2 million). The fraud rate for these payments reached 1.698%, the highest ever recorded by the Observatory. This significant change underlines the importance of implementing security measures to ensure that payments are made by the lawful cardholders.

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;

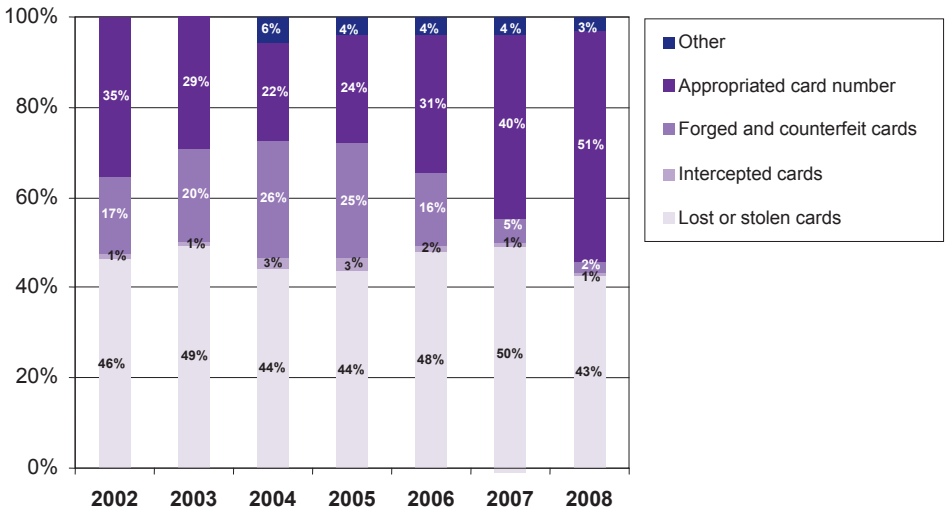
– Intercepted cards stolen when issuers mail them to lawful cardholders;

– 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 (which use programs to generate random card numbers) and then used for card-not-present transactions;

– "Other" fraud, which covers, particularly for three-party cards, fraud resulting from the fraudulent opening of accounts with a false identity.

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



Source: Observatory for Payment Card Security

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

Fraud involving the use of appropriated card numbers for fraudulent card-not-present payments has been on the increase since 2005 and is now the most common type of fraud (51.3%, compared with around 40% in 2007). Fraud involving lost or stolen cards accounted for 42.6% of fraudulent domestic payments. Counterfeit cards accounted for just 2.4% of fraudulent domestic payments, down from 5% in 2007 and 16% in 2006. "Other" fraud was stable. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for some 50% of the fraud involving these cards.

2008	All types of cards		Four-party cards		Three-party cards	
	Amount (EUR million)	Share	Amount (EUR million)	Share	Amount (EUR million)	Share
Lost or stolen cards	55.8	42.6%	53.4	43.4%	2.4	30.1%
Intercepted cards	0.9	0.7%	0.3	0.3%	0.6	6.9%
Forged or counterfeit cards	3.1	2.4%	2.6	2.1%	0.5	6.5%
Appropriated numbers	67.2	51.3%	66.6	54.2%	0.6	7.9%
Other	3.9	2.9%	-	-	3.9	48.6%
Total	**130.9**	**100%**	**122.9**	**100%**	**7.9**	**100%**

Source: Observatory for Payment Card Security

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

Box 5 – Indicators provided by law enforcement agencies

In 2008, law enforcement agencies noted a slight decline in the number of payment card fraud cases, recording 54,058 instances of payment card counterfeiting and use. In all, 3,719 individuals were charged and 1,430 suspects were detained.

Attacks on automated teller machines (ATMs) were up, with 427 such attacks registered in 2008, compared with 391 in 2007, 515 in 2006, 200 in 2005 and 80 in 2004. There were also three attacks on card-operated fuel pumps (compared with 36 in 2007), and 17 attacks on payment terminals.

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

– the arrest of a nine-person ring specialised in capturing card data, counterfeiting and using cards in France and several other European countries. Losses attributable to the ring are estimated at over EUR 500,000;

– the dismantling of payment card counterfeiting production sites, which included the seizure of equipment (computers, embossing and thermal printing devices), thousands of counterfeit cards and tens of thousands of euros in stolen funds.

In 2008, French law enforcement agencies continued to cooperate closely with their opposite numbers elsewhere in Europe, particularly in Eastern Europe. This included initiatives that led to the closure of criminal production sites in France and Romania. These actions are needed to fight effectively against fraud amid the rise of organised groups and cross-border crime.

3 | TECHNOLOGY WATCH

3|1 Security solutions for card-not-present payments

Distance selling in the broad sense, i.e. including online as well as mail order/telephone order (MO/TO) sales, has increased considerably in recent years in France, driven particularly by the rise of online selling (or electronic commerce). The value of online sales grew by 25% in 2008, according to the French e-commerce and distance selling federation (Fevad). At the same time, payment cards are now the most popular means of payment for online purchases, accounting for 85% of payments in 2008[9].

Given the specific nature of security measures implemented for card-not-present payments as compared with face-to-face payments, and in the light of the different fraud rates shown for these two types of payment in the Observatory's statistics, the Observatory decided to conduct an examination of the security solutions implemented for online and MO/TO card-not-present payments.

Security characteristics of card-not-present payments

Card-not-present transactions differ considerably from face-to-face payments in terms of the checks that are carried out.

At present, the vast majority of card-not-present payments are based exclusively on the provision of a set of static and hence reusable data, including the card's primary account number (PAN), expiry date and security code (Card Verification Value 2 in the case of Visa, Card Verification Code 2 in the case of MasterCard). Holder authentication is not usually part of the process.

These data could therefore have been intercepted by another party or appropriated by an unscrupulous person working in the payment chain. Furthermore, the holder could deny authorising the payment.

In addition, card-not-present payments do not usually include definite authentication and a record of evidence that the cardholder consented to the transaction. The merchant could therefore bill more than the agreed amount, and the holder could deny authorising the debited amount.

However, merchants and service providers can ensure that the card has not been reported lost or stolen and that the maximum payment amount is not exceeded.

Once a payment order is received, whether by internet, mail or phone, the merchant generally records the card data in its information system. To protect against the risks of card data being

9 Source: Fevad

stolen, as has happened in recent years, particularly in the USA, these files have to be specially protected.

Owing to the limitations in terms of checks on card-not-present payments, the fraud rate for such payments is much higher than that for face-to-face and UPT payments, and stood at 0.252% in 2008, compared with 0.015% for face-to-face and UPT payments. This, combined with the increase in card-not-present payments, has led to a jump in the value of fraud for card-not-present payments, which rose from EUR 50.1 million in 2007 to EUR 67.2 million in 2008. Accordingly, card-not-present payments, which account for 6% of domestic transactions in value terms, are responsible for 51% of the total amount of fraud.

Security solutions

Detection of suspicious transactions, Insurance

To combat fraud, merchants and banks increasingly use systems to detect suspicious transactions, carry out additional checks and reject certain transactions. These systems, which are reported to France's National Data Protection Authority (CNIL), are based on an analysis of the customer's behaviour, the place from which the order originated, and a comparison of the customer's purchases with several merchants to assess the probability that the transaction might be fraudulent. These systems have been adapted to cope with dynamic card numbers.

These systems may be backed up by insurance or guarantee arrangements. Holders, meanwhile, are protected by law if their card number is fraudulently used and may also take out insurance to provide protection against delivery failures.

Anti-theft protection for static card data

As long as it remains possible to make card-not-present payments using static data, it will be necessary to protect the confidentiality of such data. These data can be captured and misappropriated in several places: while in transmission, during storage in databases, or from the holder's computer (in the case of online transactions).

Card data can be captured during transmission regardless of whether they are conveyed over the internet, by mail or by phone. However, the main problems concern online transmission, where a large amount of data can be automatically and thus easily captured. For this reason, these data are always sent using a secure solution such as HTTPS, an effective protocol that has been used for years by online merchants. HTTPS's only weakness is that its security depends on proper authentication of the merchant's site by the customer, but this is an area that is open to attack by various techniques, including phishing. Educating internet users and doing additional work on interface aspects would make it easier to identify genuine and fake sites. An example of such a solution is the “Extended Validation Certificate”, which is sent to the site following additional checks and tells the online user through visual indicators (e.g. the address bar goes green) that he or she is on a site that has undergone a stricter vetting process.

The risk that card data could be captured from merchants' or financial intermediaries' databases necessitates strict controls on the security of these databases. This is why the international networks have adopted a programme like the Payment Card Industry - Data Security Standard (PCI DSS) to draw up rules for protecting card data, use and storage. The PCI DSS applies directly to merchants and their payment system hosts, setting out the security requirements that they must satisfy. Enforcement may be audited at the request of the international networks. In France, the programme will have to be adjusted to suit the specifics of using smart cards.

Card data are increasingly being taken from cardholders' computers owing to the spread of spyware. Given this situation, steps are being taken to tell cardholders about best practice in terms of computer security and to provide them with secure systems.

Use of dynamic card data

Rather than trying to protect card data against theft because they can be reused, another solution is to replace static data with one-time dynamic data. These numbers can be used online as well as by MO/TO.

A card number is said to be dynamic if it is associated with a single payment and cannot be reused. The technical difficulty involved in implementing such a solution concerns the confidential provision of one-time PANs to users by issuing banks. When a dynamic number is issued online, the holder must first be authenticated.

Holder authentication and consent

To prevent the fraudulent use of card data, measures can be introduced to authenticate the holder and validate consent for each payment order.

Holder authentication systems

In four-party schemes, the holder's consent and authentication are ensured in face-to-face payments as follows: the billed amount is displayed on a screen to the holder, who then enters his or her PIN, in accordance with the EMV standard[10]. This type of approach requires a payment terminal and is therefore unsuited to card-not-present payments, whether made on French sites with domestic or foreign cards, or on foreign sites using French cards.

Currently, the most commonly used authentication measure for online or MO/TO distance selling is to check a static piece of information, say a password or personal information such as the person's date of birth. This solution has the advantage of being simple and cheap to introduce and easy to use.

However, if holder authentication is based on static data, card-not-present payments are still vulnerable to the attacks mentioned above, i.e. online capture of passwords through phishing, spyware, etc. To respond to this threat, a number of technical solutions are possible, some of which are offered by banks to certain customers. These include:

– one-time codes sent on a paper card. There is a danger that this card could be stolen or copied, although the risk can be mitigated if several combinations known only to the holder are needed to use the card to enter the one-time code;

– one-time codes generated by the issuing bank's server and sent to the holder by phone (SMS or voice mail to fixed line). This approach has the advantage of using different communication channels, since the code is sent by a different channel from that used to place the order.

– one-time codes provided by a hardware device, such as the Chip Authentication Protocol (CAP) / Dynamic Passcode Authentication (DPA) solution used with four-party cards. Under this approach, the payment card generates a one-time code when inserted into a small

[10] However, the PIN cannot be checked in the case of payments made at French merchants with foreign four-party cards that function in magnetic stripe mode.

separate reader on which the holder types his or her PIN. This solution has the added advantage of being able to generate codes that are associated with the transaction to be validated. This prevents the characteristics of the transaction from being altered, as well as subsequent disputes.

Work is being done to enable this type of solution to be used not only for online purchases, as is currently the case, but also for MO/TO.

Architectures for authentication systems

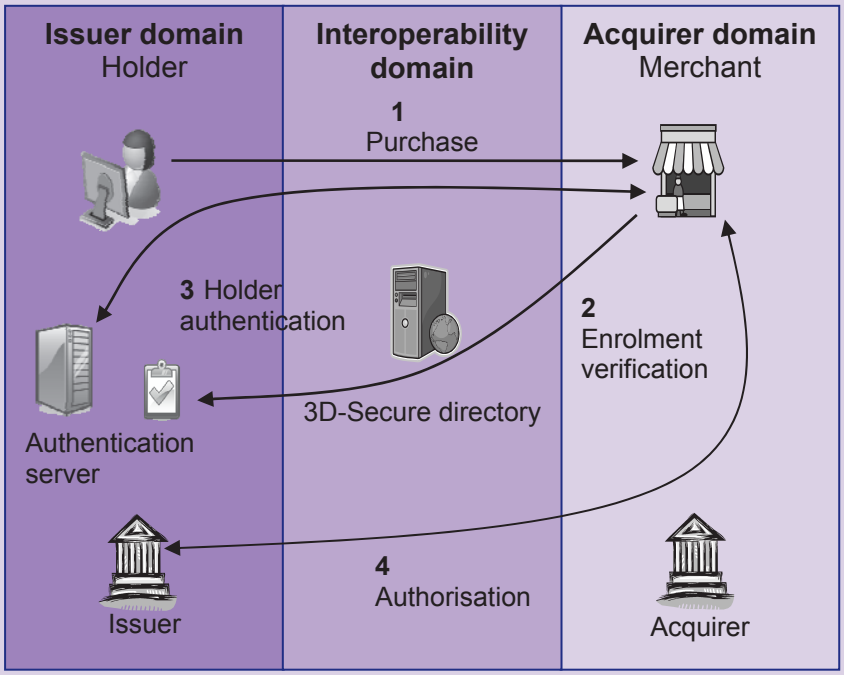
While the use of holder-activated systems protects the individual against unlawful use of his or her card and provides an additional guarantee to merchants for these protected purchases, broader use of holder authentication based on interoperability standards would help in the fight against fraud.

As regards online selling, four-party card payment schemes have introduced a common architecture that allows merchants to request holder authentication and banks to provide customer authentication data. One example of this kind of solution is "3D-Secure"[11] which, following a request by the merchant's server, makes it possible to contact the holder's bank, authenticate the cardholder, get his approval regarding the terms of the transaction (e.g. amount, etc.) and prepare a record or certificate to evidence the customer's transaction. The bank chooses the authentication method, which may be the same as the method used for online banking.

Given the internet's global scope, 3D-Secure's success will depend on its widespread introduction by card payment schemes. In France, acquiring banks in the "CB" Bank Card Consortium are gradually deploying this system among merchants. The consortium's issuing banks have also introduced holder authentication mechanisms. On 1 October 2008, liability was shifted among the banks in the "CB" scheme. As a result, when a merchant is the victim of a fraudulent payment, and the transaction was processed using 3D-Secure with the issuer, it is the issuer that is now liable, no longer the acquirer and, ultimately, the merchant.

[11] 3D-Secure is an industry communication protocol linking the merchant, the acquiring bank and the issuing bank. Developed by Visa to enhance the security of online payments, it is offered to clients under the name "Verified by Visa". Services based on the protocol are offered by MasterCard under the name "MasterCard SecureCode", and by JCB International as "J/Secure".

Box 6 – 3D-Secure: how it works



Conclusion

Fraud in card-not-present payments not only considerably exceeds that of face-to-face and UPT payments, it is also on the rise. For this reason, the Observatory decided to build on work done in 2007 and extend its study on the security of card-not-present payments.

The peculiarities of card-not-present payments preclude the direct application of the security solutions employed to protect face-to-face payments. However, specially-adapted solutions are now available and are being used, at least in the case on online sales. These include, for example, dynamic card numbers and password-based holder authentication.

But current solutions do not address all the risks for card-not-present payments, which notably include the capture of card data and static authentication information. The Observatory therefore recommends that security methods be strengthened to bring security for card-not-present payments up to the levels provided for face-to-face and UPT transactions.

Accordingly, to complement authentication by the holder of the merchant's site, the Observatory recommends placing more emphasis on card-not-present payment methods that enable the holder to be authenticated. It recommends gradually introducing holder authentication for all payments and stepping up current authentication methods, so that the merchant can be confident that both card and holder are authentic and that the cardholder has given his consent. To help protect against the risks, the Observatory strongly recommends implementing dynamic holder authentication wherever possible and appropriate. Card payment schemes and their issuers can already choose from a range of available technical solutions, including one-time codes generated by calculator or sent by SMS, and stand-alone EMV card readers. To make it easier to use these solutions, it is important that deployment costs are kept under control and

that appropriate user interface choices are made. Roll-out must be accompanied by measures to inform and educate cardholders.

The introduction of such systems concerns everyone. Accordingly, the Observatory calls on all participants to get involved.

3|2 Impact of co-branding on payment card security

Co-branding of payment cards consists in associating the card with one or more commercial partners' brands in addition to the brand of the issuing institution. It is different from co-badging, which is where an issuer enters into a partnership with various card networks and includes their logos on its cards (CB, Visa, MasterCard, Moneo, etc.).

Co-branding has been around for a long time. Widely used in some Anglo-Saxon countries, it has led to the rise of numerous affinity card offers, so called because they are used to reach holders who have special ties to one or more of the issuer's partners, which might include chains of restaurants, hotels or fuelling stations. Co-branding has been used in the past by three-party cards in France, but the technique has seen relatively little growth until recently because it was not allowed in the “CB” system, whose members wanted to give their cards a neutral and universal quality and maintain strong ties between the cards and their issuing banks. The ban was lifted on 1 October 2007 to align French practices with those in neighbouring countries as part of the Single Euro Payments Area (SEPA) project.

Since then, a number of new co-branding projects have got underway, with around 50 new card offerings now available, ranging from debit cards with an affinity programme to debit cards with a line of consumer credit, and prepaid reloadable cards.

This new development has raised a number of questions, particularly among consumer representatives. One area of concern, which lies is outside the Observatory's remit, is the possibility of confusion among cardholders about debit and credit payment functions. Another question is whether issuing institutions are maintaining control over security for co-branded cards. The Observatory thus decided to examine if these innovations were likely to affect security and whether the security for these new payment card offerings was satisfactory.

Possible changes in terms of security

Co-branding could affect practices over the various stages of the payment card lifecycle. While co-branding primarily means a change to the card's appearance and affinity offers, partners may also play an active role in card subscription and issuance. Moreover, the way that affinity offers work means that customers' private data will be shared between the issuer and its partners. Also non-bank applications may be added to the customer's card.

Subscription

The card subscription process involves the provision by the holder of a set of private and bank data, verification of supporting documentation and signature of an agreement. In the case of co-branded cards, the application for a card may be made either to the issuer or to its commercial partner.

In the first case, the procedures are the same as for non co-branded cards. However, the issuer and its partners may share holders' personal information and bank data. This may result in partners holding sensitive databases, which will require appropriate protection.

If an application for a card is submitted to a commercial partner, then that partner must collect the customer's personal data. These data must consequently be protected in the same way as when they are collected in the banking environment to ensure confidentiality, especially when they are being stored or transmitted to the issuer or its technical provider. If the partner is responsible for some or all of the process of verifying the customer's personal data, these activities must be carried out to the same standard of due diligence as in the banking environment, notably in order to ensure the truthfulness of information collected.

Issuance

Issuers or issuer-supervised technical providers manufacture and personalise most of the co-branded cards issued today in France. The issuer, or the provider acting on its behalf, then issues the cards directly to holders. These manufacturing operations are sensitive from a security perspective, notably because of the importance of protecting private and bank data during the personalisation phase. Protecting the card and security data, such as the PIN, is also especially important when sending the card to the holder. The involvement of a commercial partner in the card issuance phase could affect the order in which these operations take place, but from a security perspective, it is important that co-branded cards, like all payment cards, be subject to an issuance process that incorporates measures that ultimately deliver the same level of security as during the issuance of bank cards that are not co-branded.

In the case of three-party cards, which are currently stripe cards in France, some co-branded cards are issued instantly at the point of sale (instant issuing). This practice is also poised to see more use among four-party cards. To prevent the risk of criminals unlawfully obtaining cards, appropriate controls must be in place for instant issuing (see Chapter 1 of this report).

Use

Co-branding allows payment cards to be used in a wider range of ways. It also means a change in the way they look, since the partner's brand, logo and communication and other commercial information may appear on the card. In the future, the shape of cards may also change (e.g. cutaway style, mini format). By giving cards an unusual and even playful look, these changes might make holders think differently about the banking functions of their payment instrument. Communication and awareness-raising efforts are therefore needed to ensure that holders are properly informed that they must take the same precautions with co-branded cards as with any other payment card.

Moreover, these cards may also contain affinity applications alongside banking ones. It is important that the former do not compromise the security of the latter and associated data. For this, they must comply with the card's security policy (e.g. strict separation between applications).

Security measures

Protection of bank data

It is important that card data (PAN, expiry date, CVx2) are properly protected by the issuer and its partners during storage and transmission. Issuers of co-branded cards must make sure that their partners comply with the security requirements that apply in this area.

An example of a set of common requirements for card data protection is the Payment Card Industry - Data Security Standard (PCI DSS) programme, which has now been adopted in France, with adjustments to reflect the chip and PIN (i.e. not stripe) approach of four-party cards. French issuers of four-party and three-party cards, their technical providers and their commercial partners are therefore implementing these security requirements, including for co-branded cards.

Another good practice implemented by issuers consists in avoiding the use of private data outside the production IT environment, for example by transforming them into anonymous data in testing.

Issuance security

For the time being, in France, issuers mainly have control over the issuance of co-branded cards. Issuers are therefore in a position to ensure that this sensitive process is subject to the same security standards as apply to non co-branded cards.

Long used solely to renew lost or damaged stripe cards without changing the PIN, point of sale instant issuing is to become extended to include initial card issuance, including of smart cards. This process carries more risk and needs to be properly managed, notably to ensure the secure management of stored cards and sensitive data used in card personalisation (cf. Chapter 1).

Card security

To prevent the risk of co-branded cards being treated lightly, and to underline their status as payment cards, the issuers of co-branded cards must put their logo on the front or back of such cards, and require their commercial partners to communicate clearly the fact that their cards are payment cards. Furthermore, because the card issuer retains ownership and total liability for the card, it is important that the issuer should remain the contact point for the holder, who can thus be confident that the card enjoys the same level of protection as a non co-branded card.

To guarantee the security of multi-function cards, it is necessary to keep the different applications separate. This can be achieved by selecting cards that are designed for this purpose. The “CB” Bank Card Consortium publishes a catalogue of approved cards that provide an adequate level of security for this type of use.

Conclusion

Co-branding of payment cards consists in associating the card with one or more commercial partners' brands in addition to the brand of the issuing institution. It is a popular technique in many countries, but until recently was only used in France by three-party schemes. On 1 October 2007, the “CB” Bank Card Consortium authorised the practice for “CB” cards,

following recommendations relating to the introduction of the Single Euro Payments Area (SEPA).

Since then, there has been a flurry of co-branding initiatives in France, raising concerns among consumers about whether issuing institutions are maintaining control over co-branded cards. For this reason, the Observatory carried out an examination to see whether these new developments were likely to affect security and whether security for the new payment cards was satisfactory.

Co-branding of a payment card may lead the issuer's commercial partner to handle some or all card subscription and issuance processes, or to share the cardholder's private information or bank data with the issuer.

The Observatory found that the projects currently being taken forward in France had implemented security measures that addressed the potential risks. It recommends that whenever issuers introduce a new card, they should make sure to fully implement the security measures currently in effect in the payment card environment for the collection, storage and management of sensitive data.

As part of these developments, cards may also carry several applications, such as a commercial partner's affinity application alongside the bank payment application. It is important to have complete control over the security of sensitive data. Furthermore, if the card does hold several applications, checks must be carried out to make sure that none of them compromises the security of the payment application. If several applications are carried on the same card, the Observatory recommends that issuers select cards that can deliver a proven and recognised level of protection for the payment application.

3 | 3 Security of UPT networks

Unattended payment terminals (UPTs) are acceptance devices that allow the cardholder to make a payment by him or herself, without the involvement of any other person. To use such machines, acceptors have to set up a network infrastructure that connects several UPTs by using devices that can concentrate transaction flows on the UPTs and then send them to the acquiring bank's server. Yet the nature of these networks is changing with the use of new communication techniques, including IP[12], Wifi[13] and GPRS[14]. Furthermore, while standards and networks used in the past were held and controlled by the incumbent phone operator, new so-called open networks are now becoming more widespread. These new networks are not used solely for payments and controlling their security is more complex because they involve more participants.

Accordingly, the Observatory decided to extend its 2006 studies on the use of open networks in the payment card environment[15], and on the security of UPTs[16], to examine what challenges changes in the types of network used pose to the security of UPT networks.

---

12 Internet Protocol, standard communication protocol on which the internet is based.

13 Wifi is a wireless computer networking technique that is used to access high-speed internet services.

14 General Packet Radio Service (GPRS) is a data-oriented communication protocol used in mobile telephony. It operates on GSM networks and allows faster data throughput.

15 Cf. 2006 Annual Report of the Observatory, pp. 23 to 28.

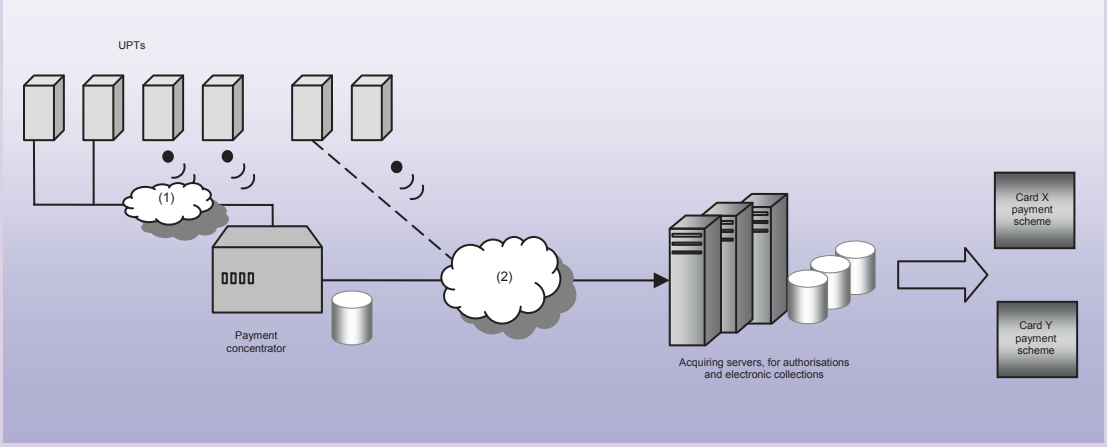
16 Cf. 2006 Annual Report of the Observatory, pp. 28 to 35.

Characteristics of UPT networks

There were around 60,000 UPTs in France in 2008, set up by merchants to meet specific automated distribution needs for products and services such as fuel, transportation tickets, tolls, car parks, DVDs, drinks, bicycle rental, and so on. These terminals usually accept four-party and some three-party cards. Some UPTs also accept electronic purses.

UPTs are set up in network infrastructures using different types of equipment, communication protocols and participants. The following diagram describes the basic structure.

Box 7 – Basic structure of UPT networks



UPTs installed on the merchant's premises, such as, for example, automated fuel pumps at a fuelling station, are generally connected to an aggregating device known as the payment concentrator, which receives data about payment transactions conducted on the terminals and provides the link to the acquiring server(s). The server then sends authorisation requests and electronically collected data to the relevant card payment scheme(s).

Some variants occur in terms of the implementation of network architectures. The UPT may for example connect to a local access point or to a remote provider that is in charge of relaying the data to the acquiring servers.

This study looks at networks that link UPTs to concentrators (shown as (1) on the diagram) and concentrators to acquiring servers (shown as (2) in the diagram), as well as the case where UPTs bypass a concentrator to access acquiring servers (shown as the dotted line in the diagram). The study does not consider networks that link acquiring servers to card payment schemes.

UPT networks use a range of devices that enable various participants to process and exchange payment transaction data, including:

– the accepting merchant;

– the acquiring bank;

– the technical or service provider(s) handling some or all of the management of communication networks and devices.

The devices used to process data are mainly computer servers running a so called “embedded” operating system, i.e. an installed operating system that is either derived from a standard system such as Microsoft Windows or Linux and specially customised to suit the functions of the device, or a specially-developed proprietary system.

A variety of communication techniques can be used to transmit payment data, based on different types of hardware and communication protocols. Generally, two main sorts of techniques are used to connect devices: wired (cable, fibre optic) or wireless (radiocommunication methods such as Wifi and GPRS). Also, the X25 communication protocol, which was widely used in wired networks up to now, is gradually giving ground to the IP protocol, which is the basis for the internet and which is also used in wireless networks.

At acceptors, UPTs and payment concentrators are increasingly connected using wireless techniques (such as Wifi and GPRS), which provide a number of benefits in terms of ease of installation and service coverage.

Concentrators and acquirers are usually connected through an IP link, often with wired devices. In the event that the accepting merchant's terminal is directly linked to the acquiring system, the link is once again typically IP and may be wired or wireless.

Security impact arising from the use of open networks

To protect the network through which UPT management data are transmitted, it is first necessary to protect the device itself, to prevent a criminal from installing hardware or software in order to take control of the communication network to which the terminal is connected. Similarly, measures must be taken to protect the network proper, particularly in the case of open networks.

Protecting hardware

Physical protection

Special attention is paid to ensure that UPTs are not tampered with, including measures to provide physical protection when these devices are handled or maintained by the merchant's staff or maintenance personnel, who are also required to be on the watch for any external modification of these devices. Furthermore, opening an UPT generally deactivates its payment functions, which can only be reactivated by an authorised operator.

Protection for operating systems

The security of installed operating systems is crucial to the protection of UPT networks. Criminals may target these systems, which comprise a suite of functionalities and default settings, seeking to exploit their weaknesses to gain access to a device and so take control of the network. The use of new communication techniques and operating systems based on retail systems could make this kind of attack easier.

For this reason, it is necessary to implement security measures to protect against this risk. One solution is to strengthen the security of operating systems, to optimise security for network devices to reflect the use made of the equipment. This would include doing away with or deactivating unused software components and functionalities that could make a criminal's job easier or be a security weakpoint, and introducing restrictions on accessing certain data. In addition, the default settings should be adjusted to authorise only necessary communications and prevent the device from connecting to the Internet without supervision. The “CB” Bank Card Consortium recommended such measures in 2003 and then updated them in 2008 for ATMs. It would be useful to extend them to all UPTs connected over open networks.

Regular operating system updates can also enhance the level of hardware security. For example, to ensure a more effective response to new fraud threats, it should be possible to introduce security patches securely and remotely, i.e. based on the signature of transmitted items, with verification on the receiving device prior to the update.

Protecting open networks

Impact of using open networks

Changes in the nature of the networks used to connect UPTs have brought more participants into the process. This raises the question of the ownership and control of the techniques used.

Prior to telecommunications deregulation, the networks were owned by one operator and could be accessed only by its personnel. The operator's oversight of the networks and associated equipment provided a degree of security.

Since that time, deregulation and the rise of the internet have fostered the emergence of numerous operators and service providers who run widely interconnected, shared networks. It is becoming harder to protect the confidentiality and integrity of data exchanged on these open networks. Knowledge of communication protocols has also become far more widespread. And increasing use of wireless techniques makes networks easier to access. These networks do not naturally have an end-to-end security system, making it harder to control the security of exchanged data.

The shift from using proprietary networks to using open networks to connect UPTs and concentrators is taking place as UPTs, which may have a service life of up to ten years, are replaced. Dedicated and open networks are therefore currently operating side by side. Networks connecting concentrators to acquiring servers are also starting to use the IP communication protocol.

Given the sensitivity of the transmitted payment data, which include the card's PAN, expiry date, cardholder name and magnetic stripe data (if read) or transaction certificates (for EMV), participants must take security measures to ensure the confidentiality and integrity of these data. Such measures should seek to provide protection against the risk of data being captured or stolen. They should prevent criminals from being able to reuse these data to carry out card-not-present payments or face-to-face transactions in countries that use the stripe method. The measures must also stop intrusions by fraudsters attempting to carry out fake transactions or attack the system.

Security measures

Communication services providers generally deploy security mechanisms that are suited to the communication protocols used and the sort of data exchanged. These mechanisms may be supplemented by requirements on the part of acquiring banks or card payment schemes, which also apply to merchants and their providers.

Measures implemented by merchants

To protect the IP link between UPTs and the merchant's payment concentrator, providers propose two types of security measure: a Virtual Private Network (VPN) or a security protocol such as Secure Socket Layer version 3 (SSLv3) or its equivalent. A VPN consists in setting up a

network that is isolated through a logical process. Data are encapsulated and secured by cryptographic algorithms that ensure confidentiality and integrity, while the hardware used to set up the VPN is also authenticated. The SSLv3 protocol is used to provide security for applications. It operates in client-server mode and handles server authentication (i.e. the concentrator in this case), data integrity and confidentiality (through an encrypted session) and, optionally, authentication of the client (i.e. the UPT).

Additional measures may also be implemented to protect against the risks linked to the use of wireless techniques. Particularly when Wifi is used, certificate-based authentication and encryption measures are generally deployed between the UPT and the wireless station with which it is communicating. Authentication is also possible if GPRS is used. The "CB" Bank Card Consortium recommends encryption for UPTs communicating in GPRS mode.

Measures implemented by the service provider in charge of the communication network

A VPN or SSLv3 is also used to secure the IP link between the concentrator and the acquiring server.

Measures implemented by acquiring banks

Despite the security measures detailed above, the acquiring bank does not have complete control over the security of data exchanged on communication networks, given the many different participants involved and the fact that networks are owned by the providers offering these services. For this reason, acquiring banks set transaction authentication and encryption requirements to ensure end-to-end protection. They also ask merchants and their service providers to apply these security measures to the links between UPTs and concentrators.

The PCI DSS standard prepared by the PCI Security Standard Council, for example, requires that card payment data transmitted over open networks be encrypted to ensure protection.

Even when data transit through a VPN, the "CB" Bank Card Consortium requires end-to-end encryption[17] of transaction data to ensure confidentiality.

Furthermore, the "CB" Bank Card Consortium requires a security protocol such as SSLv3 or equivalent to be used. Within this framework, authentication of the acquiring server (or concentrator) is obligatory and certificate-based. Authentication of the concentrator (or UPT) is also recommended, but not mandatory. This is because in UPT networks, it is the concentrator that calls the acquiring server (and the UPT that calls the concentrator) to transmit transaction data, whereas the acquiring server never calls the concentrator. To ensure a high level of security, the calling device must therefore present a certificate to the called device, but the reverse is not obligatory. In fact, all devices certified to date have been fitted by their manufacturers with an authentication system for the concentrator (or UPT).

To the extent that three-party schemes share hardware with the "CB" system, and particularly acceptors' acceptance devices, they benefit from the security measures developed to meet "CB" requirements.

[17] meaning from the UPT to the acquiring server.

Conclusion

UPTs are generally deployed in network infrastructures, which are characterised by an increasing use of open networks and wireless communication techniques such as GPRS and Wifi. This change in the nature of networks may entail new risks in terms of the physical and logical security of equipment as well as in terms of the confidentiality of processed and exchanged data.

To protect against these risks, merchants, issuers and their service providers implement specific security measures, including the use of VPNs and security protocols. Additional data encryption and hardware authentication mechanisms are also employed, particularly in situations where wireless techniques are used.

The Observatory calls on all participants to work towards the widespread introduction of these data protection measures, which are vital to guarantee the security of UPTs used in open networks and which could also be implemented to enhance security in proprietary networks.

The Observatory also recommends that all card payment schemes implement requirements to ensure that security for UPT networks is on a par with that currently recommended by the “CB” Bank Card Consortium for ATM networks. In particular, the Observatory recommends that certificates be used for UPTs and concentrators to enable mutual authentication of these devices.

Furthermore, the Observatory invites equipment manufacturers and service providers to strengthen the operating systems embedded on UPTs and payment concentrators to enhance security levels and in particular to prevent unauthorised connections to these devices. In addition, it should be possible to regularly update these systems remotely and securely.

To conclude, the Observatory considers that UPTs' payment functions, as well as their hardware, software and network environment, should be covered by a procedure for certification by the card payment scheme. Such a procedure should be based on a security evaluation and would help to ensure a high and uniform level of security for UPT networks.

3|4 Progress on the migration to EMV

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

Progress on the migration to EMV in France

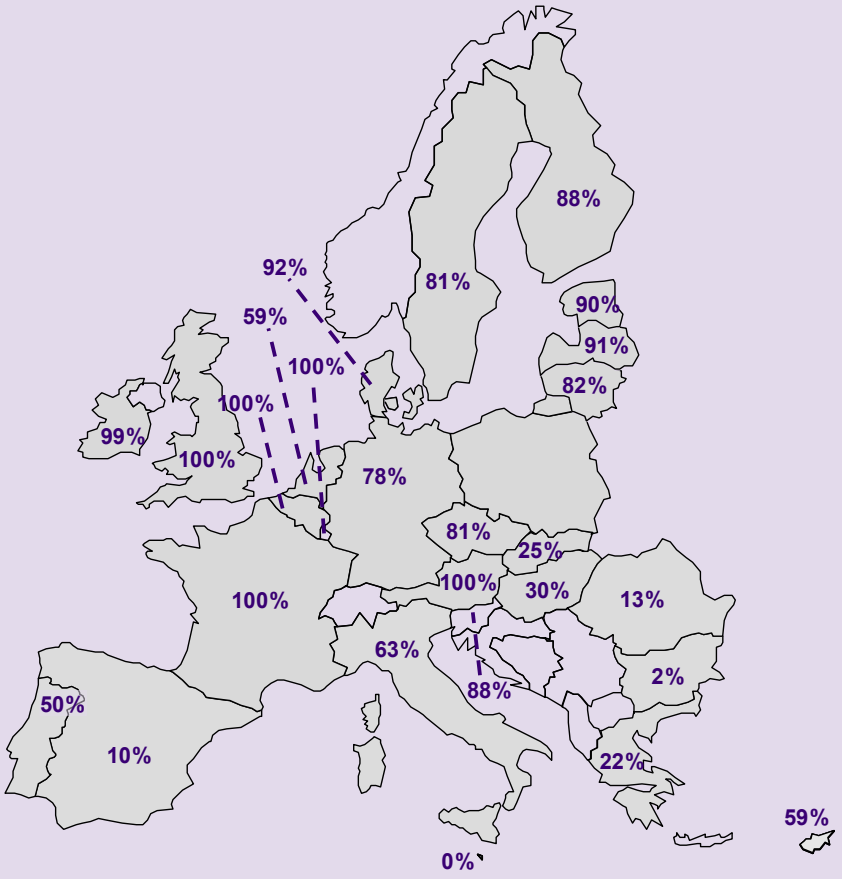
Migration to the EMV standard is practically complete in France. By the end of March 2009, according to statistics compiled by the “CB” Bank Card Consortium, 100% of “CB” cards, 99.5% of payment terminals and UPTs, and 100% of ATMs were EMV compliant. The remaining 0.5% of

terminals and UPTs, which are not much used, will migrate at the time of their normal replacement.

Progress on the migration to EMV in Europe

In Europe, according to the data provided by the European Payments Council for the period up to the end of March 2009, 67.5% of the four-party cards in use in the 27 countries of the European Union are now EMV compliant. This represents an increase of 6 percentage points in comparison with March 2008. The situation varies from one country to another (see Box 8). Whereas compliance with the SEPA interoperability rules is being ensured from early 2008 on, several countries, such as Bulgaria, have barely begun migrating to EMV, while others, including Spain, Greece and Romania, have made little progress.

Box 8 – Deployment of EMV cards in Europe



Source: European Payments Council – March 2009

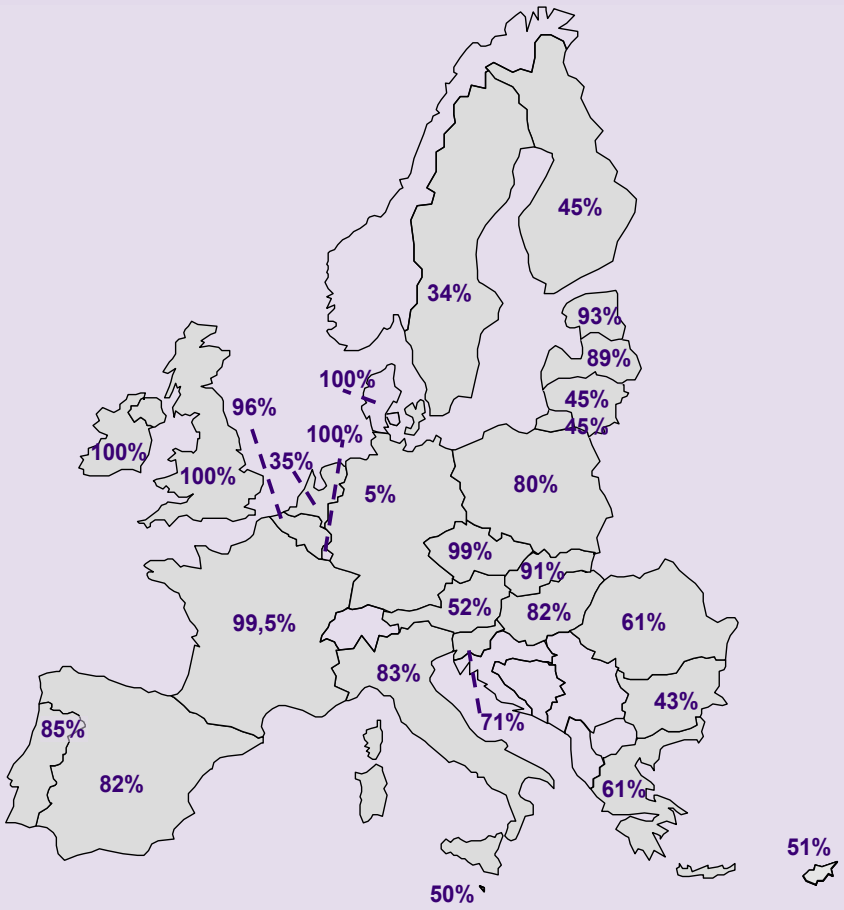
Compared with last year, the map shows overall progress in card migration to the EMV standard. However, several countries, such as Bulgaria and Malta, have barely started migration, and others, like Spain, Greece and Romania, have made little headway.

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

Reliable statistics are not available for Poland at this time.

At the end of March 2009, the migration of acquisition systems to EMV had noticeably progressed: 75.9% of payment terminals (see Box 9) and 92.0% of ATMs (see Box 10) were EMV compliant. This represents an increase of 9 percentage points for both indicators in comparison with March 2008. The situation still varies considerably from one country to the next both in terms of the percentage of compliant equipment and progress from one year to the next.

Box 9 – Deployment of EMV terminals and UPTs in Europe



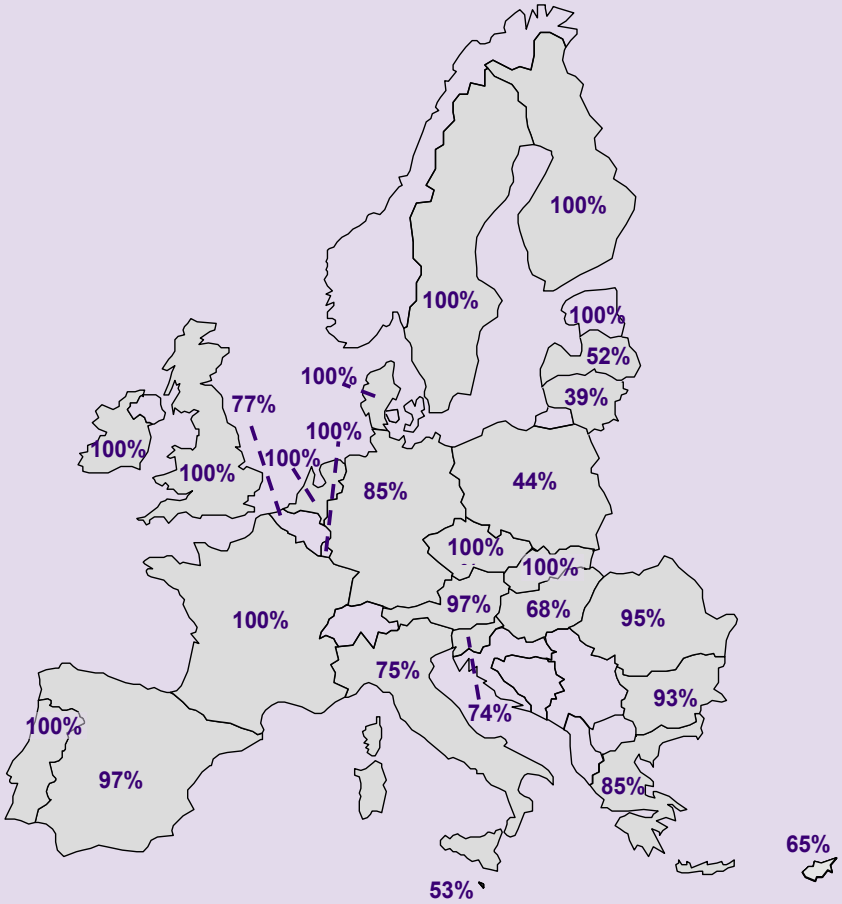
Source: European Payments Council – March 2009

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

The situation in Germany has changed very little compared to March 2008, with the level of EMV compliant equipment remaining low. By contrast, the map shows progress being made in Sweden, the Netherlands as well as Denmark, which completed the migration process.

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

Box 10 – Deployment of EMV ATMs in Europe



Source: European Payments Council – March 2009

Progress on migration of ATMs has been more uniform in Europe and is generally more advanced than among cards, terminals and UPTs. However, there are still some disparities. Countries where the migration of ATMs to the EMV standard is still on-going have probably decided to convert the ATMs used by foreign tourists and visitors first. Deployment in Germany and Italy is still lagging behind the other leading countries, although their levels of EMV compliant ATMs have improved since March 2008.

4 | SECURITY CERTIFICATION FOR CARDS AND TERMINALS

For some years, the Observatory has paid close attention to security issues for cards and payment terminals in the context of the establishment of a Single Euro Payments Area.

In 2005, it explained the importance of procedures for evaluating and certifying card and terminal security and recommended the introduction of European-level agreements to harmonise these procedures and ensure a high and uniform level of security for card payments in Europe.

Given the importance of this subject, the Observatory has decided to review the proposals put forward to date in this area by the various participants, including banks, card payment schemes, manufacturers, certification bodies, European authorities and central banks.

4|1 An heterogeneous approach to card and terminal security certification in Europe

All card payment schemes operating in Europe have introduced procedures to verify the level of security of cards and terminals. However, these procedures vary fairly considerably from one scheme to another, such that it is not possible at this time to say that cards and terminals are subject to uniform levels of security.

Certification process

The certification process for payment cards and acceptance terminals generally includes the following four stages (Cf. Box 11):

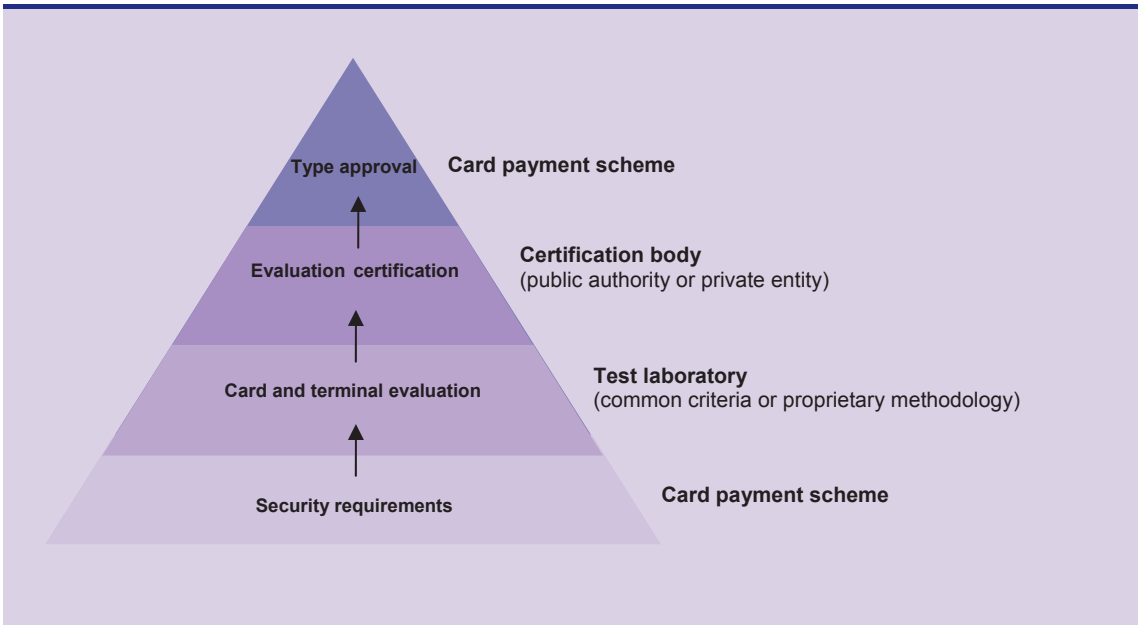
– establishment by the card payment scheme of security requirements for cards and terminals, with which manufacturers are required to comply;

– security evaluations by specialist test laboratories using a variety of methodologies. Manufacturers are required to have their products undergo an evaluation to make sure that they comply properly with the security requirements;

– certification of security evaluation, which may be carried out by a range of different bodies and which certifies the quality of security evaluations. Manufacturers can thus obtain a certificate from a certification body demonstrating that their product complies with the security requirements set by the card payment scheme;

– type approval delivered by the the card payment scheme, based on the certificate provided by the card or terminal manufacturer.

Box 11 – Typical certification process



Card payment schemes take different approaches

In France, the "CB" card payment scheme uses high-quality certification procedures[18]. Card evaluations comply with the Common Criteria (CC) international standard (see Box 12) and the certification process has been incorporated into a "national scheme" administered by the Central Directorate for Information System Security (DCSSI), which reports to the Prime Minister.

Information gathered on the situation in Europe reveals that certification practices vary widely between countries and card payment schemes, due to the use of different evaluation methodologies as well as different types of certification bodies.

As regards evaluation methodologies:

– the majority of card payment schemes base their evaluations on proprietary methodologies, most of which have been developed by the international networks (such as MasterCard CAST for cards and PCI PED for terminals);

– in some cases, however (as in France for cards and in the UK for terminals), the evaluation methodology is based on international, non-proprietary standards (cf. the ISO "Common Criteria", or CC, standard).

[18] Cf. 2005 Annual Report of the Observatory, p. 42

Box 12 – Common Criteria

International Standard ISO/IEC 15408 on Common Criteria for Information Technology Security Evaluation is used to ensure that the processes for specifying security requirements, developing products and evaluating security are carried out in the most rigorous manner possible.

Unlike other information security standards, the Common Criteria (CC) do not define a set of rules with which information processing products must comply. Instead, they establish a framework in which users can formulate their security requirements and providers can demonstrate that their products satisfy those requirements.

The CC methodology is based on three main concepts:

– the Protection Profile (PP), a document which expresses the security requirements of a community of users;
– the Security Target (ST), a document (typically drawn up by the provider of the product) which describes the product's security characteristics and lists the protection profiles which the product purports to satisfy;
– the Evaluation Assurance Level (EAL), which documents all of the measures that have been taken to comply with security requirements, as well as the vulnerability assessment, including the level of resistance to attacks. The assurance levels range from EAL-1 (the least stringent) to EAL-7 (the most stringent). They comprise requirements in different domains: configuration management (ACM), delivery and operation (ADO), development (ADV), guidance documents (AGD), life cycle support (ALC), tests (ATE), and vulnerability assessment (AVA). The level of resistance to attacks, which goes from elementary to high, is mentioned in the certificate.

As regards certification organisations:

– around one-half of European countries have a domestic certification framework, typically under the authority of a private entity, such as a banking association. In countries where there is a public authority, the authority may be involved in card or terminal certification but, unlike in France, card payment schemes do not necessarily base their type approval on the certificates issued by these authorities;
– where there is no domestic certification framework, certification is carried out under the supervision of international private bodies (Visa, MasterCard, PCI SCC, EMVCo) in the case of international card schemes that operate in these countries, as well as, where applicable, in the case of domestic co-badged card schemes.

Accordingly, card payment schemes operating in Europe have neither common rules on security levels for cards and terminals, nor a harmonised approach to certifying security evaluations. As a result, card and terminal manufacturers are forced to subject their products to different certification processes, generating additional costs and lengthening lead times. This is a sub-optimal situation from the perspective of building an integrated retail payments market.

The diverse range of practices in current use also raises another major issue in terms of security, in that this diversity makes it impossible to guarantee a high and uniform level of security for cards and terminals in Europe. If card payment scheme A accepts the cards of payment scheme B, which has a lower level of security, scheme A may be exposed to a higher risk of fraud. There is also the potential danger that increased competition on the European card payments market could cause security to gravitate to the lowest common denominator, as participants put cost-cutting ahead of security.

4|2 Importance of a harmonised certification framework in Europe

The need to harmonise certification procedures

Given the challenges raised by developments in Europe, the Observatory previously stressed in its 2005 annual report the need to harmonise the existing evaluation and certification procedures. It identified several possible ways to make headway and promote the emergence of equivalency criteria and mutual recognition for certificates.

In addition, in the Sixth SEPA Progress Report published on 24 November 2008, the Eurosystem's central banks spoke about the need for such harmonisation and identified a number of conditions that had to be fulfilled to achieve a harmonised framework:

- an appropriate and uniform level of physical security needs to be established for and met by all cards and terminals used in SEPA;
- the evaluation and certification methodologies applied by test laboratories and certification bodies must be equivalent in terms of their level of quality;
- if multiple evaluation and certification methodologies and certification bodies continue to co-exist, as seems likely, it will be necessary to establish a European governance mechanism that can provide mutual recognition for security certifications. Such a mechanism must have the necessary guarantees in terms of legitimacy and neutrality to build users' trust. A harmonised framework would also help to simplify the evaluation and certification process for card and terminal manufacturers by enabling them to receive certificates for the whole of SEPA from one of the certification authorities (under the “one-stop shopping” concept).

Progress by market participants

Market participants have progressed as the Observatory had hoped and in accordance with the guidance in the Eurosystem's Sixth SEPA Progress Report, although work still remains to be done to meet the targets. The state of play is currently as follows.

The process of establishing security requirements for cards and terminals appears to be advancing at a satisfactory pace. The EPC has chosen EAL4+ (from the CC standard), with a high level of resistance to attacks, as the required security level for card components. This requirement is currently in effect in France for four-party chip cards. The EPC has also established security requirements for terminals that include PCI PED specifications for the keypad and stripe reader plus additional requirements for the other terminal components. These security requirements will now be used as the basis for all SEPA compliant card schemes.

An evaluation methodology has not yet been settled on. Manufacturers want a common methodology, but the situation is not the same for cards as it is for terminals, owing to differences in the scope and nature of the equipment to be certified. The CC methodology has been the benchmark for card manufacturers for years, while most terminal manufacturers seem to prefer the PCI approach. However, card schemes, certification bodies and test laboratories

are doing joint work in an effort to set up a terminal evaluation framework using CC methodology[19].

There have been no developments in the various European certification frameworks that would truly pave the way for convergence between the domestic and international arrangements. While terminal manufacturers do not seem to have a preference for either model and are primarily interested in cost and time-to-market issues, card manufacturers are more accustomed to certification frameworks that are independent of the card payment schemes. If broadly adopted, the CC methodology would however entail a natural preference for an independent certification framework, along the lines of the current situation in France, with a certification body supervised by the public authorities.

The most challenging project is that of establishing a European governance mechanism to ensure the equivalency of certificates issued by certification bodies, as well as their mutual recognition by card payment schemes within SEPA. Manufacturers are for such an arrangement, of course, because it would allow them to cut costs and the time required to get products to market. The Eurosystem and the European Commission have indicated that they would like a governance mechanism to be introduced. A number of initiatives are being considered and might provide a way to lay the foundations for a body that would be responsible for setting eligibility criteria for test laboratories and certification bodies, based on shared security requirements and methodologies. The challenge would be to endow such a body with the legitimacy and neutrality needed to impose equivalency rules on market participants, who are by definition in competition.

Eurosystem central banks are closely watching progress by market participants and have taken the initiative to organise meetings with stakeholders to exchange views on ongoing projects and to promote common positions. The European Commission, meanwhile, has just begun a consultation on this issue.

Conclusion

The establishment of a Single Euro Payments Area raises major security challenges, insofar as the interoperability of different card schemes in Europe requires common standards to be set, in a setting of increased competition. To maintain France's high level of security and to prevent security from gravitating to the lowest common denominator, it is essential to set European-level security requirements at a high and uniform level.

Mechanisms have been introduced to evaluate card and terminal security and to certify the results of security evaluations, so that participants can be confident that security requirements have been properly satisfied. However, different European countries and card schemes use non-standardised methodologies and organisational rules in this area. As part of the SEPA project, it is therefore necessary to harmonise evaluation and certification procedures and to establish equivalency criteria that can be used as a basis for the mutual recognition of certificates.

The Observatory hails the progress made by market participants in establishing card and terminal security requirements. It notes also that existing certification frameworks have been maintained thus far, increasing the need for a European governance mechanism for evaluation

[19] This work is being done by the Joint Interpretation Library Terminal Evaluation Methodology Subgroup (JTEMS), which comprises card payment schemes (members of the CAS working group: Visa, MasterCard, Cartes Bancaires), banking associations (APACS, ZKA), public authorities (DCSSI and its UK, German and Dutch counterparts) along with CC accredited test laboratories and experts in the field.

and certification. The Observatory supports the work being done to this end and encourages those involved to continue their efforts. In particular, the Observatory stresses the importance of creating an appropriate European governance mechanism, in order to establish equivalency criteria for the certificates issued by certification bodies and to enable mutual recognition by card payment schemes, so that participants can have confidence in SEPA card payments. The Observatory calls on European and domestic authorities to play their part in swiftly designing a European regulatory mechanism, which could be placed under the responsibility of a public authority, and which would make it possible to maintain the public's confidence by keeping step with technological advances.

ANNEXE 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 concerning the Observatory for Payment Card Security, amended by Decree 2009-654 of 9 June 2009, lays down the missions, composition and operating procedures of the Observatory.

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 I. 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 deferred (for payments).

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

– *National cards* serve to make payments or withdrawals exclusively with acceptors established in France.

– *International cards* serve to make payments and withdrawals at all national or international acquiring points belonging to the brand or to partner issuers with which the card scheme has signed agreements.

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

Responsibilities

Pursuant to the aforementioned Article L. 141-4 of the Monetary and Financial Code and the Decree of 2 May 2002 amended by Decree 2009-654 of 9 June 2009, 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 amended by Decree 2009-654 of 9 June 2009. The Observatory is made up of:

– A Deputy and a Senator,

– Eight general government representatives,

– The Governor of the Banque de France or his/her representative,

– The General Secretary of the Commission Bancaire and his/her representative,

– Ten representatives of payment card issuers, particularly four-party cards, three-party cards and electronic purses,

– Five representatives of the Consumer Board of the National Consumers' Council,

– Five representatives of merchants, notably from the retail sector, the supermarket sector, mail-order sales and e-commerce,

– Three qualified prominent persons chosen for their expertise.

The names of the members of the Observatory are listed in Annex B 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 Commission Bancaire, are appointed for a three-year term. Their term can be renewed.

The President is appointed among these members by the Minister of the Economy and Finance. He has a three-year term of office, which may be renewed. Christian Noyer, the Governor of the Banque de France, has been the President of the Observatory since 17 November 2003.

Operating procedures

Pursuant to the Decree of 2 May 2002 amended by Decree 2009-654 of 9 June 2009, 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.

ANNEXE 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. It was altered in 2007 by two Orders dated 27 June and 25 October 2007, and again in 2009 by an Order dated 29 June 2009.

List of members until 20 April 2009

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Jean-Pierre BRARD
Deputy

Nicole BRICQ
Senator

Representative of the Secretary General of the *Commission Bancaire*

Jean-Luc MENDA
Banking System Oversight Directorate

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

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

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

- The Senior Official for Defence:
  Emmanuel SARTORIUS
  Claude MAUDELONDE

- The Head of the Treasury and Economic Policy or his/her representative:
  Catherine JULIEN-HIEBEL

Nominated on proposition by the Minister of Consumer Affairs:

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

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  Maxence DELORME
  Solène DUBOIS

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 Gendarmerie Nationale (or his/her representative):
  Éric FREYSSINET

Nominated on proposition by the Deputy Minister of Industry:

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

Representatives of payment card issuers

Brigitte CHARLIER
Head of Electronic Payments – CEDICAM

Patrice COUFFIGNAL
Director – MasterCard France

Armand de MILLEVILLE
Executive Vice President – American Express France

Jean-Marie DRAGON
Marketing Director – Argent au quotidien
La Banque Postale

Bernard DUTREUIL
Director – Fédération bancaire française

Alain GOLDBERG
Risks and Compliance Director – Natixis Paiements

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

François LANGLOIS
Director, Institutional Relations –
BNP Paribas Personal Finance

Jean-Christophe LEGALLAND
Groupement Carte Bleue

Cédric SARAZIN
Business and Strategy Director– Groupement des Cartes Bancaires

Representatives of the Consumer Board of the National Consumers' Council

Michèle DAUPHIN
Representative and technical adviser – Familles de France

Valérie GERVAIS
General Secretary – Association FO Consommateurs (AFOC)

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

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

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

Representatives of merchants' professional organisations

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

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

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

Jean-Marc MOSCONI
General Delegate – Mercatel

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

Persons chosen for their expertise

Philippe CAMBRIEL
Executive Vice President – Gemalto

Jacques STERN
Chairman of the Board – Ingenico
Chairman of the Board – Agence nationale de la recherche (ANR)

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

List of members since 29 June 2009

President

Christian NOYER
Governor of the Banque de France

Members of Parliament

Jean-Pierre BRARD
Deputy

Nicole BRICQ
Senator

Representative of the Secretary General of the *Commission Bancaire*

Jean-Luc MENDA
Banking System Oversight Directorate

Representatives of general government

Nominated on proposition by the General Secretary for National Defence:

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

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

- The Senior Official for Defence:
  Emmanuel SARTORIUS

- The Head of the Treasury and Economic Policy or his/her representative:
  Catherine JULIEN-HIEBEL

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:
  Brigitte HOUPPERT

Nominated on proposition by the Minister of Justice:

- The Director for Criminal Affairs and Pardons or his/her representative:
  Maxence DELORME
  Cédric SAUNIER

Nominated on proposition by the Minister of the Interior:

- The Head of the Central Office for the Fight against Crimes Linked to Information and Communication Technologies or his/her representative:
  Christian AGHROUM

Nominated on proposition by the Minister of Defence:

- The Director General of the Gendarmerie Nationale (or his/her representative):
  Éric FREYSSINET

Nominated on proposition by the Deputy Minister of Industry:

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

Representatives of payment card issuers

Yves BLAVET
Head of Electronic Payments and E-commerce – Société Générale

Jean-Marc BORNET
Director – Groupement des Cartes Bancaires

Jean-François DUMAS
Vice President – American Express France

Bernard DUTREUIL
Director – Fédération bancaire française

Bernard GOURAUD
Technologies Director – Banque Fédérale des Banques Populaires

François LANGLOIS
Director, Institutional Relations – BNP Paribas Personal Finance

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

Gérard NEBOUY
Director – Groupement Carte Bleue

Emmanuel PETIT
Chairman and CEO – MasterCard France

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

Representatives of the Consumer Board of the National Consumers' Council

Régis CREPY
National Confederation – Associations familiales catholiques (CNAFC)

Valérie GERVAIS
General Secretary – Association FO Consommateurs (AFOC)

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

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

Representatives of merchants' professional organisations

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

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

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

Jean-Marc MOSCONI
General Delegate – Mercatel

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

Persons chosen for their expertise

Philippe CAMBRIEL
Executive Vice President – Gemalto

David NACCACHE
Professor – Ecole Normale Supérieure

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

ANNEXE C | STATISTICS

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

– The 146 members of the “CB” Bank Card Consortium, with international data provided by MasterCard and Groupement Carte Bleue;

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

– Issuers of the electronic purse Moneo.

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

Total number of cards in circulation in 2008: 84.7 million

– 58.2 million four-party cards (“CB” and Moneo);

– 27.2 million three-party cards.

Number of cards reported lost or stolen in 2008: around 530,000

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

The payment card market in France

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
Four-party cards	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**
Face-to-face and UPT payments	5,770.62	264.43	125.04	9.46	146.05	13.03
Card-not-present payments excl. online payments	108.88	9.83	6.58	0.87	6.66	1.86
Card-not-present online payments	211.35	16.04	50.59	3.04	13.27	1.59
Withdrawals	1,478.52	104.44	40.26	4.78	29.66	5.09
Total	**7,569.37**	**394.74**	**222.46**	**18.15**	**195.64**	**21.56**
Three-party cards	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**
Face-to-face and UPT payments	250.06	23.16	10.70	1.73	16.70	2.72
Card-not-present payments excl. online payments	4.81	0.36	0.02	0.00	0.03	0.01
Card-not-present online payments	4.03	0.43	0.20	0.05	0.33	0.09
Withdrawals	11.80	1.04	na	na	na	na
Total	**270.70**	**24.98**	**10.93**	**1.79**	**17.07**	**2.82**
Grand Total	**7,840.07**	**419.73**	**233.39**	**19.93**	**212.71**	**24.37**

Source: Observatory for Payment Card Security

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

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
	Volume (k)	Value (k€)	Volume (k)	Value (k€)	Volume (k)	Value (k€)
Face-to-face and UPT payments	**569.1**	**38,240.6**	**168.4**	**30,523.7**	**309.9**	**61,687.4**[1]
Lost or stolen cards	517.4	35,707.6	78.4	8,931.8	99.8	10,589.1
Intercepted cards	5.0	269.0	1.0	176.5	4.7	541.6
Forged or counterfeit cards	46.7	2,264.0	77.6	18,963.1	67.3	24,778.3
Appropriated numbers	0.0	0.0	6.6	1,840.1	77.0	15,209.1
Other	0.0	0.0	4.8	612.3	61.2	10,569.3
Card-not-present payments excl. online payments	**395.6**	**28,060.1**	**51.7**	**8,940.3**	**na**	**na**
Lost or stolen cards	0.0	0.0	16.4	2,867.0	na	na
Intercepted cards	0.0	0.0	0.1	6.7	na	na
Forged or counterfeit cards	0.0	0.0	14.2	2,700.5	na	na
Appropriated numbers	395.6	28,060.1	13.8	1,945.2	na	na
Other	0.0	0.0	7.2	1,420.9	na	na
Card-not-present online payments	**274.6**	**38,501.2**	**418.5**	**55,543.6**	**na**	**na**
Lost or stolen cards	0.0	0.0	118.2	15,462.3	na	na
Intercepted cards	0.0	0.0	0.2	18.6	na	na
Forged or counterfeit cards	0.0	0.0	115.7	16,353.0	na	na
Appropriated numbers	274.6	38,501.2	140.9	17,432.2	na	na
Other	0.0	0.0	43.6	6,277.5	na	na
Withdrawals	**78.7**	**18,117.2**	**113.9**	**19,075.9**	**18.3**	**5,579.9**
Lost or stolen cards	76.1	17,690.1	12.7	1,955.5	3.2	777.8
Intercepted cards	0.4	80.2	0.1	27.9	0.1	28.7
Forged or counterfeit cards	2.3	346.8	100.8	17,039.2	14.7	4,691.9
Appropriated numbers	0.0	0.0	0.2	31.3	0.2	49.5
Other	0.0	0.0	0.1	21.9	0.1	32.1
Total	**1,318.0**	**122,919.1**	**752.5**	**114,083.6**	**328.2**	**67,267.3**

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, type of fraud and geographical zone

	French issuer, French acquirer		French issuer, foreign acquirer		Foreign issuer, French acquirer	
	Volume (k)	Value (k€)	Volume (k)	Value (k€)	Volume (k)	Value (k€)
Face-to-face and UPT payments	**14.54**	**6,244.39**	**7.10**	**1,490.55**	**4.12**	**1,731.08**
Lost or stolen cards	6.38	1,427.24	1.34	311.59	0.99	405.56
Intercepted cards	1.90	390.81	0.12	57.07	0.13	39.80
Forged or counterfeit cards	1.63	493.41	5.26	1,035.64	2.64	1,111.56
Appropriated numbers	0.41	184.93	0.17	52.08	0.22	131.68
Other	4.22	3,747.99	0.22	34.18	0.14	42.49
Card-not-present payments excl. online payments	**1.17**	**423.52**	**6.31**	**2,262.87**	**3.50**	**1,697.78**
Lost or stolen cards	0.08	49.35	0.11	20.39	0.12	42.30
Intercepted cards	0.03	4.80	0.01	7.40	0.02	2.07
Forged or counterfeit cards	0.17	17.64	0.42	203.07	0.33	216.06
Appropriated numbers	0.75	311.18	5.68	2,009.02	2.99	1,422.22
Other	0.13	40.54	0.10	22.99	0.04	15.13
Card-not-present online payments	**0.54**	**255.99**	**2.04**	**502.65**	**1.49**	**332.73**
Lost or stolen cards	0.11	84.32	0.02	1.67	0.03	6.36
Intercepted cards	0.04	23.35	ns	0.97	0.01	0.07
Forged or counterfeit cards	0.02	1.82	0.11	12.11	0.09	18.84
Appropriated numbers	0.32	131.43	1.87	483.99	1.35	306.50
Other	0.05	15.07	0.03	3.92	0.01	0.97
Withdrawals	**3.90**	**1,007.57**	**0.02**	**2.09**	**na**	**na**
Lost or stolen cards	3.41	826.94	na	na	na	na
Intercepted cards	0.33	131.77	na	na	na	na
Forged or counterfeit cards	0.00	0.00	0.02	2.09	na	na
Appropriated numbers	0.00	1.54	na	na	na	na
Other	0.15	47.32	na	na	na	na
Total	**20.14**	**7,931.47**	**15.47**	**4,258.16**	**9.11**	**3,761.59**

Source: Observatory for Payment Card Security

ANNEXE D | DEFINITION AND TYPOLOGY OF PAYMENT CARD FRAUD

Definition of payment card fraud

For purposes of drawing up statistics, the Observatory considers that the following acts constitute fraud:

All acts that contribute to the preparations for illegitimate use and/or illegitimate use of payment cards or data stored on them:

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

2. irrespective of:

- the methods used to obtain, without lawful reason, cards or data stored on them (theft, taking possession of cards, physical or logical data, personalisation data and/or misappropriation of secret codes, and/or security codes, magnetic stripe and chip hacking);
- the procedures for using cards or the data stored on them (payments or withdrawals, face-to-face or card-not-present, via physical use of the card or the card number, via UPTs, etc.);
- the geographical area of issuance or use of the card and the data held on it:
  - French issuer and card used in France,
  - foreign issuer and card used in France,
  - French issuer and card used abroad;
- the type of payment card, as defined by Article L. 132-1 of the Monetary and Financial Code, including electronic purses;

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

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

Fraud typology

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

The origin of the fraud:

- *Lost or stolen cards:* the fraudster uses a payment card obtained without the knowledge of the lawful cardholder, following card theft or loss;
- *Intercepted cards:* cards intercepted when sent by issuers to lawful cardholders. While this type of origin is similar to theft or loss, it is nonetheless different because it is not easy for a cardholder to ascertain that a fraudster is in possession of a card that belongs to him/her; it also entails risks specific to procedures for sending cards;
- *Forged or counterfeit cards:* an authentic payment card may be falsified by modifying magnetic stripe data, embossing or programming. Creating a counterfeit card means creating an object that appears to be an authentic payment card and/or is capable of deceiving a payment machine or a person. For payments made via UPTs, counterfeit cards incorporate the data required to deceive the system. In face-to-face transactions, counterfeit cards present certain security features found on authentic cards (including visual appearance), incorporate data stored on authentic cards, and are intended to deceive acceptors;
- *Appropriated number:* a cardholder's card number is taken without his knowledge or created through card number generation (see fraud techniques) and used in card-not-present transactions;
- *Unallocated card numbers:* use of a true PAN[2] that has not been attributed to a cardholder, generally in card-not-present transactions;
- *Splitting payments:* splitting up payments so as not to exceed the authorisation limit defined by the issuer.

Fraud techniques:

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

[2] Personal Account Number

Types of payment:

– *face-to-face payment*, carried out at the point of sale or UPT;

– *card-not-present payment* carried out online, by mail, by fax/telephone, or any other means;

– *withdrawal* (withdrawal from an ATM or any other type of withdrawal).

Distribution of losses between:

– the merchant's bank, the acquirer of the transaction;

– the cardholder's bank, the issuer of the card;

– the merchant;

– the cardholder;

– insurers, if any;

– any other participant.

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

– The issuer and acquirer are both established in France. In this case, the transaction is qualified as national or domestic;

– The issuer is established in France and the acquirer abroad;

– The issuer is established abroad and the acquirer in France.

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 8 octobre 2009
ISSN : en cours

2008 REPORT

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

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

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

This report has been prepared by the

BANQUE DE FRANCE
EUROSYSTÈME

BdF - 29598 - Ateliers SIMA - 190466 - 5-09

2009 Issue
ISSN : Pending