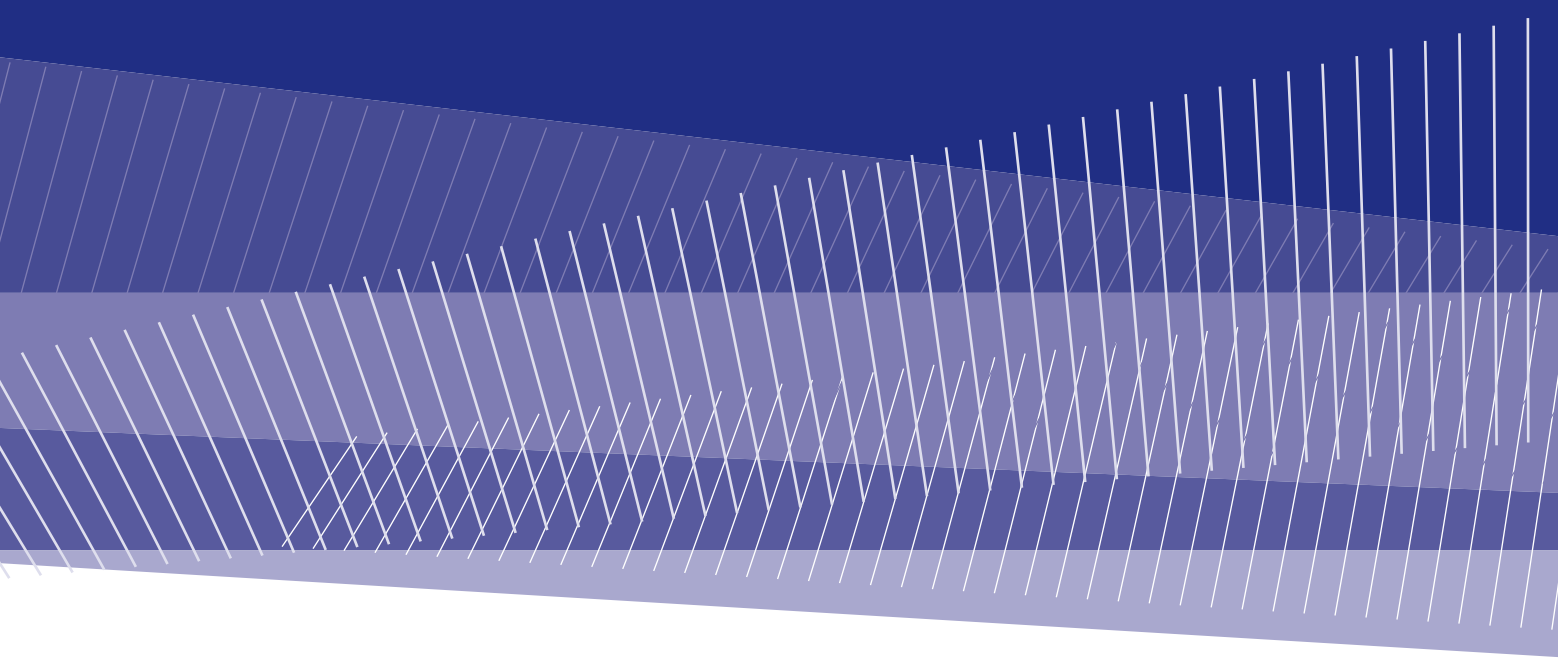
2007 ANNUAL REPORT

OF THE OBSERVATORY FOR PAYMENT CARD SECURITY



Observatoire
de la sécurité
des cartes de paiement

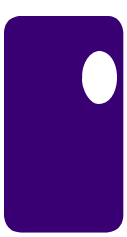
www.observatoire-cartes.fr

2007 ANNUAL REPORT

OF THE OBSERVATORY FOR PAYMENT CARD SECURITY

Observatoire
de la sécurité
des cartes de paiement

www.observatoire-cartes.fr



Observatoire
de la sécurité
des cartes de paiement

Internal Postcode 11-2323

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

2007

Annual Report of the Observatory for Payment Card Security

addressed to

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

by

Christian Noyer,

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

CONTENTS

FOREWORD 7

1 | SECURITY POLICIES OF ISSUERS AND ACQUIRERS 9

Centralised acceptance systems 9
The new range of prepaid cards 13

2 | FRAUD STATISTICS FOR 2007 17

Overview 18
Breakdown of fraud by card type 19
Geographical breakdown of fraud 20
Breakdown of fraud by transaction type 21
Breakdown by fraud type 23

3 | TECHNOLOGY WATCH 27

Security of card payments and European standardisation 27
Security of new methods for initiating card payments (via mobile phones and contactless cards) 35
Progress on the migration to EMV 41

4 | THE IMPACT OF THE PAYMENT SERVICES DIRECTIVE ON THE RULES APPLIED TO PAYMENT CARDS IN FRANCE 45

The opening-up of the payment card market to new non-bank players 45
A new approach to the regulations applied to payments 47
Harmonisation of information requirements 48
New rules concerning revocation and contestation 49
Conclusion 50

MISSIONS AND ORGANISATIONAL STRUCTURE OF THE OBSERVATORY 53

MEMBERS OF THE OBSERVATORY 57

STATISTICS 61

The payment card market in France 62
Breakdown of four-party card fraud by type of transaction, type of fraud and geographical zone 63
Breakdown of three-party card fraud by type of transaction, type of fraud and geographical zone 64

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 systems (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. At first, it includes two studies on the security policies of issuers and merchants, the first one on centralised acceptance systems, the second one on the new range of prepaid cards (Part 1), then it provides fraud statistics for the year 2007 (Part 2) and a summary of the work carried out in the area of technology watch for payment cards (Part 3). Lastly, the report contains a study on the impact of the Payment Services Directive on the rules applying to payment cards in France (Part 4).

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

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

1 | SECURITY POLICIES OF ISSUERS AND ACQUIRERS

As part of its responsibility for monitoring the security policies of card issuers and acquirers, the Observatory conducted two studies in 2007: the first on security policies in centralised acceptance systems, and the second on security measures applied to the new range of prepaid cards. Based on information collected by means of questionnaires, respectively sent to acceptors' and manufacturers' representatives and to issuers' representatives, the Observatory assessed the security measures implemented for the systems concerned.

1|1 Centralised acceptance systems

Following its 2005 examination of payment card data protection during the acquisition process, the Observatory conducted in 2007 a study on the security of the centralised acceptance systems used by certain merchants. A different approach is required for the protection of payment card data in such systems, which comprise a number of devices each playing a role in the management of these data. Indeed, centralised acceptance systems are generally composed of a series of point-of-sale (POS) or unattended payment terminals (UPTs), connected to merchants' cash registers and to a central server. This server concentrates the payment data and establishes the connection with the servers of the acquirers. Given the volume of data processed, the protection of these systems requires close attention.

Centralised acceptance systems are very widely used in France, which counts almost 150,000 acceptance terminals and 50,000 UPTs, which means around 20% of the country's acceptance points.

In order to carry out this study, the secretariat of the Observatory gathered information by means of a questionnaire filled in by its members representing acquirers and merchants[3], as well as to by company Ingenico. Manufacturers of acceptance systems via their professional association, "CONCERT International", also answered the questionnaire.

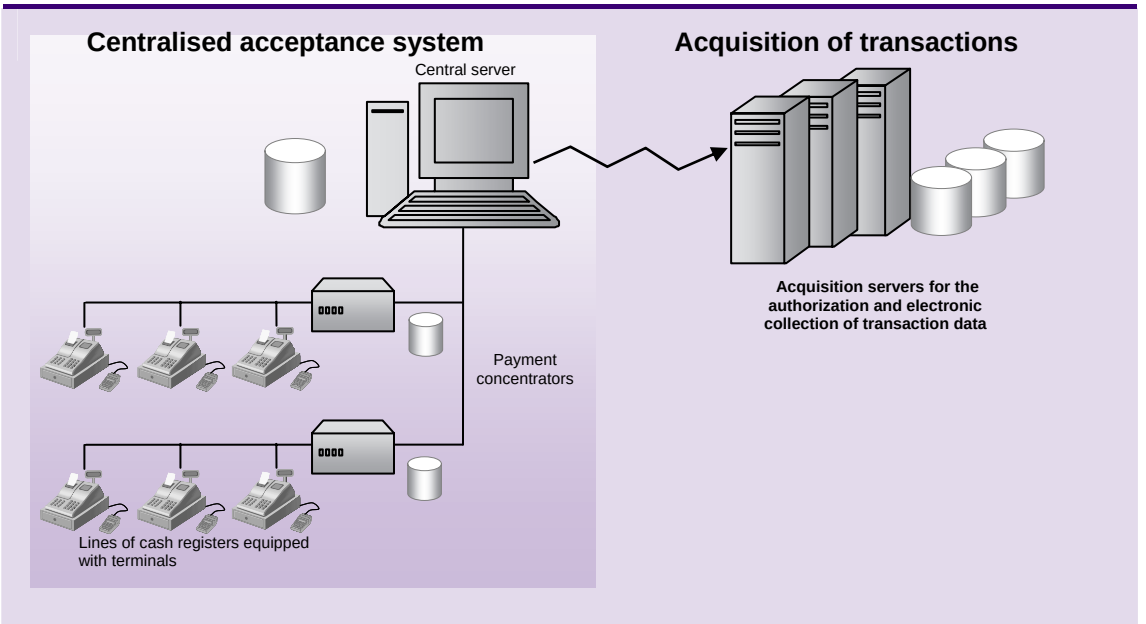
Description of centralised acceptance systems

Contrary to the acceptance points consisting of a "stand-alone payment terminal", linked to the cash register and connected by the communication networks to the server of the acquiring bank, the typical organisation of a centralised acceptance system requires different levels of equipment. Cardholders' transactions are carried out using terminals linked to cash registers, which are connected to an aggregating device known as the payment concentrator. The payment concentrators used in the system are in turn linked to a central server, which transmits information to the acquisition centres for authorisation and transaction data collection. In this study, we consider the entire payment process from payment by card at the cash register to the transmission of transaction data to the acquiring banks' servers. This also includes data storage and database management.

[3] Caisse d'Epargne, Crédit Agricole, "CB" Bank Card Consortium, and Mercatel

The equipment used in centralised acceptance systems covers a wide range of functions, ranging from the management of cash registers and terminals to data processing and storage. The manufacturers of such equipment are generally responsible for their design as well as, in many cases, their installation and maintenance. In view of the complexity of the implementation and functioning of the equipment used, it must comply with a number of security rules that are closely observed by card payment systems, banks, merchants and naturally the manufacturers themselves.

Box 1 – Typical organisation of a centralised acceptance system



The data processed in centralised acceptance systems contain the card number, the expiration date, the cardholder's name and the magnetic stripe data (if they are read). These data are sometimes stored by the payment concentrator or central server. Transaction data (date, time, amount, nature of the purchased item, etc.) may also be stored at these different levels. Processing such data is sensitive in terms of security. Merchants cashiers must therefore observe a number of rules.

Security of centralised acceptance systems

The data processed and stored in centralised acceptance systems are sensitive elements, particularly due to the volumes processed. If they were misappropriated or copied, they could be used to make fraudulent payments.

The representatives of acquirers, merchants and manufacturers of terminals surveyed consider that the main security measures to be implemented should aim to protect the data processed in payment terminals or stored in merchants' IT systems, in order to prevent data theft.

Acquiring banks thus ensure that their merchant clients comply with a number of organisational and technical security requirements, established by card payment schemes. These security measures, which are set out in merchants' contracts, include in particular the requirements of

the PCI DSS programme[4]. The latter provides for a body of security measures applicable to the storage of data and the conduct of audits.

Protection of electronic payment terminals

Security measures are in place for cashiers. One of these could consist in ensuring that cardhandling by cashiers should be reduced to the minimum, in order to prevent the installation of skimming devices[5] or the visual capture of sensitive data. Moreover, merchants segregate duties and implement strict controls in order to restrict access to sensitive data solely to authorised persons.

In addition, merchants are required to use approved equipment meeting international standards, such as EMV[6], which ensures increased protection of transactions, or PCI PED[7], which protects the entry of PIN code into payment terminals.

Furthermore, in order to strengthen the security of the operating systems installed on the different devices, most manufacturers ensure that the operating system of the terminal, the client application and the software that customises the terminal are encoded by different people. Besides, the secrets present in the terminals are generated in very high-security certified sites.

Lastly, as regards maintenance operations, special precautions are taken, such as the traceability of the opening of the secured enclosure and the loss of “banking secrets” in the event of an uncontrolled opening of the terminals. Furthermore, in many cases, maintenance staff cannot modify by itself electronic payment terminals, which must then be sent back to the manufacturer and submitted to a new certification process.

Protection of the payment concentrator and the central server

PCI DSS standards require a physical protection of systems and the use of cameras to monitor sensitive areas.

In addition, PCI DSS call for the use of logical data protection, particularly with the implementation of firewalls, the systematic use of up-to-date anti-virus programmes on all systems, the encryption of stored and sent data, bans on storing magnetic stripe data and PIN codes, the issuing of a unique password to each person having access, and secured password management. Therefore, card data and the corresponding PIN are transmitted only during the payment authorisation phase and are encrypted. The representatives of merchants nevertheless recalled that they found certain provisions of PCI DSS concerning the protection of transactions using magnetic stripe poorly suited to the French environment in that the great majority of payments use chip data (EMV).

The above measures protect sensitive data and the centralised acceptance system against internal or external attacks that would aim to put it out of service or fraudulently gain access into it.

---

4 Payment Card Industry - Data Security Standard (PCI DSS). See the 2005 Annual Report of the Observatory for Payment Card Security, Box 3, p.14.

5 See the 2003 Annual Report of the Observatory for Payment Card Security, Box 13, p.36.

6 Europay-Mastercard-Visa (EMV). See the 2003 Annual Report of the Observatory for Payment Card Security, p.20.

7 Payment Card Industry - Pin Entry Device (PCI PED)

Certification of systems and fraud monitoring

The certification procedures implemented by card schemes ensure that the equipment complies with security standards (including cards and terminals), thus contributing to better protecting the sensitive data exchanged.

In this context, manufacturers give special attention to the certification process of centralised acceptance systems, which is potentially longer due to their increased complexity in comparison with stand-alone payment terminals. In order to optimise the certification process as a whole, some card schemes and standardisation organisations publish working versions of forthcoming specifications, which allows manufacturers to anticipate changes in their equipment.

Furthermore, in order to ensure the correct implementation of these security measures, audits are required. In the framework of PCI DSS, merchants carrying out high volumes of card transactions (typically merchants equipped with centralised acceptance systems) must be audited regularly by independent firms and certified by PCI SSC[8]. In particular, an annual security audit must be conducted on the site of their IT system, as well as a quarterly scan of their telecommunication network weaknesses.

Lastly, according to the information collected during the study, merchants systematically register a complaint for the identified cases of fraud and the persons concerned assist police forces. Moreover, the “CB” Bank Card Consortium has implemented a systematic early warning system that, in the event of a problem detected in a given piece of equipment, transmits a notification of the type of attack and a complete description to its members.

Conclusion

Centralised acceptance systems are important within the payment chain since they process a substantial volume of sensitive data. They are very widely used in France and account for almost 20% of POS and unattended payment terminals. It is therefore important to prevent the theft of data and their malicious utilisation (counterfeiting, fraudulent use). Consequently, physical and logical protection measures must be put in place in order to protect against internal or external attacks to the system.

Responses collected in this study conducted by the Observatory show that the different actors are aware of these issues and are working to both set appropriate security standards and correctly apply existing security recommendations, in particular through certification programmes covering all equipment and systems. It is therefore essential to broadly implement these standards in order to better protect the sensitive data processed by centralised acceptance systems.

Lastly, it appears that very few cases of compromised data have been detected. Those cases were systematically reported to the “CB” Bank Card Consortium and triggered its early warning system, thus making it possible to mitigate their impact and rapidly solve the problems encountered.

8 Payment Card Industry – Security Standards Council (PCI SSC)

1|2 The new range of prepaid cards

The Observatory conducted in 2007 a study on the security measures applied to the new range of prepaid cards, and in particular those aimed at young customers ("gift cards", "youth cards", and "Moneo" cards). Such cards provide these customers, who are sometimes too young to have access to certain banking services, with a widely accepted means of payment. The conditions governing the use of these cards nevertheless differ from those applying to payment cards linked to a bank account and have been specifically adapted to young customers. This is why the Observatory wished to take a closer look at these conditions as well as, more generally, the measures taken by issuers to reduce the risk of fraud regarding these cards, in particular to protect the cardholders in the event of theft or loss.

To achieve this, useful information have been gathered by means of a questionnaire filled in by the Observatory members representing issuers of four-party cards and three-party cards[9].

Through this study information was gathered on gift cards, interbank youth cards and Moneo cards available to young customers. Some issuers of three-party cards also issue gift cards, primarily to reward the loyalty of their cardholders. It should also be noted that the term "gift card" is frequently used by merchants to designate the cards that can be used only in their establishment, and which are not legally payment cards and therefore do not come within the scope of this study.

Description of the different types of prepaid cards

The survey that the Observatory conducted enables to distinguish between two ways in which the prepaid cards currently issued in France function: the funds credited to the card may either be stored in the issuer's IT system (on a server), or on the card itself (on the chip).

Prepaid cards whose value is stored on the issuer's server ("gift cards", "youth cards")

"Gift cards" or other "youth cards" that have been issued by French banking issuers over the past three years or so are immediate debit "CB" cards that are generally co-badged[10] with Visa or MasterCard. Around 70,000 cards of this type are currently in use in France. These cards are linked to a reserve of funds prepaid to the issuer. The funds are generally provided by a person other than the cardholder, for example the parents. If the cardholder is a minor, his/her legal representative is legally responsible.

These cards can be used for face to face and unattended payment terminals (UPTs) in France and abroad and, depending on the choice of the issuer, remote payments and cash withdrawals. They offer the same level of security as all "CB" cards: they are equipped with a chip and their use requires the entry of a PIN code. It is only possible to make payments or withdrawals within the limits of the prepaid funds. This is why these cards require systematic authorisation, i.e. each transaction is checked on-line to verify that its amount is compatible with the prepaid reserve of funds available. The issuer manages the card's available balance in a "technical account" located on a data processing server. The maximum prepaid amount ranges

9 Caisse d'Epargne, Banque Populaire, Crédit Agricole, CETELEM, la Banque Postale, BMS (Billettique Monétique Services).

10 "Co-badging" is where the network logos of partner cards appear on payment cards. It differs from "co-branding", which consists in branding the card with, in addition to the logo of the credit institution issuing the card, a commercial partner's logo.

from tens of euro to hundreds of euro. These cards may or may not, depending on the issuer, be rechargeable. There are generally valid for at most one year.

Prepaid cards whose value is stored on the card (Moneo cards)

For almost 10 years now, French issuers of four-party cards have offered their customers prepaid cards (Moneo) known as “electronic purses”, or “e-purses”. Around one million Moneo cards are currently in use in France. Three types of Moneo cards are available. The first is a “CB” bank card on which the Moneo function is added, which enables cardholders to choose to use this function for their small-value purchases. In this case, the e-purse is necessarily recharged by debiting the account to which the “CB” card is attached. The second type is called “Moneo bleu”. Like in the first case, this card is also attached to a bank account and prepaid by debiting this account. The difference with respect to the previous case is that the e-purse is not associated to a “CB” bank card and that the account to which it is attached could be different from the one to which the “CB” card of the cardholder is. The third type is called “Moneo vert”. It is an anonymous card, not attached to a bank account and recharged by debiting a “CB” card or by purchasing prepaid coupons. Over the past two years, the development of the use of Moneo in university canteens has been mainly backed by the spreading of “Moneo verts”.

For all Moneo cards, payment is made without entry of a PIN code nor authorisation request (off-line transaction). A PIN is required only for recharging Moneo cards attached to a bank account. Payments are limited to EUR 30 and the maximum balance on the card is EUR 100. These cards cannot be used to make withdrawals. Some Moneo cards use “contactless” smartcard technology.

The security of prepaid cards

Prepaid cards may attract fraudsters or thieves in that they may be used to make immediate purchases. The Observatory wanted to ensure that cardholders, in particular the young population, were not exposed to an increased risk of being assaulted. The information gathered from issuers’ representatives shows that security measures appear to have been adapted to this context. Those applying to prepaid cards vary according to whether the prepaid value is stored on a server or on the card.

Prepaid cards whose value is stored on the issuer’s server

By definition, these cards are not exposed to risks of theft of the value stored on the card or the fraudulent creation of value. The funds are still held by the issuer and are protected as in the case of a traditional debit card. What is important therefore is that the card cannot be used without the legitimate cardholder knowing.

The issuers surveyed explained that gift cards and youth cards are not activated when they are distributed, even though the account to which they are attached is by definition prepaid. This means that the cardholder must activate the card before using it through a procedure defined by the issuer. In the case of some issuers, these cards are distributed in bank branches to further reduce the risk of theft in the delivery circuit.

Once the card has been received and activated by the legitimate cardholder, transactions require the use of a PIN, whose authenticity is verified in a cryptographic way. Card-not-present

transactions are authorised by some issuers but they require entry of the visual cryptogram CVx2[11] and are submitted to systematic authorisation.

Furthermore, the attraction for fraudsters to counterfeit these cards is limited given that some issuers do not allow withdrawals from ATMs in France and abroad. In the event of counterfeiting, the legal provisions of exemption of the cardholder's liability apply. In the event of loss or theft, the card must be reported missing, as it is customary.

Prepaid cards whose value is stored on the card

This type of card is attractive to thieves since they can directly use its electronic value. Indeed, the transactions are not protected by a PIN code due to their small value. The prepaid amount remaining on the lost or stolen card is not reimbursed to the legitimate cardholder, which is tantamount to losing banknotes or coins. Nevertheless, issuers wanted to reduce this risk by limiting the amount loaded onto the Moneo card to EUR 100, and payment transactions to EUR 30. The issuers surveyed pointed out that the small size of the sums involved had certainly contributed to reducing the number of assaults for Moneo cards.

It should also be noted that if the card is reported lost or stolen, Moneo card reloads drawing on an account are automatically blocked. It is pointless to report lost or stolen “Moneo vert” cards, since they are not attached to an account and are anonymous. These cards could continue to be loaded but this would mean that the thief would have to recharge them, which is unlikely.

During transactions, Moneo cards are dynamically authenticated by the merchant’s terminal. The counterfeiting of cards, whose electronic component is assessed in the framework of the National Evaluation and Certification Scheme[12], is technically difficult and of little interest in view of the sums involved.

Moneo cards using contactless smartcard technology have recently been marketed. The risk of prepaid card theft without the cardholder knowing (“tele-pickpocketing”, see 3.2) is not insignificant. Issuers’ security policies and the measures implemented have nevertheless reduced this risk. In particular, given the way Moneo e-purses work, the electronic value that could be stolen could only be converted into bank money if deposited at a credit institution.

Conclusion

The prepaid cards currently on offer to the French public, in particular the young, can be grouped into two broad categories in terms of security measures.

On the one hand, there are prepaid cards whose value is stored on the issuer’s server. These cards, i.e. four-party gift cards and youth cards, are immediate debit cards with systematic authorisation. Cardholders who use them benefit from general protections applicable for four-party payment cards, such as the use of a PIN code, as well as from specific measures. The latters include the systematic authorisation and maximum prepaid limit, which reduce the risk of the card being reused in the event of theft or loss.

On the other hand, there are prepaid cards whose value is stored on the card itself, such as Moneo cards. These cards present a greater risk of being reused in the event of theft or loss,

---

11 See the 2005 Annual Report of the Observatory for Payment Card Security, Box 2, p. 12.

12 See the 2005 Annual Report of the Observatory for Payment Card Security, Box 6 p.29.

especially since transactions, which generally involve small sums, do not require the use of a PIN code. The cardholder is mainly protected by the maximum prepaid limit, which is deliberately kept low in order to deter theft.

Moreover, issuers surveyed pointed out that they have recorded for the moment only a few cases of fraud regarding their prepaid cards.

2 | FRAUD STATISTICS FOR 2007

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[13]. A summary of the 2007 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 relies on a diversified sample of respondents encompassing the issuers and merchants that are most representative of four-party card and three-party card payment schemes.

Issuers provided the Observatory with data on:

– EUR 381.1 billion in transactions in France and in other countries made with 55.7 million four-party cards issued in France (including 1.1 million electronic purses);

– EUR 25.8 billion in transactions primarily in France with 25.7 million three-party cards issued in France;

– EUR 23.8 billion in transactions in France with foreign three-party and four-party cards.

Card issuers

Data were gathered from:

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

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

– Issuers of Moneo, an electronic purse.

Merchants

The Observatory collected fraud statistics from:

– Merchants that accept card payments: France Loisirs, Monoprix and the French Railways (SNCF);

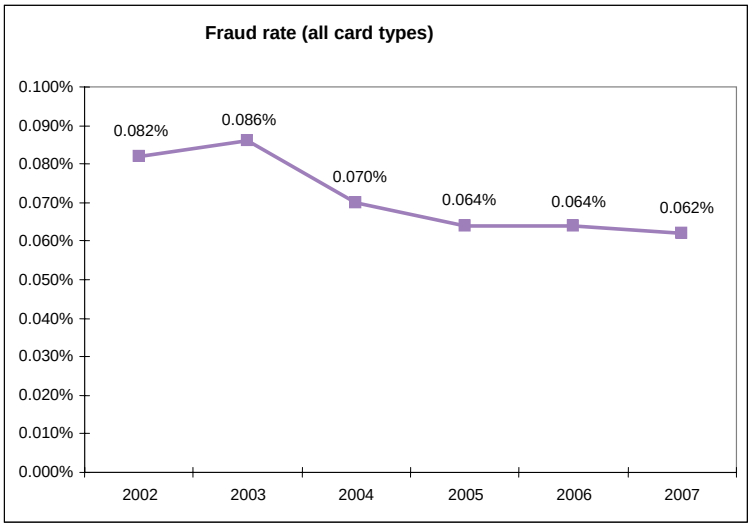
– The e-commerce and distance selling federation (Fevad), from a representative sample of 30 companies that account for 45% of revenues in distance selling to retail customers;

– FCD and Mercatel, two merchants' associations. The data were gathered from a sample accounting for around 40% of the supermarket and specialised trade market.

[13] Cf. 2003 Report, Part 3

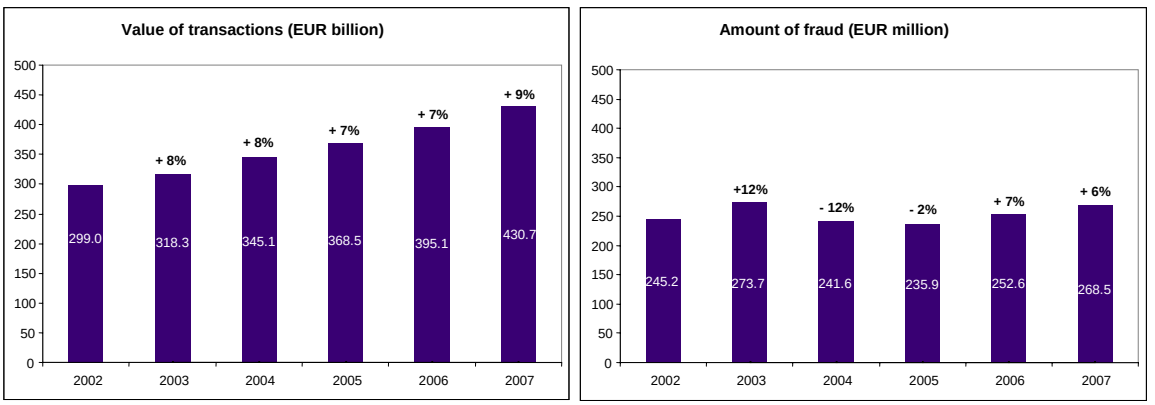
2|1 Overview

The overall fraud rate recorded by French card schemes in 2007 stood at 0.062%, more or less the same or slightly lower than in previous years (0.064% in 2006 and 2005 – see Table 1). Although there was a 6.3% overall increase in the amount of fraud from EUR 252.6 million in 2006 to EUR 268.5 million in 2007, the fraud rate was basically unchanged due to sustained growth in the value of transactions, which climbed 9.0% from EUR 395.1 billion in 2006 to EUR 430.7 billion in 2007 (see Table 2). The average amount of a fraudulent transaction also rose, to EUR 130 compared with EUR 117 in 2006.



Source: Observatory for Payment Card Security

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



Source: Observatory for Payment Card Security

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

The rate of issuer fraud, which is the total of fraudulent payments and withdrawals made in France and in other countries with cards issued in France, was also stable at 0.049% in 2007, slightly lower than in 2006 (0.050%). Issuer fraud totalled EUR 199.8 million in 2007, compared with 186.1 million in 2006.

The rate of acquirer fraud, which is the total of fraudulent payments and withdrawals made in France with all French and foreign cards, fell slightly to 0.044% in 2007 (corresponding to a value of EUR 183.2 million) from 0.047% in 2006 (EUR 176.2 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)				
	2003	**2004**	**2005**	**2006**	**2007**
Four-party cards	0.086% (259.2)	0.069% (224.1)	0.064% (218.8)	0.065% (237.0)	**0.063%** (253.6)
Three-party cards	0.082% (14.4)	0.082% (17.5)	0.067% (17.1)	0.052% (15.6)	**0.052%** (15.0)
Total	0.086% (273.6)	0.070% (241.6)	0.064% (235.9)	0.064% (252.6)	**0.062%** (268.5)

Source: Observatory for Payment Card Security

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

The fraud rate for four-party cards was down slightly in 2007, falling to 0.063%, which corresponds to fraud of EUR 253.6 million, compared with 0.065% in 2006 (EUR 237 million). Issuer and acquirer fraud rates for this type of card stood at 0.049% and 0.044% respectively, compared with 0.050% and 0.047% respectively in 2006. The average value of a fraudulent transaction was EUR 125, compared with EUR 112 in 2006.

The fraud rate for three-party cards was stable at 0.052% (corresponding to fraud of EUR 15.0 million, compared with EUR 15.6 million in 2006). Issuer and acquirer fraud rates for this type of card were 0.044% and 0.046% respectively, compared with 0.045% and 0.046% respectively in 2006. The average value of a fraudulent transaction was EUR 432 in 2007, compared with EUR 430 in 2006.

2|3 Geographical breakdown of fraud

	Fraud rate (Fraud amount, EUR million)				
	2003	**2004**	**2005**	**2006**	**2007**
Domestic transactions	**0.031%** **(88.3)**	**0.033%** **(103.9)**	**0.029%** **(97.8)**	**0.031%** **(109.6)**	**0.029%** **(114.5)**
International transactions	**0.648%** **(185.3)**	**0.417%** **(137.7)**	**0.408%** **(138.1)**	**0.362%** **(143.0)**	**0.368%** **(154.0)**
o/w French issuer and foreign acquirer	0.690% (79.3)	0.463% (55.2)	0.458% (64.1)	0.453% (76.4)	0.476% (85.3)
o/w foreign issuer and French acquirer	0.620% (106)	0.391% (82.5)	0.373% (74.1)	0.295% (66.5)	0.288% (68.7)
Total	**0.086%** **(273.7)**	**0.070%** **(241.6)**	**0.064%** **(235.9)**	**0.064%** **(252.6)**	**0.062%** **(268.5)**

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 57% of fraud, even though they make up only about 10% of the value of card payments handled by the French schemes.

As domestic transaction amounts showed sustained growth of 9.4%, the fraud rate for such transactions declined slightly to 0.029% in 2007 from 0.031% in 2006, thus remaining at a very low level.

The rate and amount of fraud involving international transactions both increased in 2007. The fraud rate for transactions by French cardholders in other countries increased to 0.476% (corresponding to fraud of EUR 85.3 million), compared with 0.453% (EUR 76.4 million) in 2006. The fraud rate for transactions by foreign cardholders in France fell slightly to 0.288% (EUR 68.7 million) compared with 0.295% (EUR 66.5 million) in 2006. This improvement was probably due to the migration of French acceptance systems to EMV, which provides more secure handling of payments made with foreign cards.

Box 3 – Breakdown of losses from fraud

Building on work initiated in recent years, 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 these indicators 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 2007: 3% for cardholders, 51% for issuers and acquirers, and 46% for merchants, mainly in distance selling.

Furthermore, out of the EUR 268.5 million in fraud recorded by the French schemes in 2007, it is estimated that foreign schemes bore EUR 78 million, or 29%. This is notably attributable to the migration of French schemes to EMV. In recent years, this shift has enabled a significant portion of fraud to be transferred to foreign schemes that have not yet completed the migration to EMV, under international liability-sharing rules.

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.

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

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 fell from 0.024% (corresponding to fraud of EUR 59.1 million) in 2006 to 0.017% (EUR 45.4 million) in 2007, owing to efforts to bolster cryptographic systems. Face-to-face and UPT payments accounted for 70% of domestic card transactions, and 40% of fraud in value terms.

– the fraud rate for card-not-present payments rose in 2007 to 0.236% (corresponding to fraud of EUR 50.1 million), compared with 0.199% in 2006 (EUR 33.2 million). Card-not-present payments thus accounted for 5% of the value of domestic card payments but for 44% of fraud in value terms. This increase took place amid substantial growth in the volume and value of card-not-present payments (27.9% between 2006 and 2007). Furthermore, the 2007 figures reveal a widening gap between the fraud rate for payments by post or phone and the fraud rate for online payments, which rose sharply.

  Statistical analyses by Fevad corroborate data gathered by the "CB" Bank Card Consortium, while showing that these data likely include some 20% of disputes that are ultimately settled by cardholders. Comparative analyses by the consortium and Fevad on the latter's sample show that the fraud rate for domestic card-not-present transactions was stable in the four-party card category, at 0.12%, after 0.13% in 2006. The large discrepancy with the overall fraud rate for card-not-present payments found by the Observatory (0.236%) suggests that, as last year, the fraud rate is lower among e-commerce specialists. Fraud rates do indeed vary across sectors of activity and even from one merchant to another, depending on the security measures in place.

  Last year, the Observatory stressed the importance of compliance with the security measures recommended by issuers, especially systematic use of the CVx2 code for card-not-present payments and verification of the buyers' identity by merchants[14]. With fraud on the rise in card-not-present payments, the Observatory is reiterating this recommendation. Moreover, the Observatory recommends that all affected participants implement interoperable[15] security solutions to enhance cardholder authentication;

– the fraud rate for cash withdrawals was well contained at just 0.020% (corresponding to fraud of EUR 19.0 million), after 0.019% (EUR 17.4 million) in 2006. Withdrawals represent some 24% of domestic transactions and account for 17% of the total fraud amount.

[14] See the first chapter of the Observatory's 2004 Annual Report for an overview of security policies in this area.

[15] allowing cardholders to use the same solution with different merchants, no matter which banks they deal with.

	Fraud rate (Fraud amount, EUR million)	
French issuer – foreign acquirer	**2006**	**2007**
Payments	**0.421% (54.0)**	**0.483% (65.2)**
- o/w face-to-face and UPT	0.288% (28.1)	0.299% (30.0)
- o/w card-not-present	0.840% (26.0)	1.024% (35.1)
- o/w by post / phone	0.684% (5.7)	0.790% (7.6)
- o/w online	0.898% (20.3)	1.117% (27.4)
Withdrawals	**0.555% (22.4)**	**0.455% (20.0)**
Total	**0.453% (76.4)**	**0.476% (85.3)**
Foreign issuer – French acquirer	**2006**	**2007**
Payments	**0.344% (61.5)**	**0.334% (62.8)**
Withdrawals	**0.107% (5.0)**	**0.117% (5.9)**
Total	**0.295% (66.5)**	**0.288% (68.7)**

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 figures show, as they do in the case of domestic transactions, that:

– The fraud rate for face-to-face and UPT payments is much lower than the fraud rate for card-not-present payments (0.299% vs 1.024%);

– The fraud rate for card-not-present payments is higher among online payments than among other types of card-not-present payments (1.117% vs 0.790%).

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)**

The most common type of fraud involves lost or stolen cards. Such fraud increased in 2007 and accounted for over 50% of fraudulent domestic payments. Counterfeit cards accounted for just 5% of fraudulent domestic payments, down from 16% in 2006 and 25% in 2005. On the other hand, fraud involving the use of appropriated card numbers for card-not-present payments increased further in 2007, after previously rising in 2005 and 2006, and accounted for around 40% of fraudulent payments. "Other" fraud was stable. This category of fraud is often used by three-party card schemes to report the opening of fraudulent accounts or the filing of credit applications under false identities. Such practices account for some 50% of the fraud involving these cards.

	All types of cards		**Four-party cards**		**Three-party cards**	
2007	**Amount** (EUR million)	**Share**	**Amount** (EUR million)	**Share**	**Amount** (EUR million)	**Share**
Lost or stolen cards	57.7	50.4%	55.2	52.3%	2.5	28.3%
Intercepted cards	1.3	1.1%	0.4	0.4%	0.8	9.4%
Forged or counterfeit cards	5.6	4.9%	5.2	4.9%	0.7	4.6%
Appropriated numbers	45.5	39.7%	44.8	42.4%	0.7	7.9%
Other	4.5	3.9%	-	-	4.5	49.7%
Total	**114.5**	**100%**	**105.6**	**100%**	**9.0**	**100%**

Source: Observatory for Payment Card Security

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

Box 4 – Indicators provided by law enforcement agencies

In 2007, law enforcement agencies noted a slight decline in the number of payment card fraud cases, recording 53,458 instances of payment card counterfeiting and use. In all, 3,256 individuals were charged and 1,349 suspects were detained.

Attacks on ATMs were also down, with 391 such attacks registered in 2007, compared with 515 in 2006, 200 in 2005 and 80 in 2004. There were also 36 attacks on card-operated fuel pumps.

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

– two ringleaders of an international network were arrested, resulting in the seizure of more than 1,000 counterfeit payment cards and over EUR 100,000 in stolen funds;

– payment card counterfeiting production sites were dismantled, which included the seizure of equipment (computers, embossing and thermal printing devices) as well as thousands of euros in stolen funds.

In 2007, French law enforcement agencies continued to cooperate closely with their opposite numbers elsewhere in Europe, particularly in Eastern Europe. This included actual operational initiatives, which are needed to counter the rise of organised groups and cross-border crime. As part of this, the first two European arrest warrants were executed in Romania on behalf of the French authorities.

3 TECHNOLOGY WATCH

3 1 Security of card payments and European standardisation

In its 2005 Annual Report[16], the Observatory welcomed the move provided by the decision of the European Payments Council (EPC) to adopt the SEPA Cards Framework (SCF) as a step forward in the European harmonisation process. It stressed that establishing technical standards for all areas of interface between the parties to card transactions was vital to promoting high levels of card security in Europe. The Observatory also recommended introducing security certification for cards and terminals based on a common methodology used by European card schemes to ensure equal levels of security for these devices.

In 2006 and 2007, the Observatory monitored progress in work in these areas. A range of initiatives were launched to achieve "standardisation", that is, convergence in the operating and communication rules and technical specifications of equipement used for card payments in Europe.

The following sections explain the importance of standardising card transactions in Europe and reports on progress in standardisation and security certification initiatives as at end-2007.

Importance of standardisation for card payments

Card payments involve multiple participants (including holders, merchants, technical providers, financial institutions and, potentially, exchange systems), whose hardware must be capable of exchanging the transaction data, i.e. merchant, cardholder and card identifiers as well as the payment order. To make these exchanges possible, the hardware and communication protocols used by the card payment schemes – in particular for cards, terminals and the servers employed by acquirers and issuers – must be standardised.

Standardisation may extend to various levels of detail depending on the degree of interoperability sought. Common operating and interconnection rules are needed to enable data transactions between the different devices of a card payment scheme and to ensure that these transactions can be executed on different types of equipment.

In a situation where a four-party card scheme coexists with multiple three-party schemes in the same market, it is possible, as in France, for the schemes to agree on a basic level of standardisation so that three-party cards can be used on the accepting devices of the four-party scheme.

16 See the 2005 Annual Report of the Observatory for Payment Card Security, Chapter 4, p. 39.

Box 5 – Standardisation

A standard is defined as "a reference document that answers technical and commercial questions asked on a recurring basis by stakeholders concerning products, capital goods or services. It is prepared on a consensual basis by all market stakeholders (i.e. producers, users, research centres, public authorities, consumers...). Standards are applied on a voluntary and contractual basis, although they may be made mandatory in some cases, such as safety-related areas and government procurement" (source: AFNOR[17]). Standards may be set in technical areas but may also deal with organisation or services. Standards may be prepared at domestic, European or international level.

Standards may be prepared by recognised international standard-setting bodies, such as the International Organization for Standardization (ISO), or by domestic standard-setters, such as France's AFNOR, which use methodologies that seek to build consensus. Other widely-used standards may be produced in a less formal setting, for example by one or more market stakeholders, but propose similar solutions to those prepared by the recognised standard-setters.

Standards are generally used to facilitate exchanges by harmonising rules and practices and by providing common reference frameworks. They are also used to make products and services comparable and compatible with each another.

Standards may go into various levels of detail. In the area of card payments, they can be grouped into three levels:

– user needs: the first level consists in defining the basic requirements that a card payment scheme must meet, such as the need for interoperability with international schemes, reliability, security, and ease-of-use for cardholders. The banking industry does most of the standard-setting at this level;
– functional specifications: the next level consists in setting standards for scheme functionalities. These standards are established jointly by the banking industry and by card and terminal manufacturers. They define exchange protocols and data formats so that these can be processed by any kind of device, regardless of the manufacturer or IT provider chosen;
– technical specifications: this is the most detailed level. It covers in particular the products' technical architecture and IT development. Manufacturers determine these technical specifications.

Furthermore, the creation of the Single Euro Payments Area (SEPA) extends the need for interoperability to exchanges between existing payment card schemes, in particular because cards issued by one scheme must be accepted by the others.

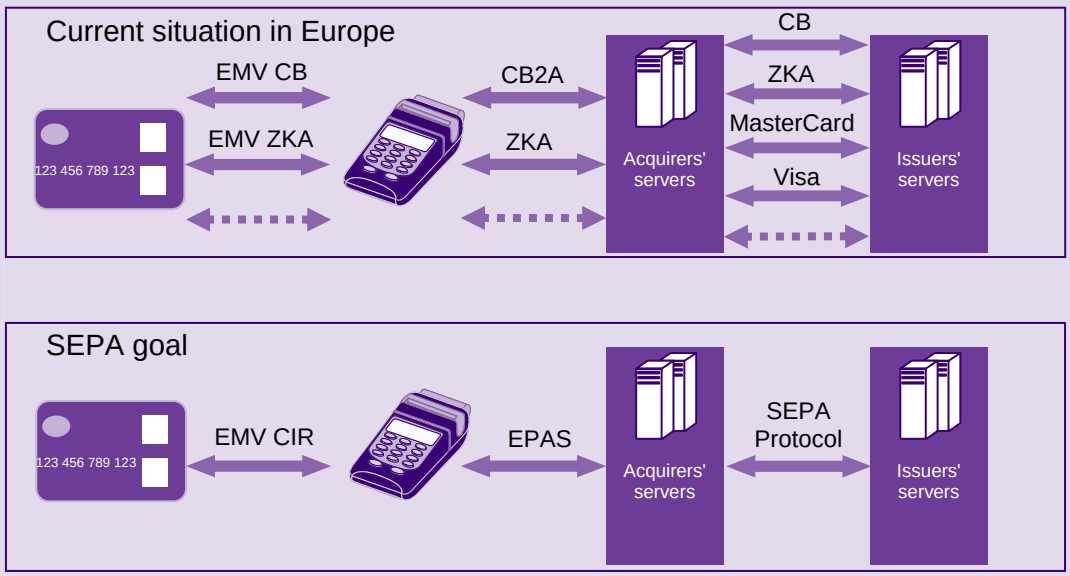
The expected benefits are mostly to do with simplifying the technical resources that card scheme participants have to deploy. Through standardisation, issuers can be sure that their cards will be accepted across a wider European network. Merchants will be free to choose their acquirer but will keep the same hardware at the same time. Card and terminal manufacturers will find it easier to distribute their products on a pan-European market.

[17] The French standards institute.

Box 6 – How SEPA is affecting technical standards

Europe presents currently a fragmented picture made up of some 30 domestic four-party card schemes. For now, cross-border card payments are therefore mainly effected through the international networks such as Visa and Mastercard. The upshot is that each card scheme has its own specifications for exchanging data between the card and the terminal, between the terminal and the acquirer's server, and between the acquirer's and issuer's servers.

European standardisation initiatives should result in common specifications being adopted for all phases of the card payment cycle. For instance, one aim of the harmonisation push must be to establish a single method for implementing the EMV standard for card/terminal dialogue, which is not the case at present.



The EPC's standardisation choices

In addition to the recommendations set out in the SCF[18], particularly on the systematic use of the EMV standard, the EPC identified a need to standardise the three interfaces that make up the entire card payment cycle:

– between the **card and the terminal**;

– between the **payment terminal and the acquirer's server**;

– between the **servers** operated by the transaction **acquirers** and card **issuers**.

For the most part, the EPC is relying on initiatives being conducted by outside working groups set up by banks, card schemes and manufacturers. These efforts are primarily centred on face-to-face payments. The EPC has signed agreements with these working groups with a view to disseminating their specifications as standards when time comes.

The EPC has made adoption of these specifications conditional on the respect of three requirements:

– the specifications must meet the needs set out by the EPC and be freely available[19];

– they must be compatible with existing worldwide standards;

---

18 cf. version 2 – March 2006

19 At the very least, the financial and contractual terms governing access and utilisation must not be an obstacle or barrier of any sort to developers and users.

– it must be possible to maintain and develop the standards.

Card/terminal interface standardisation

A key SEPA interoperability goal is to make it technically possible for a card issued in any European country to be accepted at any terminal in the area. To meet this goal, the card/terminal interface has to be standardised. Compounding this concern, there is a need for compatibility with existing international standards so that cards issued by European networks can be accepted outside SEPA.

As from 2005, the EPC selected the EMV technical specifications for this interface. These specifications were produced by EMVCo, a consortium ("Europay, Mastercard, Visa" – EMV, that also includes the Japanese network JCB). As a result of this decision, cards issued by European four-party card schemes will be chip & PIN cards, meaning that security levels are equivalent to those enjoyed in France since 1992. The Observatory has already expressed its satisfaction on this point.

In addition, the EPC expressed interest in taking standardisation work further by drawing on specifications for cards and terminals proposed as part of external initiatives.

Cards:

– Establish common methods for implementing EMV: the EMV standard allows for different implementation options. Schemes may therefore implement the standard differently, which can affect interoperability. For this reason, standardisation in this area has to be completed by choosing between the various available options. In other words, rules must be laid down for the payment application installed on the terminal (e.g. whether it checks the card's PIN) and for the issuer's network (e.g. maximum amount authorised). This is the aim of the Common Implementation Recommendations Working Group (CIR–TWG)[20], which has prepared a set of Common Payment Application (CPA) specifications for payments in EMV mode. The security features of French “CB” cards, which include dynamic authentication and PIN verification, are compatible with this draft standard.

Terminals:

– Harmonise transaction stages: the EPC recommends preparing a single model for the different stages of a transaction. All SEPA terminals would follow this model, thereby ensuring that all payment functions are handled in a uniform manner. This would also reduce technical incidents as well as development and certification costs.

  The CIR group drafted an initial set of functional specification (FAST) that describes the different stages of a transaction. This standard is currently being drawn up. Its adoption by the EPC would make it possible to carry out the security checks that are currently used with French cards (dynamic authentication, PIN verification, maximum amounts, etc.).

– Harmonise the information displayed to cardholders: since the EMV standard does not specify the cardholder/terminal interface, the CIR group included common display rules (such as detection of the card's country of origin) and standardised messages in its draft FAST specifications. Any steps to standardise the display rules would not directly enhance security, although they would help to make cardholders both more comfortable and more alert.

[20] CIR-TWG is a working group set up by European EMV users.

– Provide specifications for the hardware and software used in terminals and unattended payment terminals (UPTs): the ERIDANE[21] group is currently preparing specifications for the components that go into accepting devices, such as keypads, screens, readers or software. This standard will mean that components are standardised, regardless of the brand of the terminal. This should make the equipment easier to manufacture. The specifications do not affect terminal security much, although some of the extensions envisaged by the ERIDANE group could include secure mechanisms for the connexion of terminals and UPTs to open networks. The EPC has not yet issued a decision on application.

The EPC may also endorse the principles defined by the standard-setting bodies created by international networks. These bodies are also setting standards for certain types of devices in order to enhance card payment security. PCI SSC ("Payment Card Industry – Security Standards Council") founded by American Express, Discover Financial Services, JCB International, Mastercard Worldwide and Visa Inc, sets security standards for the card industry. The EPC now participates in a consultative capacity in both EMVCo and PCI SSC. The main guidelines issued by PCI SSC concern the protection of card data and PINs in terminals, UPTs, ATMs and merchant databases. Since most of the PCI SSC founding networks are from America and use the magstripe technology, some of the Council's guidelines are geared towards transactions that employ this method. The security measures that merchants are required to take are by definition less suited to markets where card payments are based on a chip & PIN system, as in France, because the due diligence requirements are not appropriate for all the types of fraud that affect chip cards[22]. If these standards were not adapted to the specific features of European market, adopting them would have a major impact on French merchants and issuers, which over the last 15 years have based their security arrangements on the use of chip cards[23].

Terminal/acquirer interface standardisation

SEPA's goal is to enable merchants to freely choose the acquirer that offers the best-priced services. Achieving this objective will also require further standardisation in different areas of the terminal/acquirer interface, including authorisation, acquisition and terminal management.

There are currently many protocols for connecting terminals to acquirers' servers (authorisation and batch transfer). But though they are based on the international standard ISO 8583[24], these protocols, which deal with authorisations, remittances and other areas, are not compatible.

French card schemes, for example, use the “CB2A” protocol prepared by “CB” Bank Card Consortium. The EPC is considering preparing a single protocol that would allow the same terminal to accept cards issued by different schemes. However, it has not said whether such a specification is mandatory, nor has it indicated what level of technical detail would be necessary. The EPAS consortium (Electronic Protocol Application Software)[25] is seeking to establish a single communication protocol. The main technical guidelines in this area have yet to be determined. This protocol could be based on the current international standard, ISO 8583, or on a new standard, ISO 20022[26], which is already going to be implemented in other parts of the card transaction chain (acquirer/issuer) and for other payment instruments

21 ERIDANE comprises European card payment schemes, terminal manufacturers and merchants.

22 See the 2005 Annual Report of the Observatory for Payment Card Security, § 3.2 p. 30.

23 See the 2006 Annual Report of the Observatory for Payment Card Security, p. 34.

24 Specifications for the exchange of financial transaction card originated messages.

25 EPAS brings together card schemes, merchants and manufacturers.

26 ISO 20022 is also called UNIFI, for "UNIversal Financial Industry message scheme".

(SEPA credit transfers and direct debits). The protocol will not cover protection of data exchanged on open networks. This type of protection can be delivered only by using specific security measures, such as encryption key management facilities.

Standardisation of exchanges between acquirers and issuers

Acquirers must be able to contact issuers, first to request transaction authorisations, and then to initiate clearing and settlement. Technical infrastructures used to convey authorisations and transaction files between acquirers and issuers are often closely linked to the card scheme. Where external participants are involved in the transaction, the scheme may transmit the transactions to the affected networks (as it happens with foreign cardholders in France), or conversely, re-route transactions by French cardholders at foreign merchants. The vast majority of national and international card schemes have their own communication protocols based on ISO 8583. However, differences in the implementation of these protocols require that the schemes set up special conversions gateways in order to be able to exchange between each other.

To promote competition, the EPC has introduced the principle that from now on acquisition infrastructures must be separated from card payment schemes properly. Acquirers or issuers must be free to choose authorisation and clearing infrastructures without having to use the ones proposed by the national and international card schemes to which they belong[27].

Standardising exchanges would go a long way to achieving this objective, but the EPC feels that it does not need to create a new standard in the short term. It believes that existing ISO 8583-based standards such as those prepared by Visa and Mastercard can continue to be used. In any case, these standards are necessary to process international transactions.

To make longer-term changes, however, the EPC began a series of preparatory work in April 2007 aimed at specifying its needs and identifying and describing the data to be transported (with reference to the formats defined by the EMV and UNIFI standards). It is also doing a stock-taking of the various protocols in use, assessing differences and considering ways to reduce the total number. For the time being, it is difficult to judge how a future standard might affect the security of these data exchanges. But a standard of this kind would reduce the conversion problems caused by differences in ISO 8583 implementation.

Furthermore, the proposed alliance of some national schemes, called EAPS (“European Alliance of Payment Schemes”) also plans to develop a new ISO 8583-based standard for exchanges between acquirers and issuers.

Certification

For the time being, the procedures used to certify that cards and terminals comply with card schemes' functional and security requirements are determined either at national level or by the schemes themselves[28]. As a result, security requirements may vary from scheme to scheme, and manufacturers that are required to have their products certified face repeated and costly certification processes.

---

27 This is the "unbundlinge" concept put forward in the SCF.

28 See the 2005 Annual Report of the Observatory for Payment Card Security for a description of the French system, Box 6, p. 29.

The SCF has set down several principles to facilitate convergence in this area:

– card payment schemes must no longer conduct functional and security certification themselves. Instead, they should use the services of independent organisations. This measure is intended to make it easier to have a single certification so that equipment can be used by different card payment schemes;

– security evaluation methods, such as the "Common Criteria" standard[29], that create the possibility for mutual recognition by countries and card payment schemes, should be used.

However, the SCF does not prescribe measures to standardise security requirements or harmonise certification procedures and thus enable mutual recognition by card schemes. Yet harmonisation of these security requirements and certification procedures is a major concern in order to guarantee that the SEPA would not result in lower security levels for cards and terminals. The Observatory already voiced its concerns on this point in its 2005 Annual Report.

The EPC is studying the work being done by the Common Approval Scheme (CAS) Group[30], which prepares:

– security requirements for terminals and UPTs: these requirements cover all the components of these devices, i.e. not just the keypad, or PIN Entry Device (PED), but also the magstripe reader and the software components that manage the card's data. For PEDs, the EPC seems to be leaning towards the PCI SSC specifications (PCI PED V2.0), which are on a par with those prepared by CAS. However, the PCI PED requirements also cover magstripe readers, which could prove costly for European card schemes which do not use the magnetic stripes.

– a common evaluation methodology: CAS recommends adopting the “Common Criteria” methodology currently used for cards in France and Germany and for terminals in the UK. Following this recommendation would make it possible to maintain the quality of the evaluation procedures used in these countries today and would provide the basis for a European system of mutual recognition;

– a European functional and security certification scheme for cards and terminals: it is necessary to establish procedures for evaluation and certification by specialised research centres and bodies, as well as arrangements to ensure mutual recognition of these certificates by the different card payment schemes operating in Europe. The Observatory has previously stressed the importance of such an approach and supported a proposal to amend the Draft Directive on Payment Services. Since the amendment was not introduced, the Observatory is endorsing the initiatives put forward by CAS and calls on the EPC to take them on board.

Availability of standards and product deployment

The EPC plans to make the different standards available by end-2008. Given the changes that will have to be made by stakeholders, it is hard to say at this stage when standardisation will be achieved. The availability of the standards will determine the beginning of the development work. The latter may last 6-18 months. Interoperability tests, which will also take several months, will then have to be conducted. Therefore, no fully SEPA-compliant products will be available in the timeframe provided for the implementation of the SCF (2008/2010).

---

29 See the 2005 Annual Report of the Observatory for Payment Card Security for a description of the French system, Box 12, p. 43.

30 The main European and international card schemes make up the CAS group.

In the case of payment terminals, the speed with which SEPA-compliant equipment is deployed will depend on the rate at which the equipment in place is replaced, a task usually performed by merchants. In France, for example, payment terminals are largely implemented (over a million) and most of them were recently replaced (starting in 2002). Typically they have a depreciation period of more than seven years. Pending the migration of terminals to the new SEPA standard, acquirers' current servers will however be able to convert protocols inherited from existing schemes so that they can be transmitted to the exchange systems in the required format.

French “CB” cards already comply with the EMV standard. Changing them to accommodate the CIR group's recommendations will take at least two to three years given the validity period of the cards, which determines when they are renewed.

Despite the delay in preparing a common standard for the data exchange infrastructures, migration could be effective within a reasonable timeframe given that a limited number of servers have to be modified and conversion applications could provide assistance.

Box 7 – Timetable for preparing and implementing standards

Specifications	Initiative	Mandatory	Standard available	Implementation
Card - Terminal				
EMV card and terminal standards	EMVCo	yes	available	CB 100% EMV
EMV detailed implementation recommendations	CIR	-	End 2008	
Terminal - Acquirer				
Functional and security requirements	EPAS	yes	End 2008	From 2009
Terminal security requirements	CAS	yes	End 2008	From 2009
Detailed technical specifications	EPAS	-	End 2008	From 2009
Terminal functional architecture	ERIDANE	-	End 2008	From 2009
Terminal internal interface specifications	ERIDANE	-	End 2008	From 2010
Acquirer – Issuer				
Functional requirements	EPC A2IEG	yes	End 2008	From 2009
Detailed technical specifications	EPC A2IEG	-		
Certification				
Common security requirements	CAS	yes	End 2008	From 2009
Common security certification methodology	CAS	-	End 2008	From 2009
Common functional certification methodology	CAS	-	2008/2010	From 2010

Conclusion

Enabling interoperability between payment schemes in Europe is a key goal of the SEPA cards project. Whereas the individual schemes currently use standardised data exchange protocols and hardware, common standardisation across the schemes is still at an embryonic stage, which is preventing genuine interoperability. The European opening of payment systems therefore implies common standardisation. But it must contribute to a high level of security – at least on a par with that enjoyed in France today.

The EPC is considering the reports of expert working groups on this issue and may base SEPA standards on these contributions.

Now that the necessary standardisation work has been identified, an overall timetable has been prepared showing the main deadlines for finalising the standards along with their implementation periods.

The EPC has also stepped up its dialogue with international standard-setters and is cooperating in a consultative capacity with bodies such as EMVCo and PCI SSC in order to convey its members' interests.

Further to research that it carried out in 2005, the Observatory wishes to reiterate the importance of high and uniform security levels for hardware and communications when it comes to setting standards. In particular, these standards must be consistent with the assessment of risks affecting payment cards in Europe. Accordingly, the Observatory is supporting work aimed at promoting a common methodology for the security certification of cards and terminals, which will enable mutual recognition by the schemes of each others' certificates. The Observatory considers essential that European stakeholders benefit from a certification scheme that is specific to Europe and that they should maintain resources and skills in this area.

The Observatory also wishes to emphasise that the governance of these standards has strategic importance for the security of card payments in Europe. It believes that the European schemes should play an active part in this governance.

3|2 Security of new methods for initiating card payments (via mobile phones and contactless cards)

Technological progress allows changes in the methods used to initiate card payments, i.e. formulate payment orders. Until now, face-to-face payments have been chiefly based on reading the card's magnetic stripe or setting up a dialogue between the card's chip and the terminal or UPT. In each case, contact between card and terminal is required to read the information on the card. The plastic card format, which quickly became standardised worldwide, paved the way for interoperability between terminals and the cards of different issuers. The arrival in France in the late 1980s of chip cards with embedded payment application did not result in any changes to the card format because compatibility with existing terminals had to be maintained, for cost reasons but also to ensure interoperability with the still-dominant stripe method. Since the card format stayed the same, the method used to initiate payments changed only to the extent that the card and terminal or UPT communicated through a dialogue with the chip rather than through a magnetic stripe.

Recent technological developments have got the stakeholders thinking about new applications that could change the methods used to initiate card payments. In particular, the standard plastic card format is no longer needed to execute the payment functions typically embedded in the card's electronic chip. Meanwhile, the emergence of "contactless" technologies means that the card no longer has to be inserted in the terminal. The combination of these developments has given rise to contactless cards[31] and to new devices, such as mobile phones, to carry the chip with the payment application and dialogue with terminals in contactless mode.

In building on its 2004 study on contactless cards, the Observatory looked at the security aspects of these two new modes of initiating payments, based on trials currently ongoing in

[31] The first contactless cards, which were mainly introduced in the USA, transmitted a copy of the magnetic stripe data. Tests conducted in France are looking at chip cards, which is why this study considers only contactless chip cards.

France. The study does not deal with prepaid cards, which are examined as part of monitoring work done on issuers and acquirers security policies.

Features of the new methods for initiating card payments

Two main types of mechanism are being tested out in France:

– solutions based on standard-format payment cards (ISO 7816-1 compliant) fitted with a chip that runs the payment application plus a device that enables contactless communication with payment terminals. The device comprises a microprocessor and an antenna that can communicate using the "near field communication" (NFC) protocol. It is designed to function at close distances, requiring the card to be brought up to less than 10 cm from the terminal;

– payment solutions using mobile phones fitted with a chip-based payment application and an NFC device for contactless communication.

In both cases, the contactless communication mode complies with ISO 14443, which enables data to be exchanged between a chip and a contactless reader on a terminal or UPT located a few centimetres away.

Initiating payment by a contactless card

The contactless cards now beginning to be tested out in France are based on specifications conceived by Visa and MasterCard. Although designed to dialogue in contactless mode, these cards can also still dialogue with the payment terminal in contact mode (so-called "dual cards"). The initiation of the transaction is of course altered when the contactless mode is used, as are the subsequent processing stages, which include some adjustments relative to a standard EMV transaction.

The use of contactless mode allows payments to be initiated more quickly – a valuable feature in some commercial settings where swift execution of transactions is of paramount importance. The card and terminal dialogue via the NFC protocol in less than one second. The card does not have to be entered into the reader, which processes the transaction offline (to avoid having to take the time to call the server of the acquirer or issuer). To make the system more user-friendly, the PIN is not checked and the holder does not confirm the payment order given how briefly the card is held up to the terminal. The card is simply brought up to the reader to trigger payment. However, to ensure security, contactless mode is used only up to a maximum amount of around €20 or €30, depending on what is allowed by the issuing and acquiring banks. Also, if a certain number of contactless transactions are performed, or if these transactions combine to reach a set amount, the holder must then switch to contact mode. The PIN must be checked and/or a request for authorisation is needed to reset to zero the cumulative transaction totals and so to enable contactless operations to resume.

Initiating a payment by mobile phone in contactless mode

In the field of mobile telephony, many international stakeholders are considering different ways of allowing contactless payments using mobile phones. At least two technical models are now beginning to be tested out in France:

– the first of these consists in embedding the payment application of the issuing bank in the Subscriber Identity Module (SIM) chip managed by the phone company[32]. The chip then runs the operations needed to initiate payments. The phone is also fitted with an NFC device to communicate with the payment terminal;

– the second approach entails putting the payment application on a dedicated chip, called "Secure Element", that initiates the payment transaction, controls NFC communications and holds digital certificates. This type of architecture can be used to develop services independently of the infrastructures operated by telecommunication firms, i.e. without using the SIM chips or associated telephony services[33].

In both cases, the payment application is hosted on an electronic component that has not necessarily been issued by banks even if they retain control over security aspects. The application is indeed included in a secure area reserved for the issuing bank, which sets specific requirements for that space. The payment application may be pre-loaded during personalisation or downloaded over a secure channel through the mobile phone network. The application can then be remotely activated, suspended, deactivated or updated.

With mobile phones, payments are by definition initiated in contactless mode. The telephone network is not used. The NFC device fitted on the phone allows the payment application and the terminal to dialogue contactlessly, just as contactless cards do. The payment application can be used to pay amounts of any value, with the option of dispensing with PIN entry or customer confirmation for transactions below a certain value. The bank account to which the payment application is linked is debited. Once the transaction has been recorded on the terminal, it is transmitted to the server of the acquiring bank like any other card transaction.

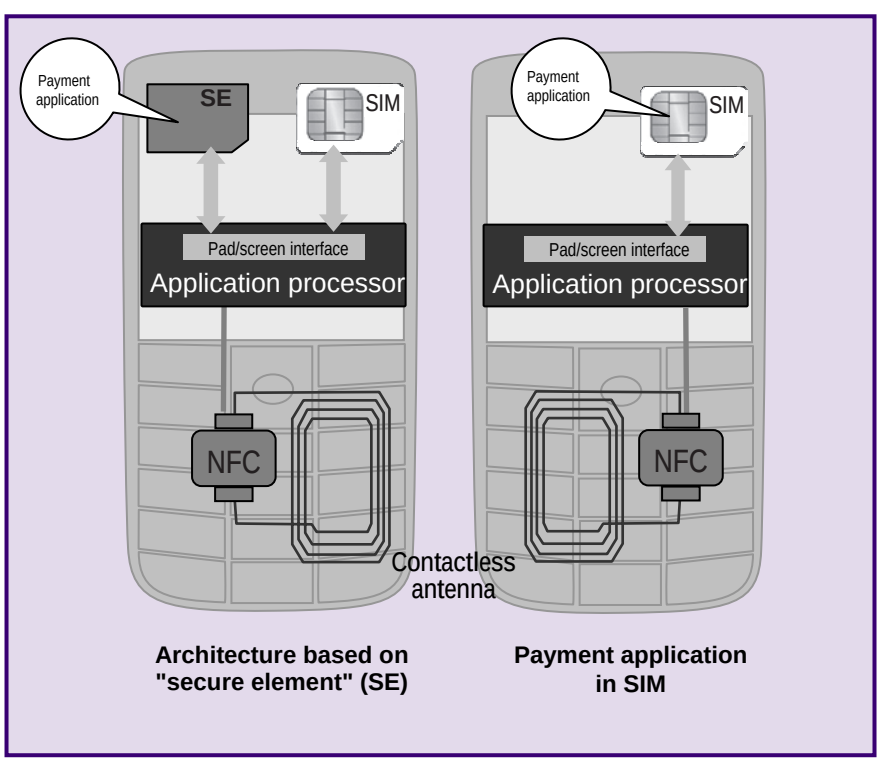


Illustration of two technical models used to put a payment application on a mobile phone

[32] The GlobalPlatform Standard used with SIM chips provides for separate "Security Domains" so that different applications can be embedded in these chips.

[33] In a third possible scenario, the mobile phone could be fitted not with a payment application of the sort used by cards, but with a simple authentication device that would allow remote access to a payment application. This approach, which is not studied in this paper, bears a closer resemblance to the remote electronic payment order solutions used in e-commerce.

Other solutions on the table are not being tested out in France. Some of these are based on connecting the processor that manages the payment application to the memory expansion slot fitted on the latest generation of phones. The processor operates as an independent module like a memory expansion card. It can therefore be used on the phone of the user's choice, leaving consumers more flexibility when it comes to selecting their equipment ("SecureMMC" technology[34].)

Impact on security

Contactless approaches, whether card- or phone-based, differ from card payments in contact mode in a number of ways:

– the payment terminal and the card or mobile phone communicate using radio frequencies;

– the method used to authenticate the holder is different. For example, in some cases, such as small-value transactions, the PIN does not have to be entered and the holder does not confirm the payment order;

– when mobile phones are used, the chip with bank data may not belong to the bank.

As a result, these payments raise specific protection issues compared with card payments in contact mode. Addressing these issues may require new security mechanisms. The legal provisions that protect holders who dispute payments may also apply to this new approach to initiating payments.

Required security measures for contactless payment approaches

Protection to prevent exchanged data from being captured

In the solutions trialled in France, the information typically exchanged between the card and the terminal are the card number (PAN)[35], the amount of the transaction and the card authentication data. This information is sensitive or even confidential and must therefore be protected from being captured and reused for fraudulent purposes. This accounts for a number of protective measures included in the trials.

To prevent captured data from being reused, the card or mobile phone payment application is authenticated dynamically at each transaction. Also, mobile phone solutions use a PAN dedicated to contactless mode (different PAN from the payment card PAN, digital certificate) that could not be used for other payment modes if intercepted.

Current contactless card payment applications do not require the PIN to be presented[36]. If a mobile phone is used, the PIN is entered directly onto the phone's keypad and is not transmitted to the terminal.

Under the current specifications published by the Visa and Mastercard international networks, the holder's first name and family name may be transmitted without protection in contactless

---

[34] The "Secure MultiMediaCard" technology is based on the specifications for "MultiMediaCards" (MMCs), flash memory cards that come in a number of standardised formats and that are widely used as multi-media storage devices for mobile electronic equipment.

[35] "Primary Account Number", which comprises data identifying the issuer and the account of the card holder.

[36] This is a design choice, not a technical problem. Other contactless applications currently at the specification stage include transmission of the encoded PIN between terminal and card.

mode, which raises data protection issues. Mobile phone payment solutions being trialled in France do not manage these data, hence avoiding the problem.

Activating the payment application without the holder's knowledge

The use of contactless interfaces raises new issues in terms of protecting card contents because it becomes possible to establish a dialogue with the card, and thus obtain information from it or even trigger a payment transaction without the holder's consent – an act known as "tele-pickpocketing".

For this reason, it is vital to take steps to ensure that these cards do not provide any information that can be directly used by fraudsters. In principle, the short operating distance of the contactless protocol should mitigate this risk, because it is extremely difficult to activate a card and read it on a fraudulent contactless terminal beyond a very short distance.

But to prevent any risk – particularly the threat of a relay to a remote device used by a fraudster – the terminal should be able to detect an unusually long delay in carrying out the transaction, which may occur if a relay is being used. The value of this type of counter-measure still has to be evaluated, especially given the constant improvement in technologies. Protective measures to render the card inoperative without any action on the owner's part should also be studied (protective case, on button, etc.).

In mobile phone solutions, the payment application is activated either by the holder before bringing the phone next to the terminal in order to make the payment, or by the terminal, with the holder potentially but not necessarily entering a PIN as confirmation. Moreover, to protect the integrity of the mobile phone payment application, the promoters of this type of solution allow new applications to be sent to the "Secure Element" or to the phone's SIM only if they are encoded and signed by the bank and transmitted by the operator over a secure channel (via SMS transmission).

Theft

Insofar as the PIN does not have to be entered and the card's validity is not checked online, a stolen card can be used to make small-value purchases. The card payment schemes and banks have taken steps to limit the risks introduced by this new type of card usage by introducing a sophisticated risk management system based on counters that switch the card back to contact mode when they reach a given ceiling. To set the counters back to zero, the holder has to be authenticated and online authorisation given. Events tracked by the counters include the number of transactions and the total value of unverified transactions. These counters therefore limit the financial losses that could be incurred if a contactless card or mobile phone is stolen. However, for this, the counters must be well protected against tampering – a feature that must be considered at the design stage and validated in security evaluations.

Contactless mobile phone payments offer scope for similar risk management arrangements that, for example, require an authorisation request and/or holder confirmation when set levels are breached, before offline payments are once again allowed. From an organisational perspective, the mobile telephony environment is more conducive than that of payment cards in several regards. In particular, if the phone is stolen, the telecommunications operator can block the application if it is on the SIM chip. If need be, the payment application and transaction limits can be quickly adjusted using "over-the-air" (OTA) technology, which allows the payment application to be remotely updated. However, this counter-measure will not work if the user has

configured the phone not to connect with the operator, e.g. if the phone is set to manual network selection mode or if the antenna is disconnected.

Ability of the payment application to withstand attacks

To ensure security, transactions must be carried out in a secure environment. Logical and physical security issues concern the functional module that contains the payment application as well as the phone itself.

Banking authorities currently require payment cards to receive security certification. This is not yet the case for the chips used to make mobile phone payments (i.e. SIM chip or "Secure Element"). But the use of mobile phones to initiate card payments raises the question of controlling access to bank data, especially when the payment application is housed on the SIM chip, which is the property of the phone operator. Evaluation for the functional modules that provide security for this embedded payment application should provide a level of certainty that is appropriate for this particular environment.

It should be possible to modify security levels to meet the requirements of these new functionalities. Several solutions are currently being considered to provide mobile phones with security levels that are appropriate for payment applications. Therefore, one of the aims of the GlobalPlatform standards for SIM chips, for example, is to enable applications and their data to be housed separately and securely. Only the issuing bank can access its application, while the operator merely supplies the secure channel required for such access.

A mobile phone represents a far more complex environment than a chip card or payment terminal. It is a combination of different technological components that have been independently developed by multiple suppliers. Until now, security has not been a major priority in phone design: functionalities and time to market have been far more pressing concerns in recent years. Mobile phones are thus exposed to malware (data capture, simulation of payment application for "phishing" purposes, etc.), which may be spread through channels such as Bluetooth, the internet and WiFi. Furthermore, the introduction of new functionalities and new ways of using mobile phones will expose these devices to more theft, fraud and mischief.

Conclusion and Observatory's recommendations

Technological progress is giving payment card issuers the opportunity to explore innovative face-to-face payment solutions. Contactless technology has brought changes to the methods used to initiate card payments, by enabling cards to dialogue with terminals and accepting devices without inserting it. The same technology, combined with the new ability of mobile phone chips to house payment application, also allows mobile phones to be used to initiate card payments.

These new methods of initiating payments meet the needs of payment situations in which swift transactions are a key concern and are therefore more convenient for holders and merchants alike.

Based on tests of the two types of solution currently being conducted in France, the Observatory sought to assess the differences in terms of security delivered by these solutions compared with current chip cards that function solely in contact mode.

Changes to the way that payments are initiated expose the new contactless card and mobile phone payment solutions to particular risks. In particular, the use of radio frequencies to

exchange transaction data with the payment terminal, or the fact that there is no authentication of the holder nor transaction confirmation for payments below a set amount require appropriate protective measures. To prevent “tele-pickpocketing”, where the payment application is activated or used without the holder's knowledge, the Observatory recommends in particular studying the possibility to introduce measures to ensure, where necessary, that the holder has given his consent. This could include for example making available simple tools for activating or deactivating the new initiation methods or for confirming transactions.

The solutions currently being introduced in France are solely at the trial stage. Security measures have already been implemented and may be supplemented given that the specifications and developments are not yet finalised. It is therefore important for banks, mobile phone operators and their technical providers to continue the risk and security analyses currently underway. That way, before any large-scale roll-out, they can identify the measures needed to protect against the specific risks associated with the new payment initiation methods and to maintain an acceptable level of risk that compares with other payment card approaches. The Observatory therefore recommends that these risk mitigation measures be assessed by an independent and supervised third party. This role is currently performed by the national certification Scheme[37].

The Observatory notes that the authorities that currently provide certification for chip cards operating in contact mode could also handle security certification for contactless cards. Security certification for mobile phones, however, which have a very different operating mode, should reflect the specific features of mobile phone architectures.

The Observatory's Technology Watch group will continue to monitor these new solutions in order to take into account the final specifications and industry developments.

3|3 Progress on the migration to EMV

The implementation of the EMV (“Europay, Mastercard, Visa”) specifications for chip cards in Europe represents a major issue in the fight against cross-border fraud. It concerns both cards themselves and accepting systems (payment terminals, ATMs, UPTs) which need to migrate to the new specifications in order to achieve a uniform level of protection throughout Europe. As it has done in the past four years, the Observatory again measured progress on EMV migration by collecting statistics on the migration in France and Europe from the “CB” Bank Card Consortium and the European Payments Council (EPC). These figures show that the migration has started all throughout Europe. The progression is correct in most of the countries, in accordance with the commitment of European banks within the EPC to complete migration by the end of 2010. The Observatory expresses nevertheless concerns 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 2008, according to statistics compiled by the “CB” Bank Card Consortium, 100 % of “CB” cards, 98 % of payment terminals and UPTs, and 100% of ATMs were EMV compliant. The remaining 2 %

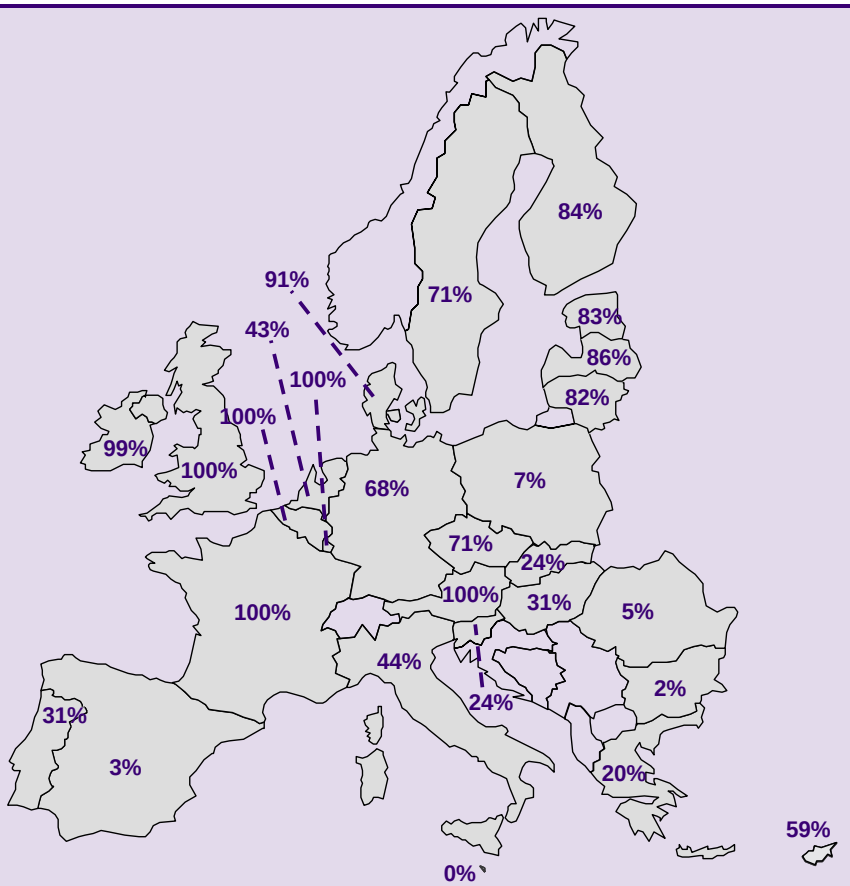
[37] See the 2005 Annual Report of the Observatory for Payment Card Security for a description of the French system, Box 6, p. 29.

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 2008, 61.6 % of the four-party cards in use in the 27 countries of the European Union are now EMV compliant. This represents an increase of 8 percentage points in comparison with March 2007. The situation varies greatly from one country to another (see Box 8). Whereas compliance with the SEPA interoperability rules is being ensured from early 2008 on, the migration in several leading ones has barely started, including Spain or Poland, or has made little progress.

Box 8 – Déployment of EMV cards in Europe

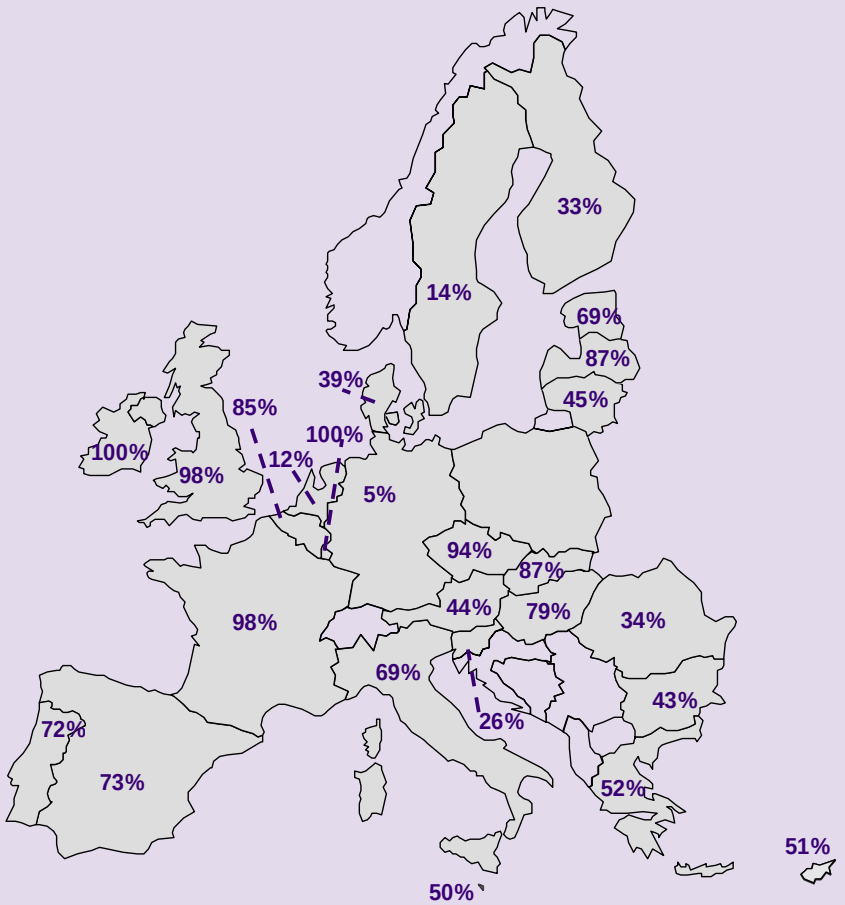


Source : European Payments Council – March 2008

In relation to last year, the map shows a general progress in the deployment of EMV cards. However, several countries such as Spain, Bulgaria, Romania and Poland have barely started migration. The EMV card deployment remains higher in the countries of Northern Europe.

At the end of March 2008, the migration of acquisition systems to EMV had noticeably progressed: 66.9 % of payment terminals (see Box 9) and 83.2 % of ATMs (see Box 10) were EMV-compliant. This represents respectively an increase of 15 and 17 percentage points in comparison with March 2007. The situation still varies considerably from one country to the next both in terms of 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 2008

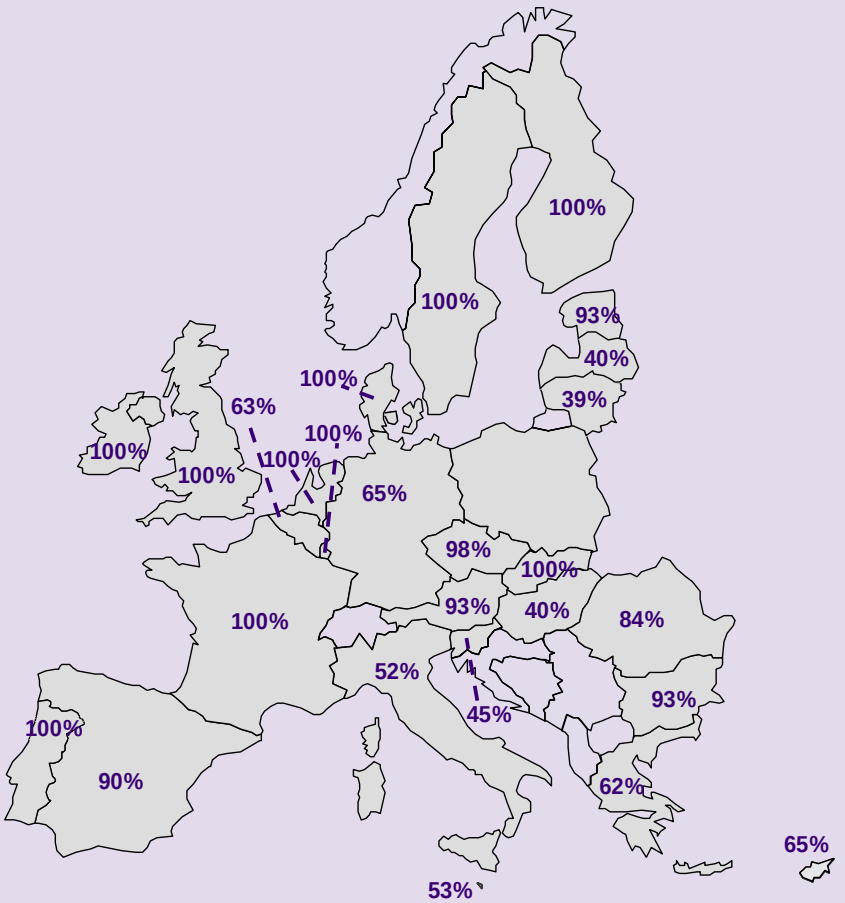
The recorded trend is the opposite of that for EMV-compliant card deployment. The migration of terminals is taking place more rapidly in the countries of Southern Europe on the whole. This pattern corresponds to the top tourist destinations, where the greatest number of cross-border transactions is likely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

The situation in Germany, Sweden and in the Netherlands shows very little development compared to March 2007. The level of EMV-compliant equipment remains low in those countries. On the contrary, the map shows a catch-up in Austria and Denmark, where the migration just started last year.

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

No reliable figures regarding Poland are yet available.

Box 10 – Deployment of EMV ATMs in Europe



Source : European Payments Council – March 2008

Progress on migration of ATMs has been more uniform in Europe and generally more advanced compared to terminal 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 even if their level of EMV-compliant ATMs has doubled.

No reliable figures regarding Poland are yet available.

4 | THE IMPACT OF THE PAYMENT SERVICES DIRECTIVE ON THE RULES APPLIED TO PAYMENT CARDS IN FRANCE

In its 2005 study on payment card security in the context of European harmonisation, the Observatory welcomed the formulation of a Directive on Payment Services enabling a common legal framework for payments in Europe to be put in place. It focused on several points in the draft Directive: the creation of the new category of "payment institutions" alongside the bank status; the definition of payment irrevocability; and lighter regulatory requirements for low-value payments.

The Payment Services Directive was adopted on 13 November 2007[38] and must be transposed into the national legislation of Member States by 1 November 2009. The new Directive substantially restructures existing law. In the area of payment cards, the Directive follows upon harmonisation efforts at the European level that had already resulted in recommendations, notably regarding electronic payments. More recently, two Directives[39] established common rules, which the provisions of the Payment Services Directive will replace.

The objectives of the new European legislation are ambitious and the Observatory wished to take stock of the scale of the changes it will induce in French law. The payments market, including that of payment cards, will thus be opened up to new non-bank players in the shape of payment institutions (I). The Directive will also lead to a harmonisation of national legislation in Member States by laying down common rules for all payment services, thus marking a different approach to that enshrined in French law (II). Moreover, there will be changes to consumer information requirements (III), but also to rules regarding irrevocability and contestation, which will modify the balance of rights between cardholders and acceptors (IV).

4|1 The opening-up of the payment card market to new non-bank players

Like current French law, the Payment Services Directive covers all of the activities related to the issuance and management of payment cards. It will nonetheless foster a substantial change in this market by allowing the emergence of new non-bank service providers: payment institutions.

A scope very similar to current French law

The Directive includes within its scope of application several payment services encompassing all of the activities relating to the issuance and management of payment cards: issuance of cards and acquisition of card payment transaction data, payment transactions whether or not they are made from an account or a credit line and, lastly, cash withdrawals. Since 1984,

[38] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

[39] Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts and Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services .

French law has in the same way included all of these activities, considered as the provision to consumers of means of payment and their management, within the field of banking activities .

The Directive excludes certain so-called “limited use” payment instruments (including cards) from its scope. Article 3(k) of the Directive thus excludes “services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services”. These provisions are close to current Article L.511-7-I, 5°, of the Monetary and Financial Code. But work is currently underway to assess whether the Directive requires a change in the way this Article is applied.

Payment institutions: a new category of payment services provider alongside credit institutions

Unlike current French legislation, the Directive does not limit the provision of payment services to credit institutions alone, but also permits new players, i.e. payment institutions, to carry them out. Payment institutions may therefore provide all payment services identified in the Directive. Ancillary to some provisions of payment services, they may also grant credit. This activity is limited and harmonised for cross-borders transactions, and should comply with national requirements for domestic transactions. The Directive sets out lighter statutory requirements for the activities of these new service providers. Some of these requirements vary depending on the payment services carried out. Thus, payment institutions must have capital of at least EUR 125,000 in order to provide card payment services, and must have own funds at their disposal. In 2005, the Observatory stated its support for the best possible protection for the funds entrusted by users to payment institutions. In this respect, the Directive only requires payment institutions to protect funds received from users when, in addition to their activity as payment services providers, they carry out other activities. But it is interesting to note that its transposition could stipulate that this obligation to protect users’ funds applies even if the institution specialises in the provision of payment services and only engages in this activity. This authorisation will enable payment institutions, via the mechanism of mutual European recognition, to engage in their activity in any other Member State.

With the aim of fostering competition, the Directive also stipulates that payment institutions should have access to payment systems, which includes some card payment schemes. The rules governing access to these payment systems must therefore be “objective, non-discriminatory and proportionate”. In 2005, the Observatory deemed that this access might constitute a risk factor if payment institutions did not provide sufficient financial guarantees. It should be noted in this regard that the Directive’s provisions specify that these rules should not inhibit access to systems “more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system”. Four-party card schemes should therefore give access to any payment services provider that requests it or, at least, should not restrict access to their scheme for reasons not objectively linked to the latter’s security. On the other hand, three-party schemes are not subject to this obligation, since the European legislation considers that these systems’ mode of operation does not require free access to them.

The Directive’s objective of fostering competition in the area of payment services is inseparable from the necessary harmonisation of the rules governing the industry, but also of the rules applied to payment transactions. This harmonisation will have a dual impact on French law: it will lead to a strengthening of the legislative and regulatory framework relating to payments and will promote a new approach to this activity, based on technological neutrality.

4|2 A new approach to the regulations applied to payments

A stronger legislative and regulatory framework

Whereas French law concerning payments is currently largely based on professional rules and much less on legislative and regulatory provisions, transposing the Directive will lead to enshrining a greater number of rules in law or regulation.

For the moment, the legislative part of the Monetary and Financial Code only comprises six articles concerning payment cards (to which the provisions regarding offences should be added). These provisions mainly aim to promote the use of this payment instrument by ensuring good protection for cardholders. In addition to a definition of a payment card and the statement of the principle of the irrevocability of payment orders made using cards, the Monetary and Financial Code stipulates cardholders' level of liability in the event of loss, theft or remote fraudulent use It also lays down the legal period during which a cardholder may make a claim. Otherwise, it is industry-based contractual rules that set out the terms and conditions governing the use of payment cards.

The Payment Services Directive establishes a much more comprehensive framework that sets out the requirements regarding information and the rules applied to payment transactions with respect to consent, revocation, contestation and execution (Titles III and IV of the Directive respectively). These provisions will be transposed into French law, in some cases into legislation, in other cases in the form of regulations.

These rules will be common to all payment service users in the European Union. Although it contains a number of provisions regarding which different options are left up to the judgement of national authorities and leave room for contractual adjustments, the Payment Services Directive is one requiring full harmonisation. Moreover, French actors have on several occasions expressed their concern that national transposition across countries should converge towards common interpretations. This will therefore be the subject of particular vigilance during the transposition process.

A common set of rules for all payment services but with some distinctions depending on the mode of initiation of the transactions or instruments used

There will no longer be specific provisions for different means of payment after the Directive is transposed into French law. In fact, unlike in French law, the Payment Services Directive is not based on the concept of means of payment. It sets out rules for a whole range of "payment services", this concept corresponding more or less to the "provision or management of means of payment" in current French law. Transactions involving payment cards will therefore be subject to the set of rules common to payment services. In line with the European law-makers' objective, this approach will provide technological neutrality regarding the rules applied to payments irrespective of the techniques used and the changes in them over time, while taking account of the specific features of the services concerned.

Regarding the application of certain provisions, such as those relating to the revocation of payment orders, payments dispute and the execution of transactions, the Directive differentiates between payment services according to their mode of initiation. It notably refers to card payments using the formulation "payment transactions initiated through the payee", one that may be adapted during transposition for greater clarity. The other types of transaction are also

referred to generically by the following designations: “transactions initiated by the payer” in the case of credit transfers; and "transactions initiated by the payee" in the case of direct debits.

To clarify certain provisions, the Directive also draws, in a small number of its articles, on the concept of payment instruments, or more specifically, the concept of a payment instrument fitted with a “personalised security feature”, i.e. one that authenticates the payer. These articles are mainly aimed at transactions made by payment card, mobile phone if the payment application make use of such features as well as those carried out via Internet banking.

Lastly, the Directive provides for a derogation for “low-value payment instruments". In 2005, the Observatory expressed its concerns regarding this regime considering that the amount then envisaged by the European Commission could have led to apply this regime to a large part of card payment transactions. In line with its initial proposals, the Directive grants a lighter regulatory regime for these instruments, particularly regarding information requirements and disputes. Nevertheless, the provision finally adopted is only applicable to instruments whose maximal transaction amount cannot, as contractually defined, exceed 30 euros.

4|3 Harmonisation of information requirements

Organised around the drawing-up of the same framework contract for all payment services, including those provided via a payment card, the information that the payment services providers must supply to consumers are set out in the Directive. The possibility is also given for merchants to adjust their fees depending on the means of payment used by the consumer.

Cardholder and acceptor contracts

The Directive harmonises the information requirements incumbent on service providers regarding both single payment transactions and transactions covered by a “framework contract”. Payment card transactions come within the latter category. A payment card is indeed issued on the basis of a contract between the issuer and the cardholder that governs the terms and conditions covering both the card’s issuance and use. The acquisition of transactions is also governed by a contract between the acquirer and the acceptor. The Directive specifies the information that must appear in framework contracts. This comprises information on: the payment services provider (name and address), the use of the payment service (form of and procedure for giving consent, execution time, possibility of agreeing on spending limits for the use of the payment instrument), charges (including interest and exchange rates), communication (frequency), safeguards and corrective measures (steps to be taken to keep a payment instrument safe, possibility of blocking the instrument, liability of the payment service provider and of the payer, conditions covering refunds, etc.), changes in and termination of framework contracts (duration of the contract, the right to terminate it) and redress.

The Directive also regulates conditions regarding changes in and termination of these framework contracts, which is a new development in terms of payment card contracts. Regarding changes in contractual conditions, these provisions are however largely in line with what already exists in account agreements. Accordingly, the Directive stipulates that any change must be proposed by the payment service provider no later than two months before its proposed date of application. Unless the payment service user explicitly refuses it before the proposed date of entry into force, this change is deemed to have been accepted. If the user does not accept the change, he has the right to terminate his contract immediately and without charge before the date of the proposed application of the change.

As regards termination, however, the Directive defines the scope of practices more and sets out regime that is a little more favourable to payment service users than that currently in force in France. The framework contract may thus be terminated by the customer at any time, unless the parties have agreed on a period of notice, which may not exceed one month. This termination is free of charge if the framework contract has been concluded for a fixed period exceeding 12 months or for an indefinite period. In all other cases, charges for the termination should be appropriate and in line with costs.

Application of charges or deductions for the use of non-cash means of payment

The Directive provides for a system inspired by Anglo-Saxon practices by laying down the principle of freedom for merchants to adjust their charges, either upwards or downwards, depending on the means of payment used. This means that, for the use of a given means of payment, the customer may be offered a reduction or have extra specific charge added to the price of the goods or services purchased. The practice of offering a reduction for the use of particular payment instrument is already widespread in France, especially for three-party cards chosen by merchants. On the contrary, the application of charges, which is not currently prohibited by French law but which is very uncommon, would be new. The question then arises of the use that should be made of the option given to Member States by the Directive to restrict or prohibit the application of specific charges for the use of a payment instrument. Its transposition into French law will need to take account of the risks that this option given to merchants might generate regarding changes in the use of the different means of payment.

4|4 New rules concerning revocation and contestation

Although the Payment Services Directive lays down the general principle of the irrevocability of payment orders, it provides increased possibilities for contesting a payment transaction. Already common in a number of countries, these possibilities are new in France. They must therefore be accompanied by actions to inform stakeholders in order to avoid potential misapplication.

A maintained irrevocability

In 2005, the Observatory highlighted that vigilance was required regarding the definition of irrevocability set out in the Directive. Indeed, the principle of irrevocability is currently a fundamental principle of card payments and is enshrined in French law (see Article L.132.2 of the French Monetary and Financial Code: “the order or commitment to pay given by means of a payment card is irrevocable”). The payment is thus regarded as definitive and irrevocable as soon as the cardholder has typed in his confidential code. The mechanism set out in the Directive is in principle close to current French law since it stipulates that for “payments initiated through the payee”, as is the case for card payments, it should no longer be possible for the payment order to be revoked once the payer has given his consent to the payee for the execution of the payment transaction. Although the principles laid down by the Directive are similar to those in current French law, the contractual derogations provided for will make it possible to diverge from it, which would lead to disparate situations for consumers. However, these contractual derogations are only possible if the cardholder, his payment services provider and the payee all agree to them.

Greater scope for contesting payments

Transposition of the Directive will noticeably increase the scope for contesting payments currently offered by French law. The Directive sets out two mechanisms depending on whether the payer did not agree to the payment or is only contesting the amount.

The first mechanism concerns unauthorised transactions, i.e. in practice, cases of loss, theft or misappropriation (including by remote fraudulent use or counterfeit) of the payment instrument. In principle, the payer has a period 13 months after the debit date to contest having authorised a payment transaction. His payment services provider then restores the debited account to the state in which it would have been had the unauthorised payment transaction not taken place. Further financial compensation may also be paid. This 13-month period gives the cardholder much greater protection than the rule currently applied under French law whereby the payer has 70 days from the date of the contested transaction, which may be contractually extended to 120 days. Notwithstanding the extension of the contesting period to 13 months, and following the current French law, the cardholder will have to inform its payment service provider without delay in case of loss, theft or misappropriation.

However, a derogation from these refund rules is stipulated by the Directive for payment instruments fitted with a personalised security feature, thus particularly for payment cards. In this case, the payer may be liable for losses, up to an amount of EUR 150, resulting from any unauthorised payment transaction following the use of a lost or stolen payment instrument or, "if the payer has failed to keep the personalised security features safe, from the misappropriation of a payment instrument". This applies except in the case of fraudulent activities or serious negligence on the part of the cardholder prior to the card being reported missing. This latter formulation used in the Directive is ambiguous and could lead to a departure from current French law, which only stipulates the cardholder's liability up to a maximum of EUR 150 in cases of theft or loss. Particular attention should therefore be given to this point during the transposition process in order to ensure that the high level of protection currently applied to cardholders in the event of unauthorised payment made fraudulently, remotely, without physical use of the card or in case of counterfeit is maintained.

The second area of contestation opened up for cardholders by the Directive concerns transactions that are authorised by the payer but where the exact amount is not specified when the transaction is authorised. This mechanism applies particularly to card payments when booking hotel and car hire, for example. Thus, if the payer has given his consent to a payment transaction, he can, within a period of 8 weeks from the date on which the funds were debited, request that this transaction be refunded where the amount of the payment transaction exceeds the amount the payer could reasonably have expected taking into account his previous spending pattern, the conditions in his framework contract and relevant circumstances of the case. Within ten business days of receiving a request for a refund, the payment service provider must either refund the full amount of the payment transaction or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter if he does not accept the justification provided. This is a new development for French law and will cover situations in respect of which a number of litigations are currently underway.

4|5 Conclusion

Transposition of the Payment Services Directive will significantly reshape the regulatory regime governing payments in France. First of all, it opens up the payments market to new players – payment institutions – alongside banks. It also sets forth a much denser legal framework based

more on legislative and regulatory provisions than on contractual rules. Adopting an all-encompassing approach, European law-makers sought not to differentiate between payment services and included payment cards in an overall set of rules that are intended to be technologically neutral, while taking account of the specific features of card payments. The Directive sets out the list of information that all payment service users should be provided with and gives a framework allowing merchants to adjust their charges depending on the payment instrument used by the customer. Finally, while confirming the principle of payment irrevocability, it creates greater scope for contesting transactions.

By 1 November 2012, the European Commission must draw up a report on the Directive's implementation that will enable it to assess the impact it has had at the European level on the way payment services are used and the competitiveness of the payments market.

ANNEX A | MISSIONS AND ORGANISATIONAL STRUCTURE OF THE OBSERVATORY

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

Scope

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

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

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

– a limited number of issuing and acquiring credit institutions (generally referred to as "three-party" cards),
– a large number of issuing and acquiring credit institutions (generally referred to as "four-party" cards).

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

– *Debit cards* are cards that draw on a deposit account and enable their holders to make withdrawals or payments that are debited in accordance with a timeframe set out in the card issuance contract. The debit may be immediate (for withdrawals or payments) or differed (for payments).
– *Credit cards* are backed by a credit line that carries an interest rate and with a maximum limit negotiated with the customer. These serve to make payments and/or cash withdrawals. They enable holders to pay the issuer at the end of a determined period (over 40 days in France). The acceptor is paid directly by the issuer without delay.
– *National cards* serve to make payments or withdrawals exclusively with acceptors established in France.
– *International cards* serve to make payments and withdrawals at all national or international acquiring points managed by national acquirers or by foreign partner acquirers.

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

Responsibilities

Pursuant to the aforementioned Article L. 141-4 of the Monetary and Financial Code and the Decree of 2 May 2002, the Observatory has a threefold responsibility:

– It monitors the implementation of measures adopted by issuers and merchants to strengthen payment card security. It keeps abreast of the principles adopted with regard to security as well as the main developments in this area.
– It compiles statistics on fraud on the basis of the relevant information disclosed by payment card issuers to the Observatory's secretariat. The Observatory issues recommendations aimed at harmonising procedures for establishing fraud statistics for the various types of payment cards.
– It maintains a technology watch in the payment card field, with the aim of proposing ways of combating technological attacks on the security of payment cards. To this end, it collects all the available information that is liable to reinforce payment card security and puts it at the disposal of its members. It organises the exchange of information between its members while respecting confidentiality where necessary.

In addition, the Minister of the Economy and Finance may request the Observatory's opinion on various issues, setting a time limit for its response. These opinions may be published by the Minister.

Composition

The composition of the Observatory is set out in the aforementioned Decree of 2 May 2002. The Observatory is made up of:

– A Deputy and a Senator,
– Eight general government representatives,
– The Governor of the Banque de France or his/her representative,
– The General Secretary of the Banking Commission and his/her representative,
– Ten representatives of payment card issuers, particularly four-party cards, three-party cards and electronic purses,
– Five representatives of the Consumer Board of the National Consumers' Council,
– Five representatives of merchants, notably from the retail sector, the supermarket sector, mail-order sales and e-commerce,
– Three qualified prominent persons chosen for their expertise.

The names of the members of the Observatory are listed in an annex to this report.

The members of the Observatory, other than those representing the State, the Governor of the Banque de France and the General Secretary of the Banking Commission, are appointed for a three-year term. Their term can be renewed twice. The President is appointed among these members by the Minister of the Economy and Finance. He has a three-year term of office, renewable twice. Christian Noyer, the Governor of the Banque de France, has been the President of the Observatory since 17 November 2003.

Operating procedures

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

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

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

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

ANNEX B | MEMBERS OF THE OBSERVATORY

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

List of members until 27 June 2007.

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

General Secretariat of Banking Commission

Representatives of public administrations

Nominated on proposition by the General Secretary for National Defence:

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

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

– The Senior Official for Defence
Emmanuel SARTORIUS

– The Head of the Treasury and Economic Policy or his/her representative
Maya ATIG

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
Jean-Yves SAUSSOL

Nominated on proposition by the Minister of Justice:

– The Director for Criminal Affairs and Pardons
or his/her representative:
Pauline FLAUSS
Maxence DELORME

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 of Business or his/her representative:
Mireille CAMPANA

Representatives of payment card issuers

Brigitte CHARLIER
Head of Electronic Payments - CEDICAM

Patrice COUFFIGNAL
Director - Europay France

Armand de MILLEVILLE
Executive Vice-President - American Express France

Jean-Marie DRAGON
Electronic Payments Expert - La Banque Postale

Bernard DUTREUIL
Director - Fédération Bancaire Française

Hervé DUCHARNE
Audit Manager and Research - Groupement Carte Bleue

Alain GOLDBERG
Risks and Compliance Director - Natixis Paiements

Gérard JOUVE
Institutional Relations Director - CETELEM

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

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)

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

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

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

Representatives of merchants' professional organisations

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

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

Jean-Marc MOSCONI
General Delegate - MERCATEL

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

Guillaume VANOVERSCHELDE
Chief Administrative Officer and Chief Financial Officer -DECATHLON

Persons chosen for their expertise

Philippe CAMBRIEL
Executive Vice-President - Gemalto

Jacques STERN
Professor - École normale supérieure (ENS)

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

List of members since 27 June 2007

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

Corinne DAUCHY

General Secretariat of Banking Commission

Representatives of public administrations

Nominated on proposition by the General Secretary for National Defence:

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

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

– The Senior Official for Defence
Emmanuel SARTORIUS

– The Head of the Treasury and Economic Policy or his/her representative
Maya ATIG
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
Jean-Yves SAUSSOL

Nominated on proposition by the Minister of Justice:

– The Director for Criminal Affairs and Pardons
or his/her representative
Pauline FLAUSS
Maxence DELORME

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 of Business or his/her representative
Mireille CAMPANA

Representatives of payment card issuers

Brigitte CHARLIER
Head of Electronic Payments - CEDICAM

Patrice COUFFIGNAL
Director - Europay France

Armand de MILLEVILLE
Executive Vice-President - American Express France

Jean-Marie DRAGON
Electronic Payments Expert - La Banque Postale

Bernard DUTREUIL
Director - Fédération Bancaire Française

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
Institutional Relations Director - CETELEM

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)

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

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

Frédérique PFRUNDER
Special Adviser - Confédération du logement et du cadre de vie (CLCV)

Representatives of merchants' professional organisations

Philippe JOGUET
Head of the Regulations and Sustainable Development Department - Fédération des entreprises du commerce et de la distribution

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

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

Jean-Marc MOSCONI
General Delegate - MERCATEL

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

Persons chosen for their expertise

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)

ANNEX C | STATISTICS

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

– The 150 members of the “CB” Bank Card Consortium, with international data provided by Europay France and the Carte Bleue Group;

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

– Issuers of the electronic purse Moneo.

The data collected came from three merchants accepting payment cards: France Loisirs, Monoprix, and the French Railways (SNCF). The Observatory also received statistics collected by the distance selling federation Fevad, from a representative sample of its members, as well as data gathered by FCD and Mercatel, two merchants' associations, on supermarkets and specialised trade.

Total number of cards in circulation in 2007: 81.5 million

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

– 25.7 million three-party cards.

Number of cards reported lost or stolen in 2007: around 460,000

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

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	5,606.80	250.66	112.35	8.55	140.41	13.03
Card-not-present payments excl. online payments	na	11.80	7.04	0.90	5.80	1.57
Card-not-present online payments	115.00	9.20	35.99	2.43	10.54	1.25
Withdrawals	1,337.51	93.12	37.06	4.39	29.11	5.01
Total	**7,059.31**	**364.79**	**192.44**	**16.28**	**185.86**	**20.86**
Three-party cards	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**	**Volume (million)**	**Value (EUR bn)**
Face-to-face and UPT payments	208.04	22.91	9.03	1.54	16.52	2.87
Card-not-present payments excl. online payments	0.45	0.05	0.29	0.06	0.10	0,03
Card-not-present online payments	1.29	0.18	0.16	0.03	0.48	0.07
Withdrawals	10.50	1.03	na	na	na	na
Total	**220.28**	**24.17**	**9.48**	**1.63**	**17.11**	**2.96**
Grand Total	**7,279.58**	**388.95**	**201.92**	**17.91**	**202.97**	**23.82**

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	**540.3**	**38,006.0**	**159.4**	**29,127.0**	**343.9**	**59,267.6**[1]
Lost or stolen cards	474.9	34,046.7	80.0	8,336.2	105.8	10,070.6
Intercepted cards	5.4	302.7	1.2	304.4	6.7	489.8
Forged or counterfeit cards	60.1	3,656.5	69.0	18,901.2	82.9	21,783.3
Appropriated numbers	0.0	0.0	2.9	402.3	8.4	749.4
Other	0.0	0.0	6.4	1,182.9	140.2	26,174.5
Card-not-present payments excl. online payments	**295.2**	**23,411.5**	**44.0**	**6,502.9**	**na**	**na**
Lost or stolen cards	50.0	2,549.4	14.8	2,541.2	na	na
Intercepted cards	0.3	18.7	0.1	16.3	na	na
Forged or counterfeit cards	7.5	607.1	12.8	1,994.1	na	na
Appropriated numbers	237.3	20,236.4	0.9	58.6	na	na
Other	0.0	0.0	16.4	1,892.8	na	na
Card-not-present online payments	**188.2**	**26,184.2**	**233.9**	**27,249.1**	**na**	**na**
Lost or stolen cards	11.2	1,010.9	69.1	8,148.6	na	na
Intercepted cards	0.1	14.6	0.2	18.1	na	na
Forged or counterfeit cards	4.2	609.3	66.1	8,398.3	na	na
Appropriated numbers	172.7	24,549.4	1.2	115.1	na	na
Other	0.0	0.0	97.3	10,569.1	na	na
Withdrawals	**81.9**	**17,989.1**	**121.3**	**19,977.5**	**19.3**	**5,848.0**
Lost or stolen cards	79.6	17,601.4	12.0	1,969.2	3.4	713.2
Intercepted cards	0.5	107.1	0.1	26.7	0.1	19.4
Forged or counterfeit cards	1.8	280.7	108.9	17,933.9	15.4	4,994.5
Appropriated numbers	0.0	0.0	0.1	23.7	0.1	49.6
Other	0.0	0.0	0.2	24.0	0.3	71.3
Total	**1,105.6**	**105,590.8**	**558.5**	**82,856.5**	**363.3**	**65,115.5**

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	**15.39**	**7,408.73**	**3.37**	**1,079.43**	**3.27**	**1,673.00**
Lost or stolen cards	6.60	1,655.52	0.75	232.93	1.14	620.37
Intercepted cards	3.08	652.37	0.32	139.10	0.01	7.58
Forged or counterfeit cards	0.79	412.71	2.17	674.00	1.86	929.22
Appropriated numbers	0.33	281.65	0.06	15.24	0.15	59.02
Other	4.60	4,406.48	0.07	18.17	0.12	56.81
Card-not-present payments excl. online payments	**0.86**	**358.55**	**3.10**	**1,146.33**	**2.74**	**1,484.06**
Lost or stolen cards	0.15	22.41	0.06	36.92	0.13	34.45
Intercepted cards	0.06	13.85	0.06	19.49	0.00	0.48
Forged or counterfeit cards	0.05	1.80	0.11	32.31	0.29	194.61
Appropriated numbers	0.52	299.71	2.83	1,048.14	2.27	1,243.92
Other	0.07	20.79	0.03	9.48	0.06	10.61
Card-not-present online payments	**0.30**	**186.11**	**0.78**	**194.50**	**1.23**	**421.09**
Lost or stolen cards	0.08	57.58	0.00	1.81	0.04	6.53
Intercepted cards	0.03	19.53	0.00	0.65	0.00	0.14
Forged or counterfeit cards	0.01	0.12	0.01	3.26	0.07	13.52
Appropriated numbers	0.17	105.00	0.76	186.88	1.09	395.00
Other	0.01	3.88	0.01	1.91	0.04	5.89
Withdrawals	**3.60**	**1,004.91**	**0.00**	**1.00**	**0.00**	**2.50**
Lost or stolen cards	3.13	800.82	0.00	1.00	0.00	0.00
Intercepted cards	0.36	160.47	0.00	0.00	0.00	0.00
Forged or counterfeit cards	0.00	0.16	0.00	0.00	0.00	2.50
Appropriated numbers	0.00	18.02	0.00	0.00	0.00	0.00
Other	0.10	25.44	0.00	0.00	0.00	0.00
Total	**20.14**	**8,958.31**	**7.24**	**2,421.26**	**7.24**	**3,580.64**

Source: Observatory for Payment Card Security

Imprimerie Banque de France
Ateliers SIMA
Document achevé de rédiger le 14 octobre 2008

2007 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 activities of the Observatory during the year 2007. 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

2008 Issue

BdF - 29598 - Ateliers SIMA - 180716 - 6-08