

### Current situation

The Observatory used two reports drawn up by the National Consumers' Council<sup>9</sup> and the National Assembly<sup>10</sup> before the adoption of the Everyday Security Act as the starting point for its work.

These reports underline how difficult it is to assess payment card fraud, due to the following:

- Available fraud statistics are not very accurate and cover only a fraction of the payment cards issued in France.

In 2001, with the exception of the Groupement des Cartes Bancaires “CB”, few payment card systems operators published payment card fraud rates. In addition, the few assessments available were published too sporadically to enable the accurate monitoring of the risks generated by the use of payment cards.

Furthermore, in many cases, the figures published only listed cases of fraud that ultimately affected issuers. They notably excluded some instances of fraud perpetrated prior to stop payment orders, fraud resulting from remote transactions at the expense of merchants and a fraction of fraud cases in which cardholders did not receive compensation from their banks.

- It is difficult to compare statistics published by different issuers. As fraud definitions and typologies, which are adapted to the needs of individual issuers, did not match each other, calculation methods were disparate. Issuers, which basically see fraud statistics as components of their risk control frameworks, focused their efforts on the main types of fraud to which they were exposed while tolerating some uncertainty for the frauds that had lesser impacts on their systems.

Lastly, due to reasons of competitiveness and information sensitivity, secrecy rules and the absence of dialogue were prevalent in the field of statistics, which did not foster the harmonisation of calculation methods.

Consequently, there are still not enough reliable fraud indicators for all payment cards in France, particularly as compared to procedures in other European countries. APACS<sup>11</sup>, for instance, which brings together most UK financial institutions, produces exhaustive fraud figures and analyses on an annual basis.

---

<sup>9</sup> *Rapport sur la sécurité des cartes de paiement* (Report on payment card security), February 2001, National Consumer Council.

<sup>10</sup> *Rapport d'information sur la sécurité des cartes bancaires* (Information report on the security of bank cards), July 2001, presented by Mr Jean-Pierre Brard, Deputy.

<sup>11</sup> Association for payment clearing services

## Methodological work carried out by the Observatory

Given the situation described above, defining a harmonised method for calculating fraud statistics was one of the Observatory's priorities. Its objective was to make up for the various inadequacies highlighted above.

To this end, the Observatory's priority was to draw up a definition of fraud in order to clearly demarcate its scope. The definition adopted covers the use of cards or the data captured on them as well as the activities contributing to the perpetration of fraud.

While certain activities that help to organise, or benefit from, fraud are individually and severally considered criminal offences<sup>12</sup>, there is no legal definition of fraud under French law. Irrespective of the criminal offences that exist under national law, the Observatory has chosen to adopt a "functional" definition (see Box 2) that links the fraudulent nature of an act to its "illicit" nature and to the harm possibly caused to the various actors involved in a card transaction. It has decided to exclude all use or attempts to use payment cards by the lawful cardholder that are considered fraudulent solely due to lack of funds.

---

<sup>12</sup> Under French law: deceit, breach of trust, counterfeiting, forgery of means of payment, theft, violation of an automated data system, intentional use or attempt to use counterfeit or forged payment cards, etc.

## Box 2: Definition of payment card fraud

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

All acts that contribute to the preparation, carrying out and illegitimate use and/or illegitimate use of payment cards or data stored on them:

1. that causes harm to the account holding bank, be it the bank of the cardholder or of the acceptor, the cardholder, acceptor (for instance, merchant or general government agency, on its own account or within a payment system<sup>13</sup>), issuer, insurer, trusted third parties or any parties involved in the chain of design, manufacture, transport, distribution of physical or logical data that could incur civil, commercial or criminal liability,
2. irrespective of:
  - the methods used to obtain, without lawful cause, reason or intent, cards or data stored on them (theft, taking possession of cards, physical or logical data, personalisation data and/or misappropriation of secret codes, and/or cryptograms, magnetic stripe and chip hacking),
  - the procedures for using cards or the data stored on them (payments or withdrawals, face-to-face or remote, via physical use of the card or the card number, via automated payment machines, etc.),
  - the geographical area of issuance or use of the card and the data captured on it:
    - French issuer and card used in France,
    - Foreign issuer and card used in France,
    - French issuer and card used abroad.
  - the type of payment card, as defined by Article L. 132-1 of the Monetary and Financial Code, including electronic purses,
3. whether or not the fraudster is a third party, the account holding bank, the cardholder him/herself (for example, using the card after it has been declared lost or stolen, wrongful termination of transactions), the acceptor, issuer, an insurer, a trusted third party, etc.

The Observatory has in addition defined a fraud typology in line with the various approaches outlined in the definition of fraud and closely based on the classification criteria used by the various issuers. This typology makes distinctions between:

- The origin of the fraud:
  - *Lost or stolen cards*: the fraudster uses a payment card obtained without the knowledge of the lawful cardholder, following card theft or loss.
  - *Non-received cards*: cards intercepted when sent by issuers to lawful cardholders. While this type of origin is similar to theft or loss, it is nonetheless different because it is not easy for a cardholder to ascertain that a fraudster is in possession of a card that belongs to him/her; it also entails risks specific to procedures for sending cards.
  - *Forged or counterfeit cards*: an authentic payment card may be falsified by modifying magnetic stripe data, embossing or programming. Creating a

---

<sup>13</sup> In the case of the Internet, the acceptor may be different from the service provider, or a trusted third party (payments, donations made by Internet users wishing to support a web site, an ideology, etc.).

counterfeit card means creating an object that appears to be an authentic payment card and/or is capable of deceiving a payment machine or a person. For payments made via automated terminals, counterfeit cards incorporate the data required to deceive the system. In face-to-face transactions, counterfeit cards present certain security features found on authentic cards (including visual appearance), incorporate data stored on authentic cards, and are intended to deceive acceptors.

- *Misappropriated card numbers*: a cardholder's card number is taken without his knowledge or created through "card number generation" (see "fraud techniques") and used in remote transactions.
- *Unallocated card numbers*: use of a PAN<sup>14</sup> that is consistent but not attributed to a cardholder, generally used in remote transactions.
- *Splitting payments*: splitting up payments so as not to exceed the authorisation limit defined by the issuer.

– Fraud techniques:

- *Skimming*: technique that consists in copying the magnetic stripe of a payment card using an illegal card reader known as a "skimmer" embedded in merchants' payment terminals or automated machines. The confidential PIN may also be captured visually, using a camera or by tampering with the keypad of a payment terminal. Captured data are then re-encoded onto the magnetic stripe of a counterfeit card.
- *Opening of a fraudulent account*: opening of a reference account using false personal data<sup>15</sup>.
- *Usurpation of identity*: fraudulent acts linked to payment cards and involving the use of another person's identity.
- *Wrongful repudiation*: a cardholder, acting in bad faith, disputes a valid payment order that he/she initiated.
- *Hacking automated machines*: techniques that consist in placing duplicating devices in automated machines.
- *Hacking automated data systems, servers or networks*: fraudulent intrusion into these systems.
- *Card number generation*: using issuers' own rules to create payment card numbers that are then used in fraudulent transactions.

– Types of payment:

- *Face-to-face payment*, carried out at the point of sale, via an automated machine, by splitting payments, by modifying the transaction amounts, or for electronic purses, by double debit.
- *Remote payment* over the Internet, by mail, by fax/telephone, or any other means.
- *Withdrawal* (withdrawal from an ATM or any other types of withdrawal).

– Losses are shared between:

- the merchant's bank, the acquirer of the transaction,
- the cardholder's bank, the issuer of the card,
- the merchant,
- the cardholder,

---

<sup>14</sup> Personal Account Number.

<sup>15</sup> See footnote on page 2.

- insurance companies,
  - and any other operators involved.
- The geographical area of issue or use of the card or the data encoded on them:
- The issuer and acquirer are both established in France. In this case, the transaction is qualified as national or domestic.
  - The issuer is established in France and the acquirer abroad.
  - The issuer is established abroad and the acquirer in France.

The Observatory conducted a first data collecting initiative in early 2004 on the basis of this typology. Data collected from the various respondents were for the year 2002, and were therefore stabilised.

It was decided not to focus this first exercise on fraud techniques and loss sharing, given the difficulties that certain issuers could face in obtaining data in this area. The difficulties faced in this first data collection and consolidation exercise will be analysed with a view to improving the quality of the statistics produced.

The statistics were gathered from payment card issuers and merchants represented within the Observatory. Other issuers and merchants contributed to this survey in order to ensure a good representative sample of the French payment card market (see Box 3).

### Box 3: Fraud statistics – respondents

In order to ensure the quality and representativeness of fraud statistics<sup>16</sup>, the Observatory has set out to produce a diversified sample, comprising as many respondents as possible, and encompassing the most representative operators on the market. The sample covers almost all “four party” card transactions. It covers roughly 25 million “three party” cards (i.e. almost 70% of the cards in this category in circulation), which were used to generate EUR 13 billion of domestic transactions in 2002. This sample is large enough to ensure the representativeness of the statistics obtained. The French “three party” card market in fact comprises a dozen or so issuers: responding institutions represent the majority of these issuers and also rank among the most important. Moreover, the merchants that contributed to the establishment of statistics accept cards amounting to a total of almost EUR 14 billion.

#### A – Payment card issuers

Data was gathered from:

- seven issuers of “three party” cards (American Express, Banque Accord, Cetelem, Cofinoga, Diners Club France, Finaref and S2P for the Pass card),
- all members of the Groupement des Cartes Bancaires “CB”, i.e. 160 issuers. The data was obtained through the Groupement des Cartes Bancaires “CB”, Europay France and the Groupement Carte bleue,
- issuers of the electronic purse Moneo, gathered through BMS (Billettique Monétique Services).

#### B – Merchants

Data was gathered for 11 payment card acceptors: C&A, Casino, Cora, Eram, France Loisirs, Leclerc, Monoprix, Selectour, SNCF, Super U and 3 Suisses.

## Fraud assessment for 2002

Most respondents were able to provide almost all of the data that was requested of them: the widespread automation of card payments facilitated the establishment of statistics. It must nonetheless be pointed out that there were differences in the aggregates monitored by the various respondents. For example:

- issuers of “three party” cards remain constantly on the lookout for accounts opened under false identities, particularly for credit cards, while issuers of interbank cards closely monitor other sources of fraud.
- merchants are not always aware of the origins of the fraud incidents they experience and therefore do not generally define statistical indicators in this field.

---

<sup>16</sup> See definition of fraud in Box 2.

## Evaluation of the French payment card market

Based on the data available in 2002, the following estimates may be provided for the French payment card market:

- roughly 46 million “four party” cards – including 840,000 electronic purses – generating a total value of EUR 257 billion in national transactions (payments and withdrawals). Cross-border transactions represent a small proportion of all transactions recorded in the French systems (respectively 3.0% for transactions with French issuers and foreign acquirers and 6.2% for transactions with foreign issuers and French acquirers).
- between 30 and 35 million “three party” cards<sup>17</sup> generating a total value of between EUR 20 billion to EUR 25 billion in domestic payments. Most “three party” card payment systems do not allow cross-border transactions, which are therefore much fewer in number in this category than domestic transactions.

## Fraud assessment

### Overall view

The data collected show that the overall fraud rate (i.e. for all fraudulent transactions recorded in the French systems) is estimated at 0.082% in amount. The rate stands at 0.082% for “four party” cards and 0.078% for “three party” cards.

Data provided by issuers make it possible to estimate total payment and withdrawal fraud at EUR 141.4 million in 2002<sup>18</sup>, for cards with French issuers, and at EUR 193.3 million for transactions with French acquirers. The corresponding fraud rates are 0.051% and 0.067% respectively. “Issuer” and “acquirer” fraud rates for “four party” cards are 0.051% and 0.066% respectively. The rates are 0.052% and 0.072% respectively for “three party” cards.

Data for merchants are more incomplete than those obtained from issuers. The typology of data provided by merchants does not always match the data defined by the Observatory. They nevertheless give an indication of the level of fraud experienced by merchants: in 2002 the fraud observed by the merchants surveyed amounted to EUR 3.8 million for all transactions, i.e. a fraud rate of 0.027%.

---

<sup>17</sup> This estimate does not include single-purpose cards benefiting from an exemption to banking monopoly.

<sup>18</sup> This estimate concerns only issuers that contributed to the calculation of statistics. It should be noted in addition that these figures cover only the origins of fraud that issuers were questioned about (card loss or theft, use of non-received cards, use of counterfeit cards and use of appropriated card numbers) and do not include transactions performed following the fraudulent opening of accounts.

## Breakdown of fraud by geographical area and transaction type

Fraud is broken down as follows, according to the geographical area of card issue or transaction acquiring.

### Box 4: Amount and rate of fraud in 2002

	Amount of fraud (EUR millions)	Fraud rate
French issuer / French acquirer	89.5	0.033%
French issuer / Foreign acquirer	51.9	0.558%
Foreign issuer / French acquirer	103.8	0.519%

Source: sample constituted by the Observatory 2002

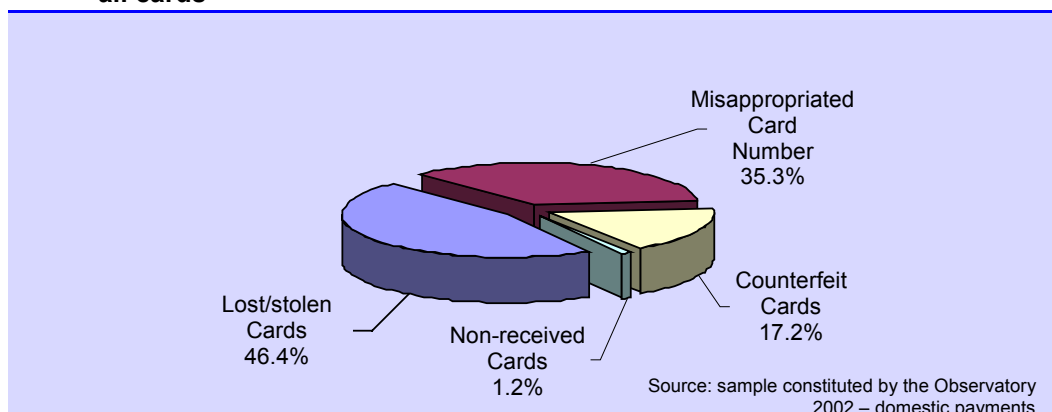
Fraud rates on international transactions are therefore higher by far than those on domestic transactions.

Some 66% of fraudulent national payments are face-to-face payments and the remaining 34% are remote payments.

## Breakdown of fraud by origin<sup>19</sup>

The majority of fraud incidents in domestic payments originates from lost or stolen cards and misappropriated card numbers.

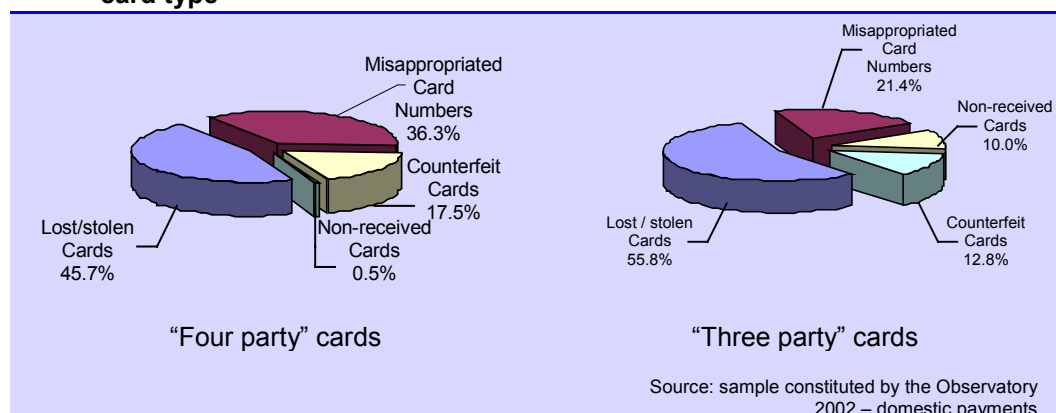
### Box 5: Breakdown of fraud amount by source, all cards



<sup>19</sup> In line with the typology defined by the Observatory.

These origins of fraud are broken down as follows according to card type.

#### Box 6: Breakdown of fraud amounts by origin, card type



The most widespread type of fraud in cross-border transactions is the use of counterfeit cards. In 2002, counterfeit cards were used in fraudulent transactions between French issuers and foreign acquirers amounting to a value of EUR 24 million. The use of lost or stolen cards was the next largest origin of fraud.

Electronic purses are mainly exposed to the use of lost or stolen cards. This type of fraud nonetheless remains very limited.

### Conclusions

These findings make it possible to characterise fraud for the different types of card systems identified:

- issuers of "four party" cards record very high levels of fraud for cross-border transactions and when the chips embedded in cards can not be used,
- issuers of "three party" cards that involve a limited number of acceptors and are restricted, in addition, to certain types of transactions (i.e. mostly domestic and carried out at point of sale) are little exposed to forgeries but are vulnerable vis-à-vis lost and stolen cards,
- issuers of "three party" cards that have a widespread acceptance network (in France and abroad) and may be used in a wider range of transactions, are, like issuers of interbank cards, exposed to fraud in the use of cards for remote payments or international transactions (forgeries are used in these types of transactions).