

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2022





"This publication may not be represented or reproduced, in whole or in part, without the express permission of the Banque de France, except as provided for under Article L. 122-5 2° and 3° a) of the French Intellectual Property Code, or where relevant, within the limits of the terms and conditions laid down in Article L.122-10 of said Code."

© Observatory for the security of payment means – 2023

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2022

addressed to

The Minister of the Economy, Finance and Industrial
and Digital Sovereignty

The President of the Senate

The President of the National Assembly

by François Villeroy de Galhau,

Governor of the Banque de France,

President of the Observatory

for the Security of Payment Means

NOVEMBER 2023

CHAPTERS

| | |
|--|-----------|
| SUMMARY | 6 |
| 2022 IN NUMBERS | 8 |
| CHAPTER 1 FRAUD IN 2022 | 11 |
| 1.1 Overview | 12 |
| 1.2 Current state of payment card fraud | 14 |
| 1.3 Current state of cheque fraud | 20 |
| 1.4 Current state of credit transfer fraud | 21 |
| 1.5 Current state of direct debit fraud | 22 |
| CHAPTER 2 TERMS AND CONDITIONS FOR THE REIMBURSEMENT OF FRAUDULENT PAYMENT TRANSACTIONS | 27 |
| 2.1 Background to the work | 27 |
| 2.2 Regulations applicable to payment transaction disputes | 29 |
| 2.3 General recommendations for handling payment transaction disputes | 31 |
| 2.4 Recommendations applicable to the treatment of specific cases | 31 |
| 2.5 Recommendations for consumers and their representatives | 34 |
| 2.6 Recommendations to prevent fraud | 36 |
| 2.7 Conditions in the implementation of the recommendations | 38 |

**CHAPTER 3
SMARTPHONE OR TABLET PAYMENT ACCEPTANCE SOLUTIONS** **39**

- 3.1 Introduction**
- 3.2 Overview of current solutions**
- 3.3 Risks**
- 3.4 Security standards**
- 3.5 Technical security of SoftPOS solutions**
- 3.6 The Observatory's recommendations**
- 3.7 Conclusion**

**CHAPTER 4
ACTIONS CONDUCTED BY THE OBSERVATORY IN 2022** **41**

- 4.1 Strong customer authentication of card payments** **41**
- 4.2 Following up of Observatory's actions and recommendations against cheque fraud** **47**
- 4.3 Reminder of the Observatory's primary recommendations on technology monitoring topics** **47**

APPENDICES **51**

- A1 Precautionary advices for the use of means of payment**
- A2 Responsibilities and organisation of the Observatory** **52**
- A3 List of Observatory members by name** **54**
- A4 Methodology for measuring fraud involving cashless means of payment** **57**
- A5 Statistical file on payment card use and fraud** **67**

Chapter 3, Section 4.2 and Appendix 1 are available in French only in the original version of the report, which can be found here: https://www.banque-france.fr/system/files/2023-09/rapport_annuel_de_lobservatoire_de_la_securite_des_moyens_de_paiement_2022.pdf

Appendices 2, 3 and 4 are available in English in this report.

All tables in Appendix 5 can be downloaded in English at the following address: *en attente*

SUMMARY

The general increase in the use of cashless means of payment – a trend observed since the onslaught of the health crisis – has continued throughout 2022 (+8%). Within this trend, certain payment instruments have grown more than others. Contactless payments now account for more than six out of every ten card payments at point of sale. Mobile card payments continue to grow at a sustained rate (up 137% to almost 6% of payments at point of sale), and instant transfers are up 85%.

Chapter 1 of this report, which presents statistical trends on usage and fraud in cashless means of payment, shows a general improvement in security. Overall, despite the growth in flows, fraud fell by 4% in terms of both volume and value, amounting to losses of EUR 1.19 billion. However, trends differ depending on the means of payment:

- **The payment card, which is further consolidating its status as the main payment means for everyday use, has seen its fraud rate fall to 0.053% (from 0.059% in 2021), the lowest level ever recorded by the Observatory.** This historic result is the fruit of the significant improvement in the security of payments over the internet, which have benefited for more than a year now from the strong authentication rules introduced by the second European Payments Services Directive (PSD 2). Compared with 2019, when these rules had not yet been implemented, the fraud rate for card payments over the internet has fallen by a third, to 0.165%. Following the initial trends observed in 2021, these figures confirm the very positive results brought about by the implementation of strong authentication for payments over the internet. The report does, however, highlight the still relatively high fraud rate for mobile payments at point of sale (0.061%), which, although down from 2021, is still six times higher than for all card payments at point of sale. This is mainly due to vulnerabilities in the e-wallet enrolment processes, which do not always involve strong authentication of the cardholder under the control of the issuing institution.
- **The cheque fraud rate has also fallen, to 0.073% (from 0.079% in 2021), although it is still the highest fraud rate among all payment methods.** The fall in cheque fraud, which comes against a backdrop of declining flows (-8%), marks the first positive results of the Observatory's action plan adopted in 2021. The new systems for monitoring the cashing of cheques, deployed by banking institutions a number of years ago, are also contributing to this trend. Given the persistently high levels of fraud, users must remain vigilant and efforts must be sustained by industry players. Further progress is expected towards making the postal delivery of cheque books more secure and towards simplifying the procedures for cancelling lost or stolen cheques.
- **Transfers recorded a new annual increase in value defrauded (+9%),** while the fraud rate for this instrument remained extremely low (0.001%), highlighting the significant value of the total amounts exchanged through it; credit transfers are the main payment instrument used by businesses and public authorities. Nevertheless, the amount of fraud linked to credit transfers has more than tripled in five years, rising from EUR 78 million in 2017 to EUR 313 million in 2022. While large companies and public authorities continue to be affected, individuals and small businesses were the main victims in 2022. In fact, 70% of the value of fraudulent transfers was initiated from online banking interfaces, which are mainly used by individuals and small businesses. On the other hand, the Observatory is pleased to note that the fraud rate for instant transfers has remained stable (0.044%), which is lower than that for cards, and that the use of instant transfers is set to increase over the next few years. To meet these new security challenges, the Observatory will launch work in September 2023 to identify additional measures to combat credit transfer fraud and accelerate their implementation on the French market.

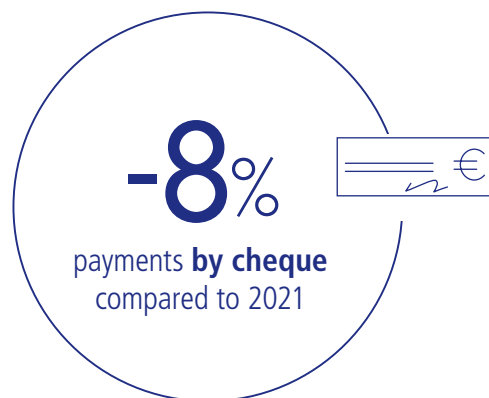
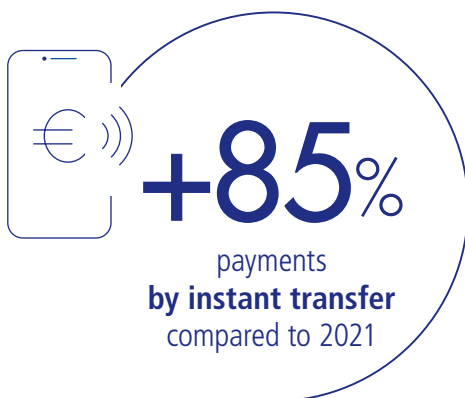
In the remainder of the report, the Observatory makes a number of recommendations in response to changes in payment practices and fraud techniques.

- Against a backdrop of general improvement, 2022 was marked by the development of scam techniques and operating methods based on manipulation, in particular those based on a telephone call impersonating bank staff seeking to deceive a customer.** Using various means to gain control over their victims, fraudsters are able to elicit the strong authentication of fraudulent transactions. Under these circumstances, victims may have encountered difficulties in obtaining reimbursement from their banks. In response to these frauds, which affect all customer profiles, the Observatory issued a set of 13 recommendations in May 2023 aimed at improving reimbursements to victims while stepping up fraud prevention and combating actions by all the players involved (Chapter 2). The Observatory will closely monitor their implementation, with the support of the French Prudential Supervision and Resolution Authority (ACPR – Autorité de contrôle prudentiel et de résolution) as part of its remit to monitor commercial practices. An initial assessment will be drawn up and published at the end of 2024. It is essential that consumers are assured that their complaints will be dealt with rigorously, so as to reinforce the feeling that they too are fully benefiting from the collective progress made in the fight against fraud.
- Drawing on its ongoing technology monitoring work, the Observatory also makes a number of recommendations on the use of devices (such as mobile phones and tablets) as card payment terminals (Chapter 3).** These solutions, which are very much in the minority and still often in the experimental stage, are beginning to appear on the French market. In 2016, the Observatory highlighted the fact that mobile phones remained a weak link in the security of mobile payment solutions. In 2022, increasing the technical security of these new acceptance solutions is now possible, as long as they are duly audited and certified. However, the Observatory calls on merchants to remain particularly cautious, rigorous and selective when deploying these new “consumer” terminals, so as to maintain the same high standards as for terminals dedicated to electronic payments, as these have proven their safety and robustness in payments with mobile phones. Merchants using this type of “mass market” terminal must also provide an alternative for visually impaired people, who cannot always use the touch screens and virtual keyboards of these solutions.
- The Observatory’s work during 2022 on strong authentication for online payments is included in Chapter 4. The report provides detailed data on cardholder equipment and online payments for the first time.** These highlight the clear path towards progress in strengthening the security of payments over the internet, particularly for so-called “MIT” transactions (merchant initiated transactions) and certain transactions exempt from strong authentication not using 3D-Secure-type authentication protocols. The guidelines published in this report should contribute to a more secure and compliant use of the strong authentication exemption protocols based on transaction risk analysis.

Against a backdrop of rapidly evolving payment methods and ever-changing threats, the Observatory remains committed to ensuring the security of all payment methods, guaranteeing for all users, from individuals to businesses, genuine freedom of choice in their day-to-day payments. In its work programme for 2023-2024, the Observatory will focus in particular on intensifying dialogue with the telecommunications sector, which has a key role to play in preventing the risks of identity theft and contributing to the fight against payment fraud.

2022 IN NUMBERS

THE USE OF MEANS OF PAYMENT IN 2022



FRAUD TRENDS IN 2022

EUR **1.192** bn
damages


-4%
fraud in volume
and value


0.053%

in card fraud rate,
a historic low


0.044%

in instant transfer
fraud rate



close to

70%
of large-transfer
fraud affects
online banking
interfaces


-33%

in fraud rate
for card payments
on the internet
since 2019


-15%

value of
cheque fraud
compared to 2021

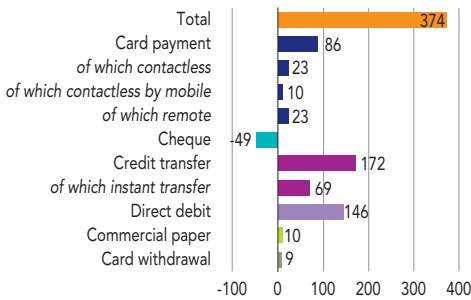
1

FRAUD IN 2022

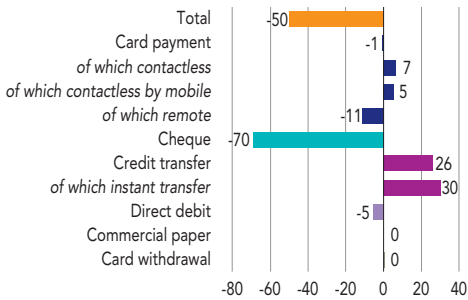
Key data

C1 Changes in means of payment between 2021 and 2022

a) Payment flows (in EUR billions)

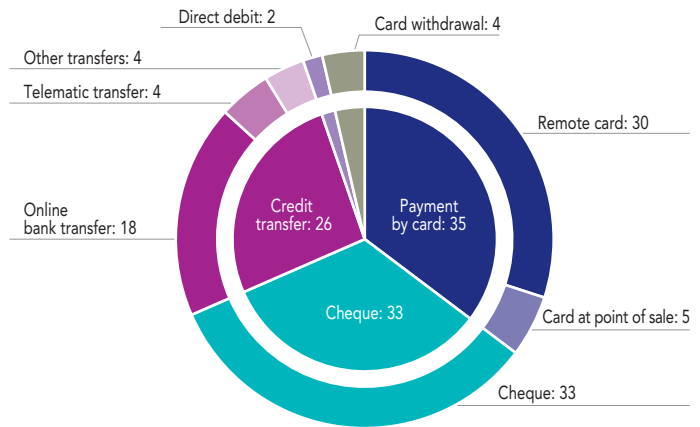


b) Fraud (in EUR millions)



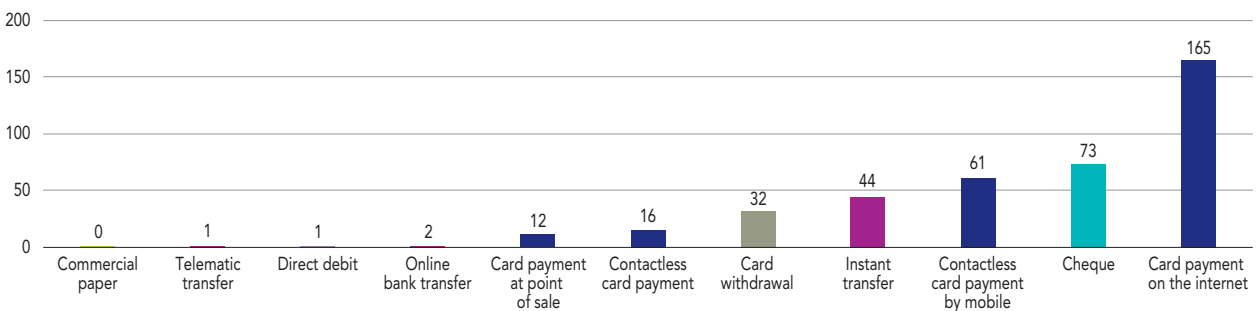
Source: Observatory for the Security of Payment Means.

C2 The main sources of fraud by value (%)



Source: Observatory for the Security of Payment Means.

C3 Vulnerability to fraud of the main payment channels (in EUR defrauded per EUR 100,000 in transactions)



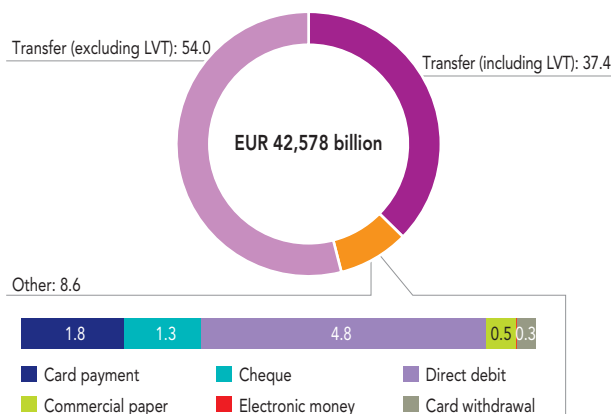
Source: Observatory for the Security of Payment Means.

1.1 Overview

1.1.1 An overview of means of payment

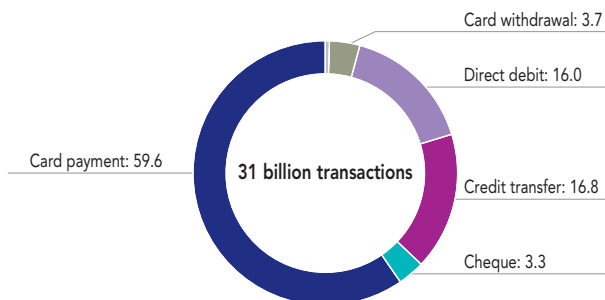
C4 Use of cashless means of payment in 2022 (%)

a) In value



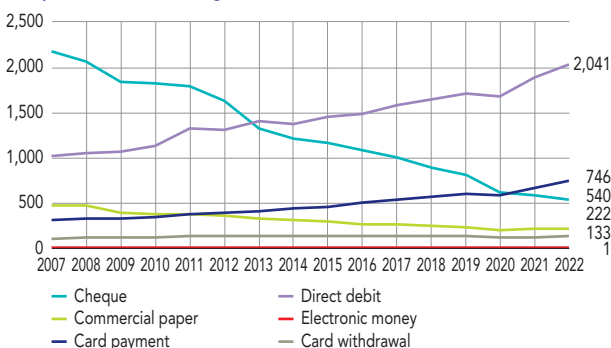
Source: Observatory for the Security of Payment Means.
Note: LVT – large value transfer.

b) In volume



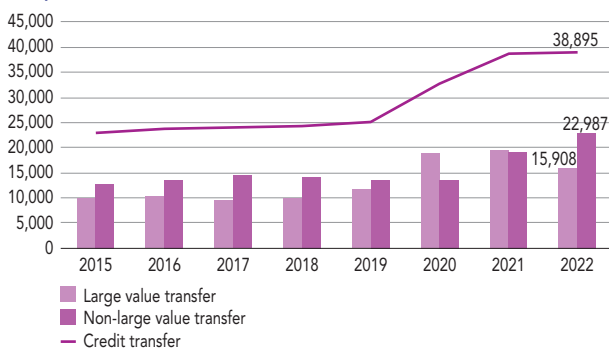
C5 Payment flow value (in EUR billions)

a) By instrument (excluding bank transfers)



Source: Observatory for the Security of Payment Means.

b) By bank transfer



Cashless payment transactions carried out by individuals, businesses and public authorities reached 30.6 billion transactions in 2022 (+8.1% from 2021), for a total of EUR 42.578 trillion (+0.9% from 2021).

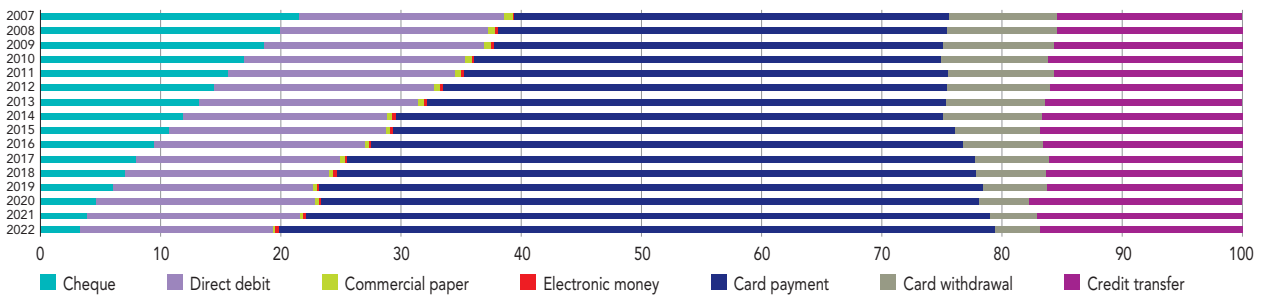
Instant transfers continue to grow rapidly (+85% in volume and +138% in value) and now account for 3.8% of all transfers (compared with 2.2% in 2021).

Bank cards are still the preferred cashless payment method in France. Their share of transactions (in volume), excluding withdrawals, is rising steadily, from 56.9% in 2021 to

59.6% in 2022. A growth in flows in terms of both volume and value can also be seen in contactless payments (accounting for more than 61% of payments at point of sale, compared with 57% in 2021), and particularly in payments with mobile phone (accounting for almost 6% of payments at point of sale, compared with less than 3% in 2021).

Cheques remain the only means of payment down both in volume (-8.8%) and in value (-8.3%), while cash withdrawals with card are increasing steadily (+4.5% in volume and +7.3% in value).

C6 Changes in the use of means of payment in terms of volume (%)

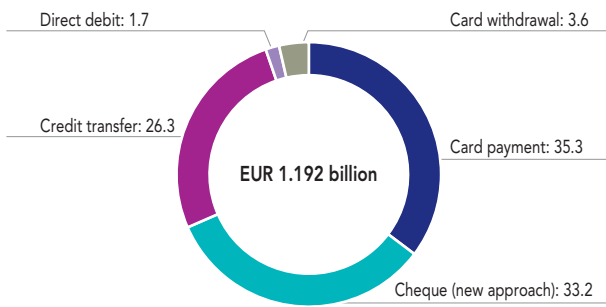


Source: Observatory for the Security of Payment Means.

1.1.2 Overview of payment fraud

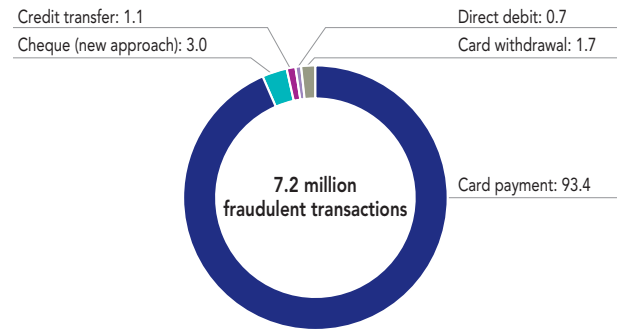
C7 Breakdown of fraud (%)

a) In value

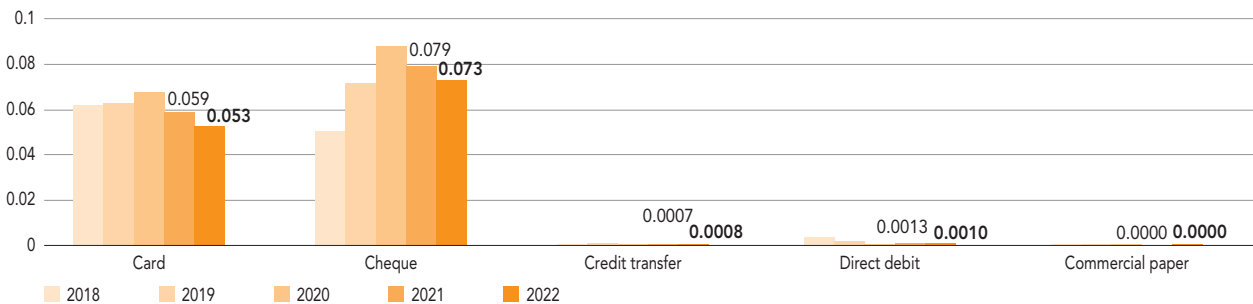


Source: Observatory for the Security of Payment Means.

b) In volume



C8 Changes in fraud rate in value by means of payment (%)



Source: Observatory for the Security of Payment Means.

Note: For 2021 and 2022, cheque fraud rate is calculated using the new approach.

Cashless payment fraud is decreasing even against a backdrop of increasing transactions in terms of both volume and value. There were 7.2 million fraudulent transactions in 2022 (down 3.6% from 2021), representing losses of EUR 1.192 billion (down 4% from 2021).

The general decline in cashless payment fraud is due in particular to the reduction in card fraud (down 0.2% in terms of value), with the fraud rate reaching an all-time low of 0.053%, and to the decline in cheque fraud (down 15% in terms of value), which is faster than the fall in values

exchanged by cheque (down 8%). Direct debit fraud, which by its nature is quite erratic, is down (-21.6% in terms of value) and its share of total fraud in cashless payments remains stable and moderate.

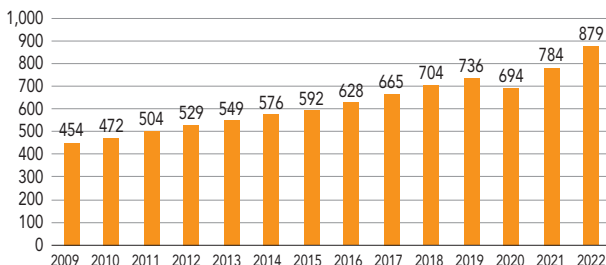
However, although the credit transfer fraud rate remains extremely low as a share of the amounts exchanged (0.0008%), it continues to rise, with total losses of EUR 313.1 million, up 9% from 2021. Credit transfers will account for 26.3% of cashless payment fraud in 2022, up from 23.1% in 2021.

1.2 Current state of payment card fraud

1.2.1 Overview – Cards issued in France

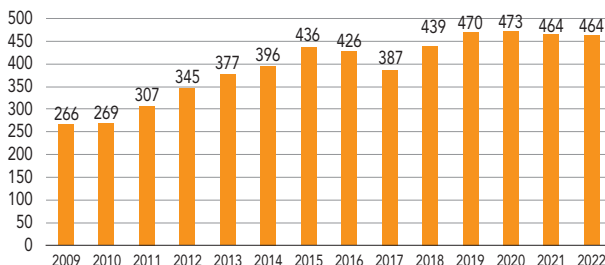
C9 Cards issued in France in 2022

a) Total value of transactions (in EUR billions)



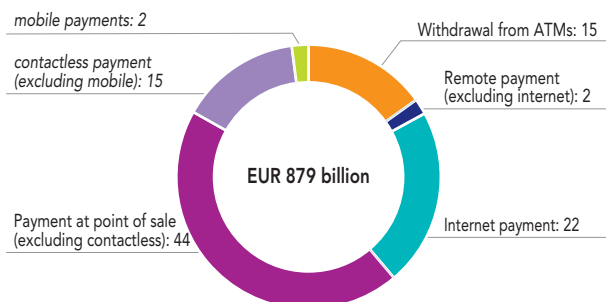
Source: Observatory for the Security of Payment Means.

b) Total value of fraud (in EUR millions)



C10 The use of cards issued in France by payment channel in 2022 (%)

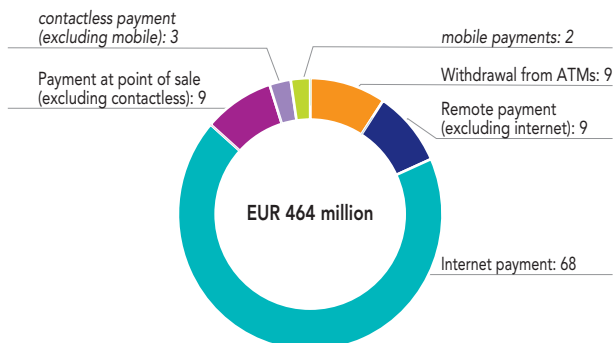
a) Breakdown of transaction value



Source: Observatory for the Security of Payment Means.

Note: ATM – automatic teller machine.

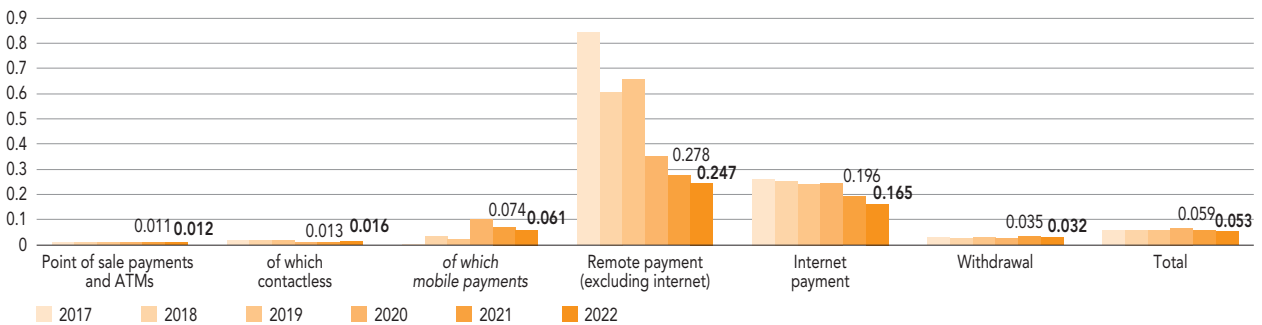
b) Distribution of the value of fraud



The use of cards continues to grow, with payment flows rising in 2022 in terms of both volume and value (by 13% and 12% respectively). The total amount of fraud in payments by card issued in France has stabilised at EUR 464 million even against this backdrop of growth, thanks in particular to the application in 2022 of strong

authentication rules for transactions over the internet. However, payment by card over the internet remains the channel most exposed to fraud: although it only accounts for less than a quarter of cashless payment flows (22%), it represent 68% of cashless payment fraud in terms of value.

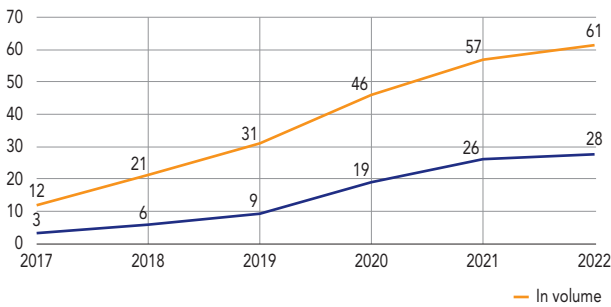
C11 Changes in fraud rates on French cards in value terms, by payment channel (%)



Source: Observatory for the Security of Payment Means.
 Note: ATM – automatic teller machine.

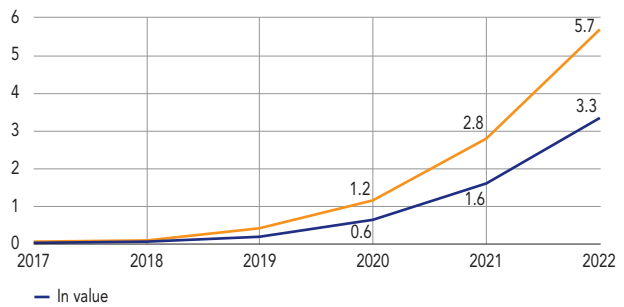
C12 Card payments at point of sale (%)

a) Share of contactless payments



Source: Observatory for the Security of Payment Means.

b) Share of mobile payments



The fraud rate on all transactions by card issued in France has fallen significantly, from 0.059% in 2021 to 0.053% in 2022, a reduction of 10% for the second year running (13% into 2021). This trend can be seen across most payment channels for cards issued in France. Below are the channels where the fraud rate has fallen more substantially.

The fraud rate for payments over the internet continues to fall, from 0.196% in 2021 to 0.165% in 2022 (-16%), a new all-time low. In five years, the fraud rate has fallen by 37%, confirming the very positive effect of the PSD 2 strong authentication rules and the improvement in risk measurement tools used by electronic payment operators.

Although remote payments (excluding internet) still suffer from a high fraud rate, their fraud rate nevertheless fell by 16%. These remote payments, where the payment card

number is communicated by post, telephone or email, represent less than 1% of card payments.

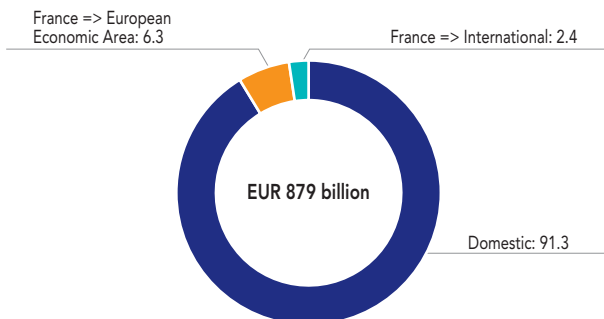
The fraud rate for mobile payments remains six times higher than the rest of card payments at point of sale. Fraudulent use of stolen cards in mobile applications is the main reason for this. However, the fraud rate for this payment channel fell to 0.061% in 2022, even though it is growing rapidly (+137% in volume, or 5.7% of payments at point of sale).

While contactless payment has consolidated its position as the preferred point-of-sale payment method (accounting for 61% of transactions and 28% of value), its fraud rate has risen slightly to 0.016%, while still remaining low. This slight increase is mainly due to an upsurge in the theft of cards that are used for a few transactions under the EUR 50 limit.

1.2.2 Breakdown of fraud by geographical area – Cards issued in France

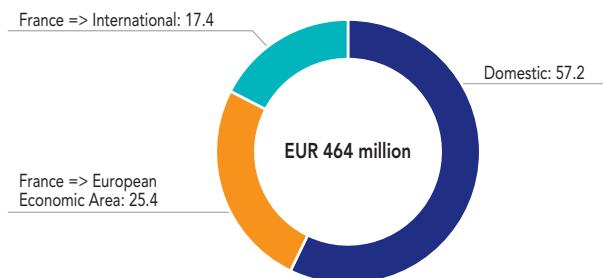
C13 Cards issued in France by geographical area (%)

a) Breakdown of transaction value

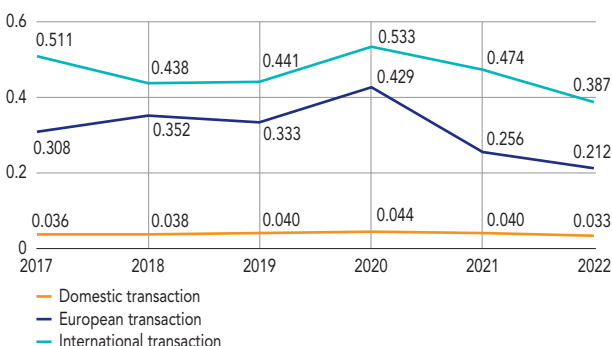


Source: Observatory for the Security of Payment Means.

b) Distribution of the value of fraud

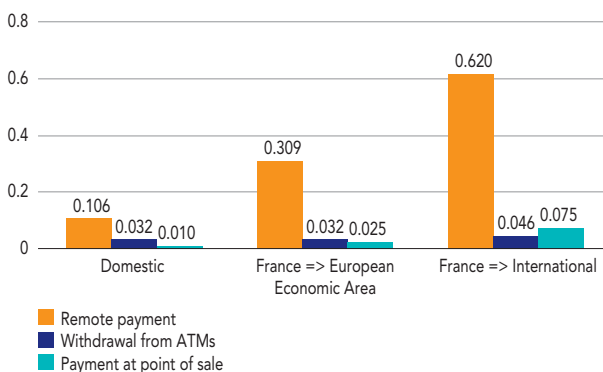


C14 Changes in fraud rates on cards issued in France by geographical area (%)



Source: Observatory for the Security of Payment Means.

C15 Fraud rate by geographical area and by channel (%)



Source: Observatory for the Security of Payment Means.

Note: ATM – automatic teller machine.

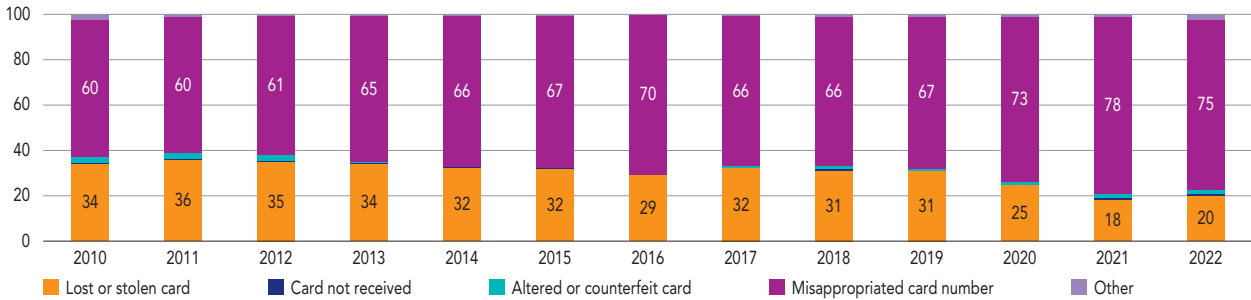
The proportion of international transactions (including transactions to the European Economic Area) carried out using cards issued in France remains low, representing only 9% of transactions in 2022, yet, with EUR 198 million in losses incurred, they will account for almost 43% of cashless payment fraud (compared with 38% in 2021).

However, while international card transactions are structurally more prone to fraud, as they mainly involve remote payments, their fraud rate continues to improve. The fraud rate for European transactions (i.e., cards issued in France and payments processed in Europe) fell by 17%, and for international transactions by 18%.

For all geographical areas, the channel with the highest fraud rates is remote payments, the biggest share of which corresponds to internet payments. Although the rate of internet payment fraud within the European Economic Area has fallen by 15%, thanks to the effects of strong authentication rules, it is still three times higher than the figure for domestic internet payments (0.300% compared with 0.099%). International payments at point of sale are more exposed to fraud, due to the use of less robust technologies. They are therefore more vulnerable to counterfeiting, for example by reading the magnetic stripe or taking a physical imprint of the card.

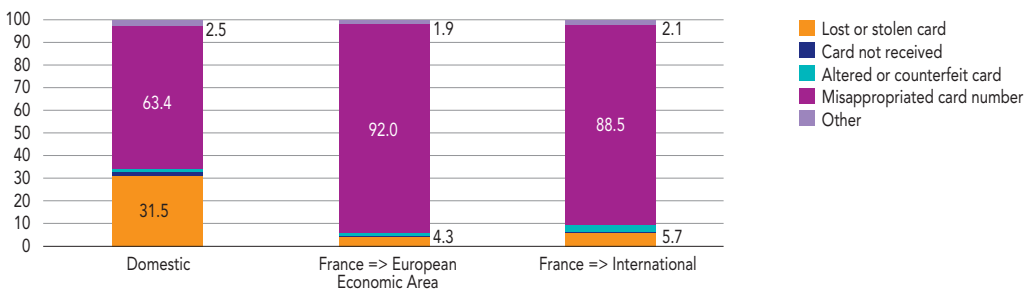
1.2.3 Breakdown of fraud by *modus operandi* – Cards issued in France

C16 Changes in fraud type since 2010 in value terms (%)



Source: Observatory for the Security of Payment Means.

C17 Types of fraud by geographical area according to value in 2022 (%)



Source: Observatory for the Security of Payment Means.

Fraud based on the misappropriation of card numbers continues to dominate, although it is declining slightly: from 78% in 2021 to 75% in 2022. The fraud techniques used to obtain card numbers continue to be phishing by email or SMS.

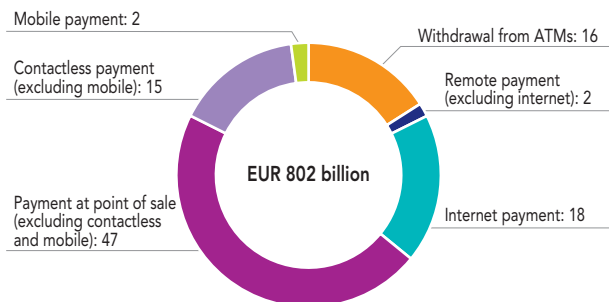
Conversely, the proportion of fraud linked to the loss or theft of a card is increasing slightly, for the first time since 2017,

although it remains at a low level (20%). Logically, the use of lost or stolen cards is most prevalent in France (31.5% of cases). Fraud involving the misappropriation of a card number takes place primarily over the internet, regardless of geographical location. Altered or counterfeit cards are mainly used in countries outside the European Union (EU), where smart card distribution is not yet widespread (in the EU it only accounts for 4% of fraud).

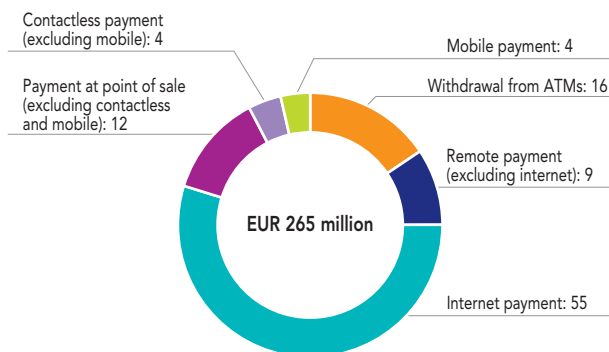
1.2.4 Breakdown of fraud on domestic transactions

C18 Domestic card transactions by value (%)

a) Breakdown of transactions

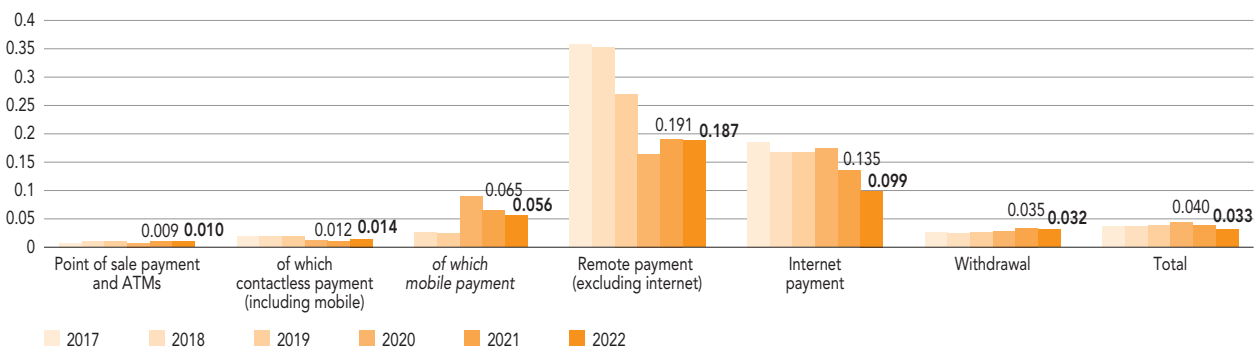


b) Breakdown of fraud



Source: Observatory for the Security of Payment Means.
Note: ATM – automatic teller machine.

C19 Changes in fraud rate on domestic card transactions (%)



Source: Observatory for the Security of Payment Means.
Note: ATM – automatic teller machine.

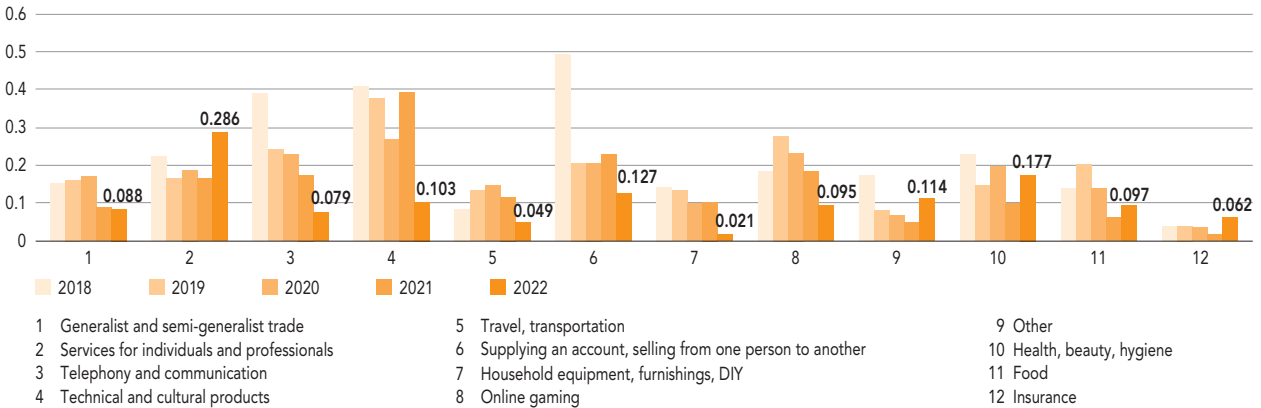
Remote payments account for a stable one-fifth of domestic transactions, the bulk of which are internet transactions (92%). Remote payments account for 64% of fraud (internet payments accounting for 55% of fraud), down 6 points from 2021. However, internet payments benefited from the effects of the widespread introduction of strong authentication in 2022. The fraud rate for these payments fell by 27% compared with 2021. This puts it below the 0.1% threshold, a new all-time low. The

rate has fallen by 47% since 2017, when the PSD 2 strong authentication rules came into force. In 2022, the fraud rate only rose very slightly for point-of-sale and automatic teller machine (ATM) payments (including contactless payments).

Overall, the fraud rate for domestic card transactions is falling substantially: by 18% into 2022 (to a fraud rate of 0.033%), after an initial fall of 9% into 2021.

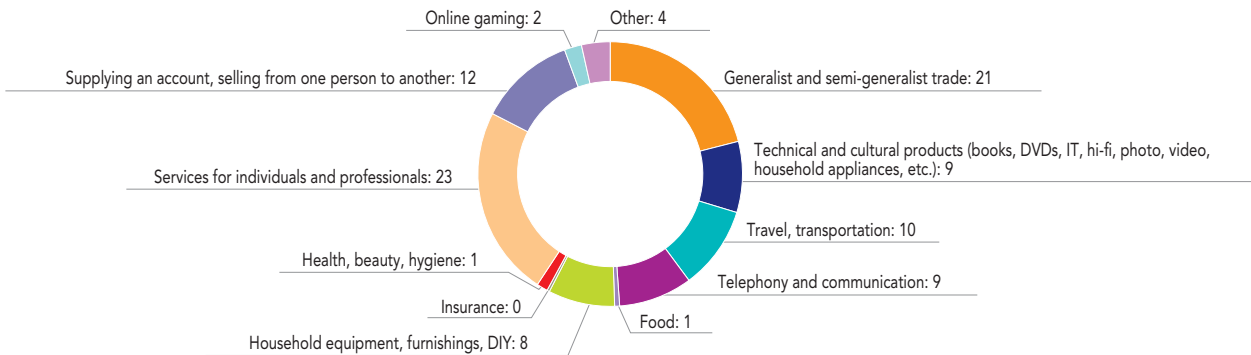
1.2.5 Focus on domestic card payment fraud on the internet

C20 Trends in fraud rate for domestic card payments over the internet, by sector (%)



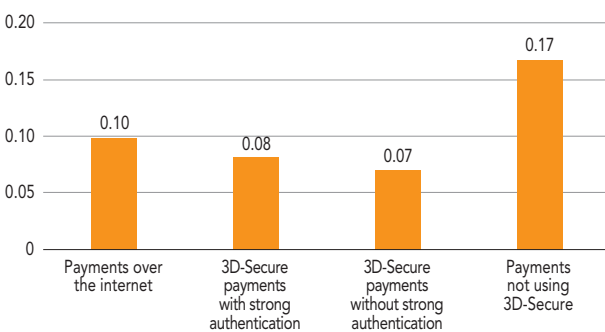
Source: Observatory for the Security of Payment Means.

C21 Breakdown of domestic card payment fraud over the internet by sector, in value in 2022 (%)



Source: Observatory for the Security of Payment Means.

C22 Fraud rate for domestic payments over the internet, by channel (%)



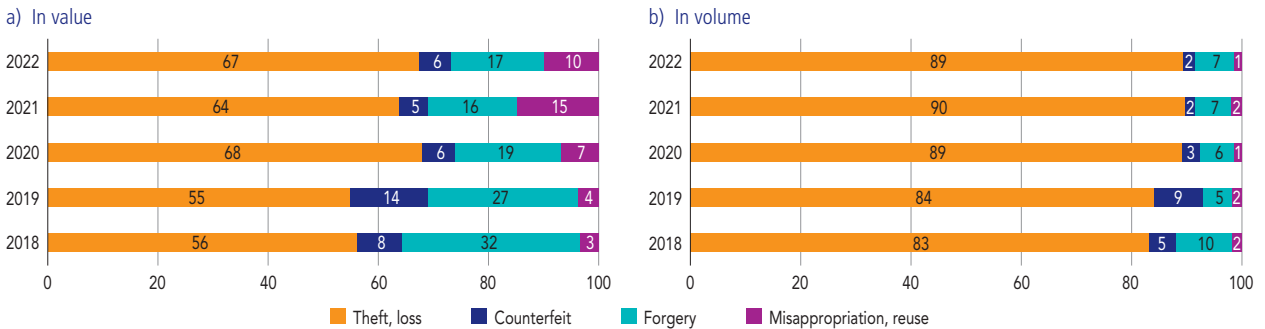
Source: Observatory for the Security of Payment Means.

At the domestic level, internet transactions that use the 3D-Secure exchange protocol (or an equivalent proprietary protocol) are subject to half as much fraud proportionally as those that do not. Non-3D-Secure transactions mainly include merchant initiated transactions (MITs), which are similar to direct debits but using the card as a medium (e.g. subscriptions, deferred payments or reservations), as well as a few other transactions exempt from strong authentication.

We also found a reliable application of authentication exemption rules in domestic transactions. In fact, exempt transactions processed through 3D-Secure have a fraud rate slightly lower than those subject to strong authentication (0.07% compared with 0.08%), revealing that exemptions are successfully assigned to the least risky transactions.

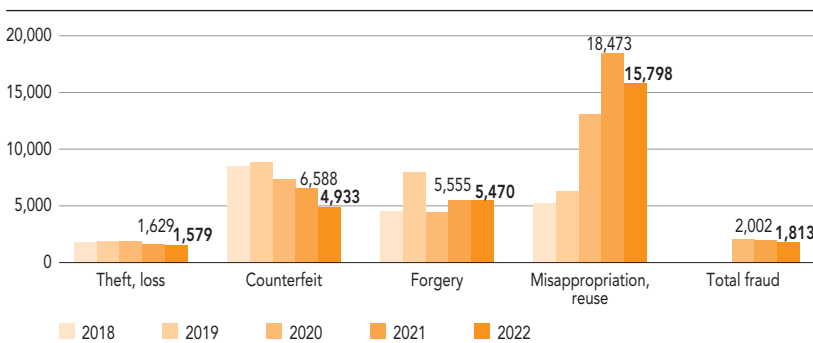
1.3 Current state of cheque fraud

C23 Breakdown of cheque fraud by type of fraud (%)



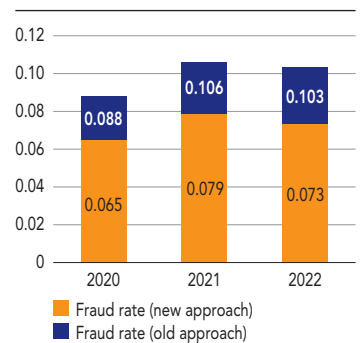
Source: Observatory for the Security of Payment Means.

C24 Average value of cheque fraud by type of fraud (in euro)



Source: Observatory for the Security of Payment Means.

C25 Effect of thwarted fraud on the cheque fraud rate (%)



Source: Observatory for the Security of Payment Means.

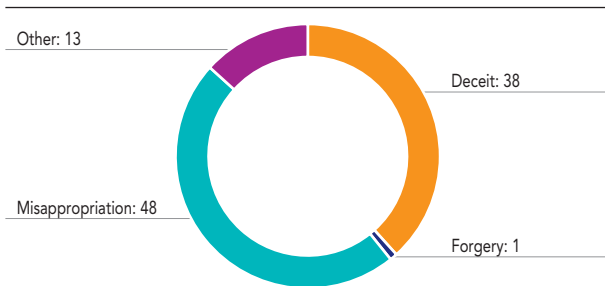
In 2022, the gross amount¹ of fraudulent cheque transactions fell to EUR 395 million (a reduction of 15% from 2021). The fraud prevention mechanisms deployed by banks following the roadmap drafted by the Observatory (in particular the systems for blocking or delaying cheque payments) have neutralised EUR 161 million in fraud. The fraud rate fell from 0.079% in 2021 to 0.073% in 2022. By far the main type of fraud remains the misappropriation of lost or stolen cheques, whether presented directly for payment by a fraudster or used as a means of payment with merchants or private individuals (representing 68% of fraud in terms of value and 89% of fraudulent transactions in terms of volume). The average amount of a fraudulent cheque has been falling steadily since 2020, dropping to EUR 1,813 in 2022.

These positive results start to reveal a solid impact of the action plan to combat cheque fraud drawn up by the Observatory in 2021. However, cheques are still the means of payment with the highest fraud rate. The Observatory calls on all stakeholders to continue their efforts and maintain their vigilance to ensure that the use of this means of payment develops in the most secure conditions possible.

¹ From 2020, the new approach to cheque fraud excludes fraud that is thwarted after the cheque has been cashed.

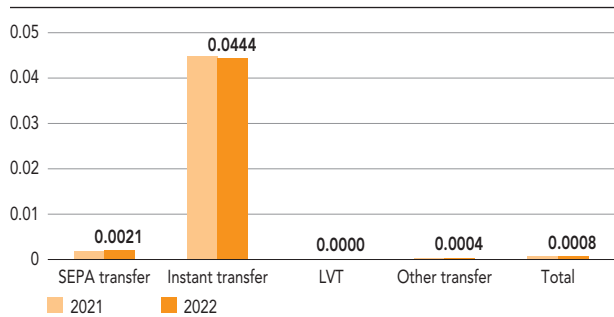
1.4 Current state of credit transfer fraud

C26 Breakdown of transfer fraud by type of fraud, in value in 2022 (%)



Source: Observatory for the Security of Payment Means.

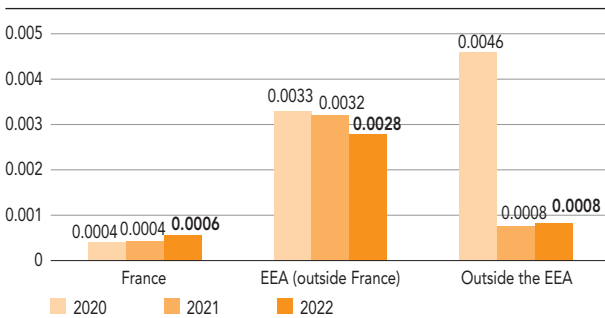
C27 Fraud rate by type of transfer (%)



Source: Observatory for the Security of Payment Means.

Note: SEPA – Single Euro Payments Area, LVT – large value transfer.

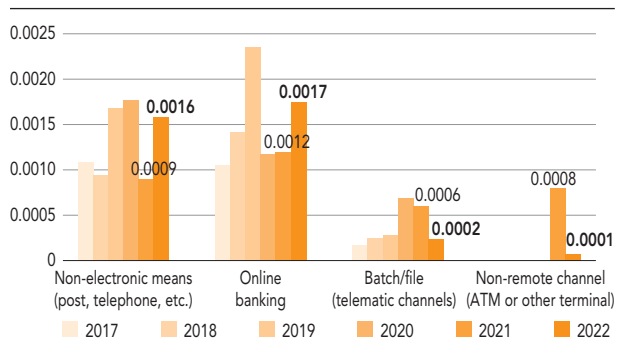
C28 Changes in transfer fraud rate by geographical area (%)



Source: Observatory for the Security of Payment Means.

Note: EEA – European Economic Area.

C29 Transfer fraud rate by payment channel (%)



Source: Observatory for the Security of Payment Means.

Note: ATM – automatic teller machine.

Bank transfer fraud continues to rise significantly. Transfer fraud has tripled in the last five years, rising from EUR 98 million in 2018 to EUR 313 million in 2022. In 2022, the number of fraudulent transactions rose by a further 64%, while their value only rose by 9%, resulting in a significant drop in the average value of a fraudulent transfer, to around EUR 4,000 (compared to *circa* EUR 6,000 in 2021).

Regarding the profile of its victims, transfer fraud is increasingly affecting private individuals and professionals, both in their use of online banking (EUR 216 million in fraudulent transactions) and in the transfers they initiated by non-electronic means (EUR 42 million). Conversely, the security of transfers initiated by businesses and public authorities through telematic channels has improved

significantly (EUR 53 million in fraudulent transactions, compared to EUR 92 million in 2021).

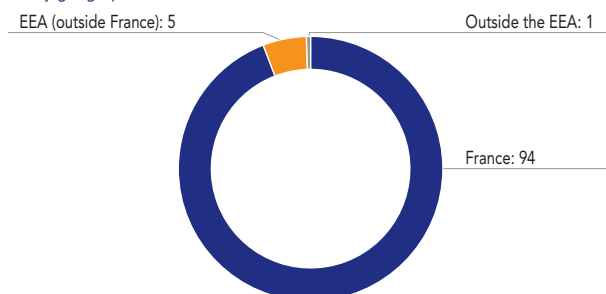
The methods used in defrauding transfer are evolving. Fraudsters make greater use of accounts opened in France to retrieve their funds even though European transfers are proportionally four times more defrauded than national transfers. Moreover, fraudsters increasingly use both phishing techniques to gain access to online banking, and telephone manipulation techniques to persuade their victims to provide sensitive data or validate a transaction.

The Observatory is nonetheless pleased to note that the fraud rate for instant transfers has stabilised and remains lower than for cards (0.044% compared with 0.053%).

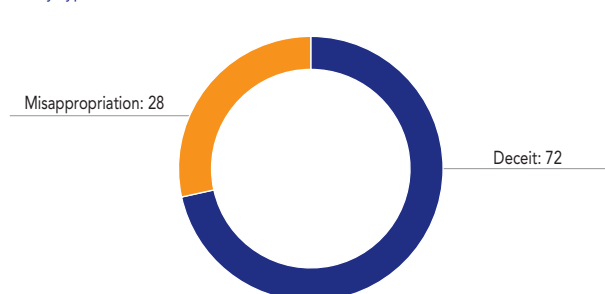
1.5 Current state of direct debit fraud

C30 Breakdown of direct debit fraud by value (%)

a) By geographical area



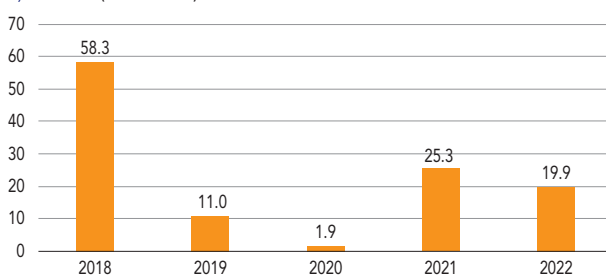
b) By type of fraud



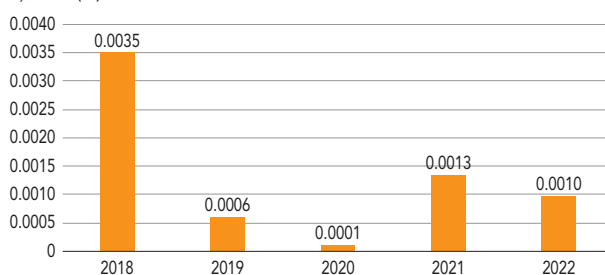
Source: Observatory for the Security of Payment Means.
Note: EEA – European Economic Area.

C31 Direct debit fraud

a) In value (EUR millions)



b) Rate (%)



Source: Observatory for the Security of Payment Means.

Direct debit fraud is volatile. It ended 2022 with a slight decrease, at EUR 20 million (compared with EUR 25 million in 2021), which is reflected in the payment channel's fraud rate (0.0010% in 2022, compared with 0.0013% in 2021). Most of these are the result of fraudsters issuing false orders, without having a direct debit order nor an economic relationship with the victim.

The Observatory notes three notable changes compared to 2021:

- firstly, most of the fraud recorded by creditors' institutions involves accounts opened in France (94%), whereas accounts opened in another European country had been the main target in 2021 (57%);

- secondly, the average value of a fraudulent direct debit multiplied by four, indicating that fraudsters targeted their actions more effectively;
- finally, misappropriation fraud, where the fraudster uses the identity and IBAN of a third party to sign a direct debit order, accounts for 28% of the total value defrauded, although this type of fraud had virtually disappeared by 2019.

1 Indicators, lessons and recommendations from the French Ministry of the Interior on payment fraud in 2022

The French Ministry of the Interior is represented in the Observatory by the central criminal intelligence service (SCRC – *Service central de renseignement criminel*) of the *Gendarmerie nationale* and the central directorate of judicial police (DCPJ – *Direction centrale de la police judiciaire*) of the French national police. In 2022, as they do every year, these two departments reported their main observations on payment fraud to the Observatory.

The statistics collected by the French Ministry of the Interior are based on methodological approaches that differ from those used by the Observatory. However, where comparisons are possible, the data show consistent trends, reinforcing the Observatory's findings on cashless payment fraud.

1. Bank card fraud: a rising rate of complaints, as well as figures consistent with those reported by payment operators to the Observatory

The French national police and *Gendarmerie* record offences relating to the fraudulent use of a bank card, whether the data is captured in France or abroad, relying on two statistical sources:

- figures from the French ministerial statistical service for internal security (SSMSI – *Service statistique ministériel de la sécurité intérieure*), which lists all the data reported by the national police and *Gendarmerie*;
- figures from searches by NATINF (nature of offence), an indicator designed according to the criminal classification of offences drawn up by the French Ministry of Justice.

These two classifications do not allow us to quantify the number of fraud cases by card specifically, nor the financial losses incurred. Because they are part of an aggregate measuring card theft, fraudulent use of lost cards, forgery and counterfeiting, the options for reconciling their data with that of the Observatory are limited.

By contrast, comparisons are easier with data from the *Gendarmerie's* Perceval platform, which is the national platform for reporting fraudulent use of cards on the internet, intended for all users. According to this data, in 2022 there were 304,923 reports (compared with 324,594 in 2021, a drop of 6.1%), with total losses incurred of EUR 161 million (compared to EUR 140 million in 2021, an increase of 14%), representing an average loss per report of EUR 529 (compared with EUR 431 in 2021, an increase of 23%).

One single report on the Perceval platform may, however, cover several different fraudulent transactions initiated using the same stolen card details.

A comparison with the Observatory's statistics shows an increase in the number of frauds reported on Perceval. In fact, in 2022, the reports on Perceval account for 51% of the remote payment card fraud quantified by the Observatory, compared with 40% in 2021. Victims tend to report only the largest frauds: in 2022, the average value of a fraudulent transaction, according to the Observatory's statistics, was EUR 58, compared with EUR 131 according to Perceval.

The Observatory would like to point out the usefulness of fraud declarations on the Perceval platform, which enable law enforcement agencies to cross-check the information needed to dismantle fraud networks.

T1 Number of bank card fraud incidents recorded by the French national police and *Gendarmerie* (number in units, change in %)

| | 2018 | 2019 | 2020 | 2021 | 2022 | Changes 2022/2021 |
|-----------------------------|--------|--------|--------|--------|--------|-------------------|
| Source: SSMSI ^{a)} | 57,796 | 67,366 | 61,235 | 74,706 | 78,373 | 4.91 |
| Source: NATINF | 53,276 | 64,168 | 58,414 | 70,425 | 72,955 | 3.59 |

a) The figure for the number of fraud incidents on a given year may increase from one year to the next, as the police may record complaints relating to fraud in previous years.

Sources: French ministerial statistical service for internal security (SSMSI – *Service statistique ministériel de la sécurité intérieure*) and French Ministry of Justice.

2. Hacking of payment and cash withdrawal terminals: in decline for several years now, despite a few high-profile cases

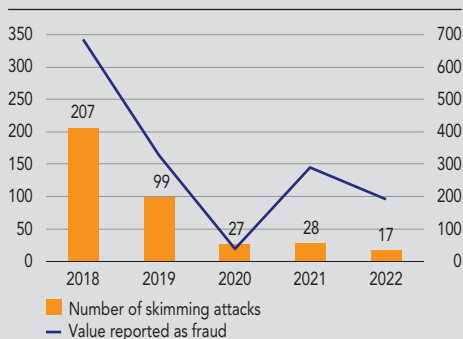
Hackers target payment or cash withdrawal teller machines (cash dispensers, automatic fuel dispensers, motorway vending machines, car park payment machines, etc.). Payment terminals, including handheld terminals or contactless acceptance sets, can also be compromised or misused, for example by being replaced by a fraudulent acceptance device.

Skimming¹ involves the capture of bank details stored on the card's magnetic strip by means of tampered payment terminals. In both cases, the card data obtained by the crime networks is then re-encoded on magnetic stripe cards. These counterfeit cards are then used for withdrawals or payments at point of sale where reading the chip is optional, such as payments at motorway toll booths or in countries where smart cards are not yet widely used (countries in South America or South-East Asia). Skimmed details can also be used for remote payments, mainly on non-European e-commerce sites that have not implemented strong cardholder authentication.

Law enforcement figures show a drastic fall in skimming piracy in recent years.

For the year 2022, 17 attacks have been recorded for a total loss of EUR 190,000 (compared with EUR 290,000 in 2021, i.e. a fall of 53%), including 3 attacks on cash dispensers (ATMs – automatic teller machines), compared with 15 in 2021, and 14 on fuel dispensers, compared with 13 in 2021. These trends

Number of skimming attacks and reported amounts of fraud in euro since 2018 (left-hand scale: volume in units, right-hand scale: value in EUR thousands)



Sources: Groupement des cartes bancaires (GCB) and the central directorate of the French judicial police (DCPJ – Direction centrale de la police judiciaire).

are consistent with those reported by payment operators to the Observatory. The Observatory reports, for 2022, a 64% drop in fraud linked to counterfeit cards used for cash withdrawals outside Europe, representing total damages of EUR 127,000.

Nevertheless, service station managers, like ATM managers, must remain vigilant to prevent attempts to replace a legitimate payment terminal with a compromised terminal or any installation by a third party of a fraudulent external device (reader, camera, keyboard, etc.), as law enforcement agencies report that fraudsters are still very active. The French central office for combating information and communication technology crime (OCLCTIC – *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*) receives, from Interpol, an increasing number of requests to freeze service station surveillance videos: 110 applications in 2022, compared with 91 in 2021 and 76 in 2020. The cards pirated in France, mainly fuel cards, would then be used on motorway tolls in France or in Central and Eastern Europe, particularly in Poland, the Czech Republic, Slovenia, Slovakia and Bulgaria.

Shimming² is based on processes similar to skimming, but aimed at capturing the data contained in the card chip. The technical complexity of this system limits attacks considerably. The financial losses associated with this type of attack were not estimated for 2021, but amounted to close to EUR 50,000 in 2022.

3. Jackpotting attacks on ATMs: down thanks to the dismantling of criminal networks

The police are continuing their investigations into ATM jackpotting attacks. This is a physical or digital attack on an ATM with the aim of hacking into the embedded computer, taking control of it and thus activating the cash dispensing mechanisms. These highly sophisticated techniques are only accessible to organised criminal networks or specialised criminals.

1 A device that slides into the card reader of a vending machine, leaving space for a payment card to be inserted naturally. A copy of the data on the magnetic strip of the card will then be made by the device, without this having any effect on the correct operation of the card.

2 A device somewhat similar to a skimmer in its integration into an ATM, but which intercepts the data on the card's chip, including its confidential code.

The losses caused by jackpotting are falling sharply: in 2022, 22 incidents of jackpotting were recorded, causing a total damages of EUR 74,970, compared with 32 incidents in 2021, causing damages of EUR 335,370, and 95 incidents in 2020, costing EUR 681,170. This type of attack is not reported in the Observatory's data, as these losses are recorded as operational risk by ATM managers, and not as payment fraud as such.

The net reduction in this type of crime derives from the action taken by law enforcement agencies (infiltration, use of video surveillance images, bugging, etc.), which has allowed them to dismantle the criminal networks behind the attacks: in 2021, the OCLCTIC arrested 12 professional criminals and dismantled 5 criminal gangs in regard to the attacks. In 2022, they also arrested a suspect known to the law for similar offences. The case is still under investigation.

These good results are also linked to the increased security of ATMs by ATM managers. However, the OCLCTIC points to the obsolescence of hardware and software, which still too often facilitates successful attacks. It therefore recommends that ATM operators take minimum security measures, in particular to:

- systematically update operating systems;
- encrypt the hard drive to prevent attacks that do not go through the operating system;
- install anti-intrusion sensors capable of disabling the ATM in the event of an attack;
- or reinforce the security of communication between the ATM and the devices dedicated to its maintenance.

4. Fraudulent transfer orders: stable overall, but a point of vigilance for local authorities

False transfer orders (FOVI – *faux ordres de virement*) are characterised by law enforcement as a financial scam in which the victim is asked to make an unscheduled transfer to a bank account managed by the fraudster. Usually operating by telephone or email and using social engineering techniques, fraudsters exploit the technical, human and organisational vulnerabilities of a company or public authority to provoke fraudulent transfers.

The widespread introduction of telework since 2020 has led to an exponential increase in cases of FOVI; a rapid deployment of new operating and organisational methods has enabled malicious actors to exploit new or pre-existing vulnerabilities. **While, in 2022, the number of FOVI cases rose, overall losses from these attacks fell:** law enforcement agencies identified 670 FOVI cases in 2022, leading to losses of EUR 64 million, compared to 517 cases in 2021, causing losses of EUR 101 million, including a single fraud case generating exceptional damages of EUR 33 million.

Private sector companies are not the only targets of fraudsters. **In 2022, public institutions, particularly local authorities (university hospitals, municipal theatres, town halls, metropolitan areas, municipalities, cities, départements, etc.) accounted for half of the incidents known to the French criminal investigation police.**

T2 Comparison of transfer fraud data involving manipulation of the victim between 2021 and 2022 (value in EUR, number in units, change and rate in %)

| | Observatory ^{a)} | | | FOVI reported by French national police | | | Reporting rate | |
|---|---------------------------|-------------|-------------------|---|------------|-------------------|----------------|------|
| | 2021 | 2022 | Changes 2022/2021 | 2021 | 2022 | Changes 2022/2021 | 2021 | 2022 |
| Total value of fraud | 168,094,274 | 148,732,203 | -12 | 101,200,000 | 64,000,000 | -37 | 60 | 43 |
| Number of fraudulent transactions | 8,523 | 16,991 | +99 | 517 | 670 | +30 | 6 | 4 |
| Average value of a fraudulent transaction | 19,722 | 8,754 | -56 | 195,745 | 95,522 | -51 | nd | nd |

a) In the Observatory's methodology, FOVI can be equated with embezzlement (see Appendix 4 on statistical methodology). However, the comparison is limited by the fact that the figures provided by the French national police mainly concern companies and public authorities, whereas the Observatory's figures cover all users, including private individuals.

Sources: Central directorate of the French judicial police (DCPJ – Direction centrale de la police judiciaire) and Observatory for the Security of Payment Means.

Note: FOVI – *faux ordres de virement*, false transfer orders; n/a – not applicable.

These developments are consistent with the general trends reported to the Observatory by payment operators: transfer fraud is on the rise in online banking both for individuals and professionals, but is stabilising in the channels used by businesses and public authorities.

2

TERMS AND CONDITIONS FOR THE REIMBURSEMENT OF FRAUDULENT PAYMENT TRANSACTIONS

2.1 Background to the work

2.1.1 Introducing strong customer authentication to secure electronic payments

The use of strong authentication of the payer to initiate an electronic payment is a key provision in payment security, introduced by the Second European Payment Services Directive (PSD 2).¹ For card payments over the internet, the implementation of this provision on the French market followed a migration plan adopted by the Observatory in autumn 2019, and strong authentication was then rolled out over a period of around two years.

For reference, strong authentication is based on the use of two or more elements belonging to at least two different categories of authentication factors, from among the following three categories:

- knowledge: information that only the user knows, for example a confidential code, a password or personal information;
- possession: an object that only the user has, and which can be recognised without risk of error by the payment service provider (PSP), such as a card, smartphone, USB key, secure box, connected watch or bracelet, etc.;
- inherence: something the person is, i.e. a biometric feature (fingerprint, face, voice, etc.).

When the registration of a possession element (registering the association of an object with a user, an object that only this user possesses) which will be used as a strong authentication factor, is carried out remotely, then this registration must itself be validated by strong authentication.

PSD 2 provides that these elements must be independent: having one element compromised should not affect the reliability of the others, thereby preserving the confidentiality of authentication data. For remote payments, PSD 2 adds a requirement: the authentication data must be linked to the payment transaction, so that it cannot be reused for a subsequent payment transaction. This is known as a dynamic link:

- the authentication code generated for the transaction is specific to the amount of the transaction and the identified beneficiary;
- any change to the amount or beneficiary requires a new authentication.

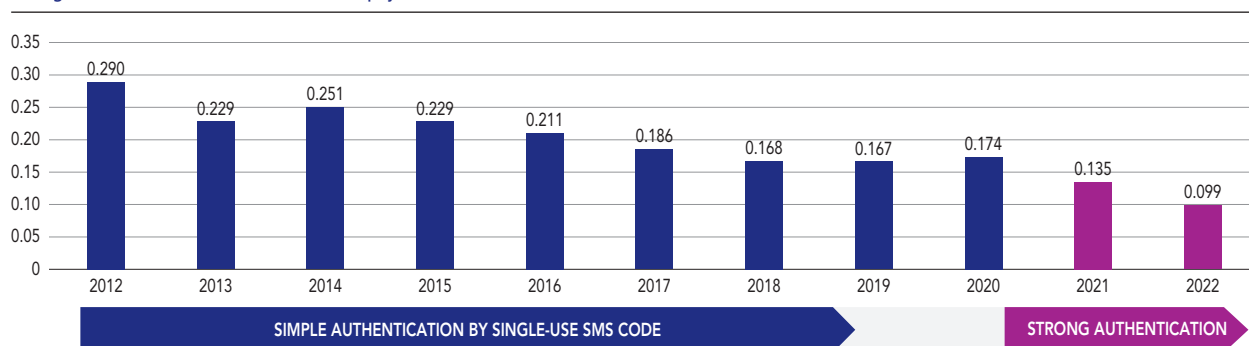
If a biometric element is used, the validation key generated as a result of the biometric reading should also be a one-time use key.

Although it is still too early to draw up a definitive assessment of the effects of the introduction of strong authentication, the Observatory can already observe that it has contributed to a substantial fall in the fraud rate for payments over the internet, following two stagnant years that highlighted the security limits reached in the use of simple authentication (SMS-OTP – one time password, single-use SMS code) deployed during the 2010s. The first data available for 2022 show that the fraud rate should continue to fall significantly.

¹ Directive (EU) 2015/2366 of the European Parliament and of the Council

of 25 November 2015 on payment services in the internal market.

Changes in the fraud rate for domestic card payments over the internet (%)



Source: Observatory for the Security of Payment Means.

The fraud rate for all card payments over the internet (including payments made to foreign sites by French cardholders) fell from 0.249% in 2020 to 0.196% in 2021, its lowest level ever, while the value of card payment transactions rose by 21% to EUR 177.1 billion over the same period.

2.1.2 The development of new fraud techniques based on manipulation to circumvent strong authentication

While the introduction of strong authentication makes it possible to ensure a high level of technological security throughout the payment chain, it also makes it all the more necessary to heighten the vigilance of users, who are increasingly being targeted by fraudsters. When fraudsters are unable to issue fraudulent payments themselves, they try to manipulate their victims by telephone or instant messaging to get them to validate the transactions on their behalf, usually by pretending to be their bank (for example, using the pretext of security tests in the fight against fraud, or warning about an atypical transaction on the victim's account requiring authentication). They manage to persuade their victims to provide them information, thereby acquiring the capacity to use their payment methods remotely. They first gather information about their victims through phishing attacks by SMS or email, through data theft from third parties, or through social networks and various public sources, and then contact the victim directly. Fraudsters also resort to misappropriation, where they manage to fake the telephone number of a bank branch in order to reassure their victim.

While the Observatory has observed that the proportion of fraudulent payments with strong authentication remained low in 2021, at 9% of the total number of fraudulent card

payments over the internet, their proportion of the total amount of fraudulent transactions is much more significant (30% of a total amount of EUR 103 million).

According to consumer associations, this new type of fraud is likely to lead to an increase in the amount of financial losses borne by consumers, despite an overall decline in fraud, given that the implementation of strong authentication is likely to increase significantly the rate of the bank refusing to reimburse a customer for a fraudulent transaction.

Consumer associations have alerted the Banque de France and the Observatory for the Security of Payment Means to the difficulties encountered by their members in exercising their right to reimbursement in the event of fraud provided for in the legislation, particularly in cases where the disputed transaction has been subject to strong authentication.

2.1.3 The work carried out by the Observatory on the processing of complaints on grounds of fraud

The Observatory has set up a working group to issue recommendations on the processing of requests for reimbursement of fraudulent transactions, with a view to ensuring the proper application of the provisions of PSD 2 on the protection of consumers who are victims of fraud.

The working group met five times between October 2022 and February 2023. Its participants represent consumer associations, payment service providers, their professional federations, ombudsmen and the authorities (French national police, *Gendarmerie*, French Prudential Supervision and Resolution Authority – ACPR, *Autorité de contrôle prudentiel et de résolution* –, and Banque de France).

The secretariat of the working group has defined the input elements and the expected output for the project:

Scope of the working group's remit

| Input elements | Expected output |
|---|--|
| <ul style="list-style-type: none"> Regulations and jurisprudence applicable to disputes | <ul style="list-style-type: none"> Reminder of the rules applicable to the processing of claims for reimbursement on grounds of fraud |
| <ul style="list-style-type: none"> Identification of recent developments in fraud typology | <ul style="list-style-type: none"> Claims analysis grid (identify cases where immediate reimbursement should be systematic) |
| <ul style="list-style-type: none"> Experience of banking ombudsmen and consumer associations with unsatisfied requests for reimbursement on the grounds of fraud | <ul style="list-style-type: none"> Recommendations on the processing of fraud claims |
| <ul style="list-style-type: none"> Summary of on-site inspections carried out by the ACPR on the processing of customer claims for reimbursement on grounds of fraud | <ul style="list-style-type: none"> Review of the reasons identified in the declarations to the Banque de France under Article L. 133-8 of the French Monetary and Financial Code (to be undertaken following publication of the recommendations presented in this document) |

Source: *Observatory for the Security of Payment Means*.

Note: ACPR – *Autorité de contrôle prudentiel et de résolution*, French Prudential Supervision and Resolution Authority.

2.2 Regulations applicable to payment transaction disputes

2.2.1 The “authorised” nature of the transaction as a determining factor

Under the French Monetary and Financial Code (CMF – *Code monétaire et financier*), reimbursement of a disputed transaction is conditional on whether or not it has been authorised by the payer.² Payment authorisation by the payer means that the latter has explicitly given their consent to the execution of the payment under the conditions set out in their account agreement, in particular by using the strong authentication means made available to them.

The diagram below illustrates the provisions relating to disputed transactions provided for in the French Monetary and Financial Code.

- If the transaction is deemed “authorised” and has not been affected by an execution error on the part of the payer’s payment service provider, the regulations relating to means of payment do not provide for a right to reimbursement.** This is the case in particular for claims for reimbursement due to a commercial dispute between the payer and the beneficiary (for example: non-delivery or poor quality of a product,

taking out a savings, credit or financial service on behalf of a malicious intermediary, etc.). **In the absence of a right to reimbursement under the regulations, the fact that the transaction is classified as “authorised” does not preclude a claim against the beneficiary, or even civil or criminal proceedings.**

- If the transaction is deemed to be “unauthorised”, the payer generally has a right to immediate reimbursement under the French Monetary and Financial Code.** However, the terms and conditions differ depending on various parameters (such as the nature of the payment instrument, whether it is equipped with personalised security data or whether a device registered for strong authentication is used in the transaction), **and reimbursement may be refused on the grounds of fraudulent behaviour on the part of the user or, for transactions that have been strongly authenticated following the conditions laid down by law,³ on the grounds of gross negligence on the part of the user as demonstrated by the payment service provider.**

Assessing whether a transaction has been authorised or not is therefore a decisive criterion for reimbursing customers who dispute a payment transaction on the grounds of fraud. This question is particularly relevant in the case of transactions which have been subject to strong authentication, where it is necessary to determine to what extent the success of the strong authentication can or cannot be equated with the consent of the holder of a payment instrument.

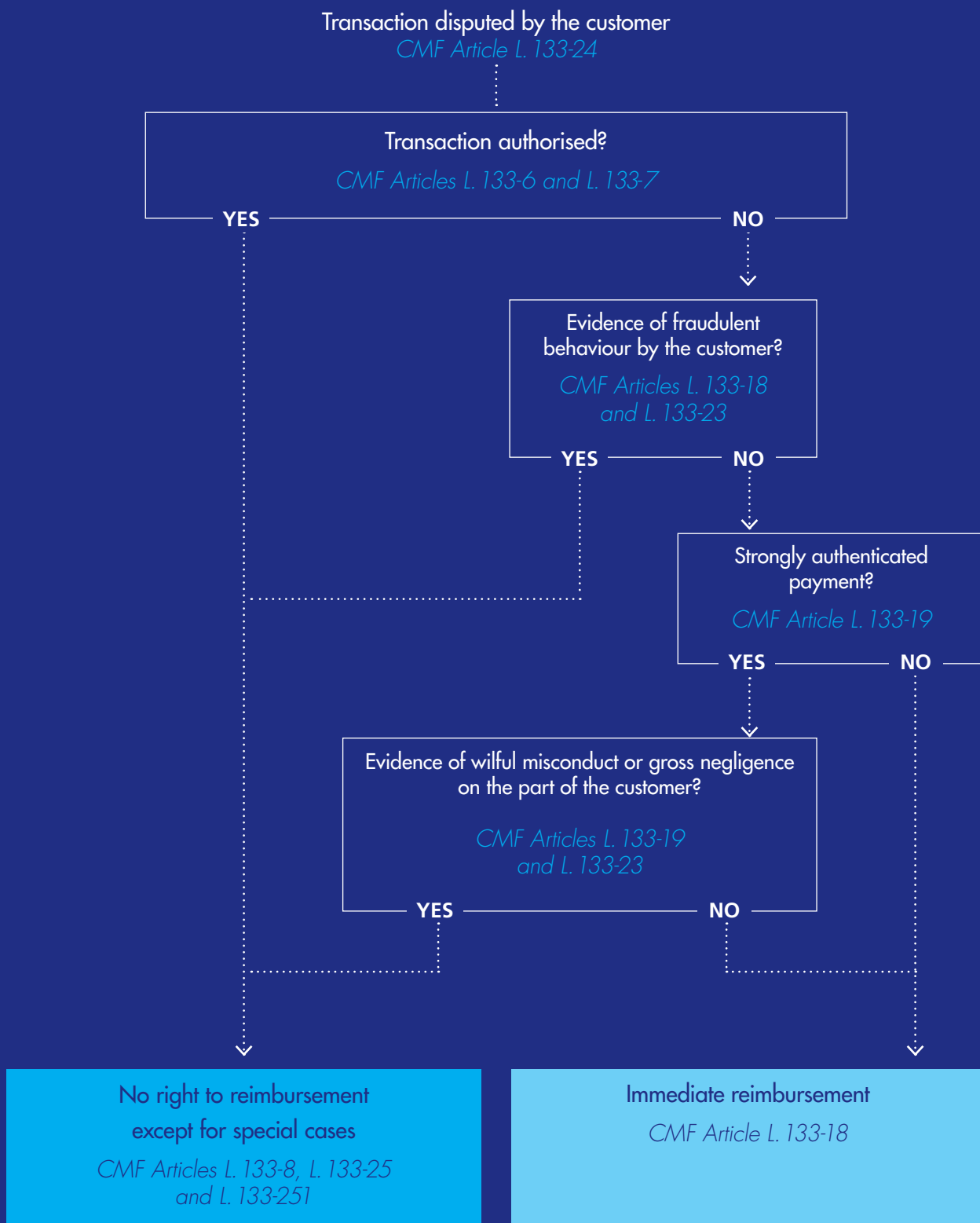
By considering the various potential cases of dispute, from the simplest to the most complex, the recommendations below set out to reduce the grey areas in the assessment of whether a disputed transaction has been authorised. The aim is to determine the conditions under which a transaction may be presumed to be unauthorised and give rise to an immediate reimbursement, provided the payment service provider cannot prove fraud or gross negligence on the part of the user.

² Excluding the specific case provided by regulations on reimbursement applicable to certain authorised transactions, including withdrawals made less than eight weeks prior (Articles L. 133-25 and L. 133-251 of

the CMF – *Code monétaire et financier*, French Monetary and Financial Code).

³ Article L. 133-4 paragraph f of the CMF (*Code monétaire et financier*, French Monetary and Financial Code).

SPECIFICATIONS OF THE FRENCH MONETARY AND FINANCIAL CODE (CMF – CODE MONÉTAIRE ET FINANCIER) RELATING TO PAYMENT TRANSACTIONS DISPUTED BY THE CUSTOMER



Source: Observatory for the Security of Payment Means.

2.2.2 Jurisprudence in the assessment of gross negligence on the part of the payment service user

Prevailing legislation does not explicitly state what constitutes gross negligence on the part of the user, and this loophole is taken advantage of by payment service providers to justify refusing to reimburse an unauthorised payment. There is as yet no jurisprudence from the French Supreme Court (*Cour de cassation*) relating to a disputed transaction carried out after the entry into force of PSD 2, nor are there any texts transposing or applying PSD 2 for such cases. Current jurisprudence (relating to disputed transactions carried out prior to the entry into force of PSD 2) is based on the concept of the “normally attentive” user. Payment service providers wishing to refuse reimbursement on the grounds of gross negligence by the user should assess cases in light of the concept of the “normally attentive” user; although the jurisprudence is yet to grow in the coming years, some of its judicial decisions are already instructive.

2.3 General recommendations for handling payment transaction disputes

2.3.1 Deadline for investigations

Where investigations have to be carried out by the payment service provider (e.g. investigations relating to a payment transaction that has been strongly authenticated, see *paragraph 4.3 below*), the duration of these investigations should be limited in time. The aim is to prevent information useful to the PSP from disappearing or being forgotten, and to ensure that the customer receives a clear and definitive response to their complaint at a sufficiently early and known date.

Recommendation 1: Deadline for investigations

Payment service providers are asked to initiate investigations as soon as they receive communication of the dispute, taking into account any descriptive information provided by the user (as specified in Recommendation 8), and to limit the duration of the investigation to 30 days, other than in exceptional circumstances.

2.3.2 Terms and deadlines for recovering funds

There are various situations where an initial decision by a payment service provider to reimburse their customer

may be challenged after the event. This means that the service provider can reclaim the funds, for example, if further investigations lead it to reverse its initial decision or if the user is reimbursed through another channel (by the counterparty to the transaction, via an insurance mechanism, etc.). Users should be informed of this possibility at the time of their reimbursement.

Recommendation 2: Informing the customer in the event of repossession of reimbursement

In the event of a reimbursement that may give rise to the subsequent repossession of the funds on the basis of the results of the investigations carried out, the payment service provider is to inform the customer of this possibility at the time of the reimbursement, and ensure that the funds are not repossessed more than 30 days after the date on which the reimbursement was made, other than in exceptional circumstances.

2.3.3 Information given to the customer in the event of refusal to reimburse or of repossession of reimbursement

Recommendation 3: Justifying a refusal to reimburse

If the payment service provider refuses to reimburse or repossesses a reimbursement, it must inform the customer of this decision and give the reasons for it, attaching any supporting documents (e.g. direct debit order, information provided by the merchant, evidence of gross negligence, etc.). The same communication also sets out the procedures for lodging a complaint.

2.4 Recommendations applicable to the treatment of specific cases

The cases presented in this section deliberately exclude claims that do not fall within the scope of payment fraud, such as commercial disputes and scams (e.g. bogus savings products, investments in rogue cryptoassets, credit scams, etc.), where the transactions concerned have been authorised.

Similarly, the recommendations focus on the application of the right to reimbursement provided for in the regulations on means of payment. They exclude other mechanisms that may exist, such as payment instrument insurance or commercial offers made by payment service providers.

2.4.1 Payment transactions carried out without strong authentication

Not all transactions require strong authentication. The regulations resulting from the Second European Payment Services Directive (PSD 2) provide for a series of exclusions or exemptions from its application:

- **Payments outside the European Union (one leg out);**
- **Payment orders issued by the beneficiary of the payment**, such as direct debits or merchant initiated transactions (MITs), i.e. card payments issued by the merchant without an active user login, including fractional or deferred payments, subscriptions and pay-as-you-go;
- **Payments eligible for exemption from strong authentication under the regulatory technical standards (RTS)** laid down by the European Banking Authority (EBA):⁴
 - low-value payments over the internet (Article 16), i.e. less than EUR 30, up to a limit of five consecutive transactions or a cumulative amount of EUR 100;
 - payments with a low level of risk (Article 18), i.e. corresponding to the cardholder's purchasing habits
- **Payments issued as part of the authentication infrastructure continuity mechanisms** (should there be an incident preventing the implementation of strong authentication of the payer), as well as card payments made during the transitional phase in the deployment of strong authentication (from 14 September 2019 to 15 June 2021).
 - (purchase from their usual terminal, known delivery address, nature of the purchase, amount, etc.) and for an amount not exceeding EUR 500;
 - recurring payments (Article 14), i.e. payments of a fixed amount and frequency to the same beneficiary, from the second transaction onwards;
 - payments to a trusted beneficiary (Article 13), i.e. to a beneficiary designated as trusted by the payer, this designation having itself been subject to strong authentication when the beneficiary was added (this strong authentication has neither the purpose nor the effect of strongly authenticating subsequent payment transactions made to this beneficiary);
 - payments initiated electronically using secure payment processes or protocols reserved for use between professionals (Article 17).

Recommendation 4:

Principles applicable to transactions without strong authentication

Where a payment service user disputes one or more transactions which they deny having authorised and where those transactions have not been strongly authenticated, the payer's payment service provider shall refund the amount of those transactions without delay,¹ except if it has good reason to suspect fraud by the payment service user.

This immediate reimbursement does not prevent the funds from being repossessed at a later date if the payment service provider has evidence either that the transaction was authorised (for example, by the existence of a SEPA direct debit order)² or that fraud was committed by the user. However, even serious negligence on the part of the user cannot be used as a basis for refusing to reimburse a transaction that has not been strongly authenticated.

In the case of payments initiated by the payee (direct debits or MIT card payments), the user also has the right to immediate reimbursement within eight weeks of the debit to the account:

- for direct debits, the reimbursement is unconditional, regardless of whether or not a direct debit order exists;
- for card payments ordered by the payee (MIT), if the

authorisation given did not indicate the exact amount of the payment transaction and if the amount of the disputed transaction exceeds the amount that the payer could reasonably have expected taking into account their past spending pattern, the conditions set out in their framework contract and the specific circumstances of the transaction.

References: Articles L. 133-19, L. 133-18, L. 133-25 and L. 133-251 of the CMF (Code monétaire et financier, French Monetary and Financial Code) and the SEPA Direct Debit Core Scheme Rulebook V1.1 Section 4.3.4.

¹ The regulations stipulate that the reimbursement must be made immediately after becoming aware of the transaction or after being informed of it, and in any event no later than the end of the first working day following the date on which the claim was lodged, and must include any additional charges incurred temporarily as a result of the fraudulent transaction (overdraft charges, debit interest, etc.).

² Except for direct debits disputed within eight weeks of the account being debited, for which the payer has an unconditional right to reimbursement. SEPA – Single Euro Payments Area.

In no case listed above can the transaction be considered as strongly authenticated within the meaning of the regulations. In fact, in most of these cases, the absence of strong authentication is authorised or tolerated.

The payment service provider must be able to prove that a transaction has been authenticated, and must therefore retain the technical elements (audit trail) relating to this authentication. The same applies to the audit trail of the strong authentication performed for the registration of an authentication factor.

2.4.2 Payment by means of a mobile application replacing the payment instrument

To make payments using a mobile solution that has its own authentication method (which is the case, in particular, with the X-Pay mobile solutions offered by terminal manufacturers and operating system developers), users must first register their payment instrument with the payment application on their mobile terminal. This registration, which is considered a sensitive operation within the meaning of the regulations, requires strong authentication on the part of the user (EBA: Single Rulebook Question and Answer – Q&A – 2021_6141). Responsibility for implementing strong authentication rests with the payment service provider, who is responsible for proving compliance with this obligation.

Recommendation 5:

Principles applicable to transactions carried out with a mobile application replacing the payment instrument

Where the user disputes a payment transaction which they deny having authorised and which was carried out using a mobile solution for which strong authentication was not used to register the payment instrument, the payment service provider shall refund the amount of the transaction without delay.¹

References: Article L. 133-18 of the CMF (Code monétaire et financier, French Monetary and Financial Code) and EBA Q&A 2021_6141.

¹ The regulations stipulate that the reimbursement must be made immediately after becoming aware of the transaction or after being informed of it, and in any event no later than the end of the first working day following the date on which the claim was lodged. The reimbursement must also include any costs incurred as a result of the fraudulent transaction (overdraft charges, debit interest, etc.).

2.4.3 Payment subject to strong authentication

Most of the “grey area” referred to above concerns disputed transactions that have been strongly authenticated. The investigation process of payment service providers must focus on examining the elements and parameters likely to alter the user’s strong authentication.

The **elements of analysis to be taken into account** are as follows:

- **The possibility of a misappropriation of the strong authentication means by a third party**, in particular in the event of the occurrence of one or more of the following factors:
 - upstream transfer of the strong authentication method (e.g. registration of a new mobile phone);
 - the issue of a new SIM card by the telephone operator, in the case of a “reinforced SMS” type strong authentication solution;
 - identifiers entered by a third party or on a terminal that does not belong to the user (in the case of strong authentication solutions requiring authentication data to be entered on the payment site).
- **The parameters of the transaction, aimed at assessing the extent to which the user is or is not behind it:** this analysis is necessary to determine whether, on the one hand, the disputed transaction is the result of a commercial dispute rather than payment fraud (in the case of a commercial dispute, the transaction was initiated by the user) or, on the other hand, the transaction was clearly initiated by someone other than the user (although the user may have been approached by the fraudster at the time of authentication).
- **Elements relating to the context of the transaction**, in particular the quality and completeness of the information provided by the payment service provider when authenticating the transaction or through real-time alert mechanisms, as well as **the elements reported by the user** (see Recommendation 8).

⁴ Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament

and of the Council with regulatory technical standards for strong customer authentication and common secure open standards for communication.

Recommendation 6:

Principles applicable to strongly authenticated transactions

When a customer disputes a payment transaction that they deny having authorised and the transaction has been strongly authenticated, the payment service provider must carry out an initial analysis of the transaction within one working day. The analysis will aim to assess, by taking into account the three families of parameters mentioned below, whether the user is likely to have consented to the transaction or whether it is an unauthorised transaction:

- the technical parameters associated with the operation (such as the origin of the transaction, the terminal used for the purchase or the connection to the online bank, the geographical location, etc.), to assess whether the user could have initiated the transaction;
- the strong authentication methods used (such as type of solution, integrity of the authentication factors and communication channel, proof of previous use of the solution by the user or, on the contrary, the recent nature of the registration, etc.), to assess whether the user is being impersonated;
- the background information available: such as the information given to the user during authentication (*see Recommendation 11*), any alerts linked to the transaction and sent to the user via different communication channels, elements reported by the user (*see Recommendation 8*), such as any manipulative methods which they may have encountered.

After this first analysis:

- either the payment service provider finds that the transaction has not been authorised or has doubts about the consent given, in which case it proceeds without delay¹ to reimburse the transaction;

- or the payment service provider has good reason to suspect fraud by the user² and communicates its reasons to the Banque de France, with the option of refusing to reimburse the transaction immediately under the conditions set out in Recommendation 3;
- or the payment service provider has sufficient evidence to consider that the transaction was authorised by the user,³ or that the user was grossly negligent,⁴ or that the user intentionally failed to meet their obligations, in which case it may refuse reimbursement of the disputed transaction under the conditions provided for in Recommendation 3.

In the first two cases, and on the basis of the same criteria mentioned above and any new information provided by the user, the payment service provider may continue its investigations under the conditions set out in Recommendations 1 to 3 in order to determine the user's right to reimbursement.

References: Articles L. 133-18, L. 133-19 and L. 133-23 of the CMF (Code monétaire et financier, French Monetary and Financial Code).

1 The regulations stipulate that the reimbursement must be made immediately after becoming aware of the transaction or after being informed of it, and in any event no later than the end of the first working day following the date on which the claim was lodged. The reimbursement must also include any costs incurred as a result of the fraudulent transaction (overdraft charges, debit interest, etc.).

2 Within the meaning of Article L. 133-18.

3 Within the meaning of Article L. 133-6.

4 Within the meaning of Articles L. 133-19 and L. 133-23.

2.5 Recommendations for consumers and their representatives

2.5.1 Good practices for the security of payment means

Faced with the ingenuity of fraudsters looking for ways around increasingly sophisticated security systems, consumers have a key role to play in protecting the security of their own payment methods through vigilant and responsible behaviour.

In particular, as regards their use of the internet, they are responsible for ensuring the security of the data associated with their means of payment. In particular, users must avoid disclosing them to third parties, as this action is conducive to fraudulent attacks; such data are just as sensitive as the confidential code of their payment card. Failure to comply with these best practices may constitute negligence on the part of the user, which may be held against them.

Recommendation 7:**Good practices for the security of payment means**

Consumers should endeavour to remain vigilant about preserving the confidentiality of the security data associated with a payment instrument (password, confidential code, cryptogram, etc.), by complying with good practices in this area:

- not communicating these data to a third party;
- not storing these data on any medium whatsoever, whether physical (notebook, post-it notes, etc.) or electronic (email, hard disk, laptop, etc.);
- not responding to requests from persons claiming to be employees of payment service providers (bank advisers, anti-fraud staff, etc.), always using a secure and known channel to establish contact with a payment service provider, and never opening a link received by email or SMS with uncertain origin;

- never entrusting a payment instrument to a third party (relative, courier, etc.);
- remaining attentive to communications from a payment service provider and the security authorities.

It is important to remember that a payment service provider's staff will never ask for this information in a call with their customer and do not need it to cancel a fraudulent transaction.

Consumers are also invited to choose the most secure authentication solution offered by their payment service provider, provided they are able to use it. These are generally solutions based on a robust hardware element such as the banking application on a smartphone (the majority solution in France) or a standalone physical device provided by the payment service provider (card reader, USB key, etc.).

Reference: Article L. 133-16 du CMF (Code monétaire et financier, French Monetary and Financial Code).

2.5.2 Transparency in reporting cases of fraud

The fight against fraud, whatever the type of fraudulent transaction, requires all stakeholders, including victims of fraud, to cooperate and be as transparent as possible in describing the facts of the fraud. Providing comprehensive information is necessary on many levels:

- processing the application;
- identifying the perpetrators;
- initiating criminal proceedings against them;
- strengthening anti-fraud filtering mechanisms for payment providers;
- improving consumer warnings in a constructive manner, thereby helping to raise awareness among users of payment services.

There are usually several levels of recourse when disputing fraudulent transactions with PSPs:

- the initial dispute must be addressed to the account manager of the account-holding institution, who is the user's main point of contact, or, depending on the dispute procedure specifically provided for by the institution, on the customer area of the online banking service, for example;
- in the event of receiving an unsatisfactory response, the user may contact the complaints department of their payment service provider;⁵
- finally, they may refer the matter to the mediator appointed by their payment service provider.

In addition, customers may take legal action, if they consider it appropriate, at any time after their initial complaint has been rejected.

Recommendation 8:**Duty of transparency on the part of fraud victims**

When reporting fraud to their payment service provider or to law enforcement agencies (whether online via the Perceval or Thésée platforms¹ or when filing a complaint at a police station or *gendarmerie* unit), consumers and their representatives must provide all the information they have about the fraud they have suffered.

In particular, users must provide all the information they have on:

- the nature and context of the transaction: for example, their relationship, if any, with the beneficiary, the technical or manipulative procedures that the fraudster used, the instrument and terminals employed in the transaction, the messages or calls received, the actions carried out as a result of manipulation by the fraudster, etc.;
- the actions taken once the fraud was discovered: for example, freezing the instrument, reporting or lodging a complaint with the police, etc.

¹ Perceval is the teleservice available for reporting online bank card fraud to the police. Thésée allows users to lodge a complaint online against scams or frauds on the internet, particularly in the case of transfer fraud.

⁵ If the user lodges a complaint about the final decision of their payment service provider following a dispute, then Recommendation 2022-R01 of 9 May 2022 of the ACPR (*Autorité de contrôle prudentiel et de résolution*,

French Prudential Supervision and Resolution Authority) on the handling of complaints is fully applicable, supplementing these recommendations. See <https://acpr.banque.france.fr/>

2.6 Recommendations to prevent fraud

2.6.1 Consulting the customer's accounts using online banking or the mobile application

One of the fraud scenarios being explored involves the fraudster phishing for a customer's online banking login and password, as well as their personal details (first and last name, telephone number, etc.).

With this information, the fraudster connects to the customer's online banking service to gather information on the products held by the customer and the status of the accounts (balance, last transactions carried out, etc.). The fraudster can then contact the customer by impersonating the payment service provider, the impersonation made credible by providing precise banking information about the customer that a third party is not supposed to know. Once the fraudster has gained the trust of the victim, they will request the victim to validate a transaction (adding a beneficiary, transfer orders, etc.) using strong authentication.

This scenario can be avoided by implementing strong authentication every time the user consults the online bank, unless the consultation is made from a terminal regularly used by the user and the last connection with strong authentication was made less than 180 days ago.

Recommendation 9:

Applying strong authentication when accessing online banking from a new internet access point or terminal

Payment service providers are invited to require strong authentication when online banking or mobile application accounts are accessed from a terminal or internet access point not previously used by the customer.

2.6.2 Information given to customers when adding a transfer beneficiary

Current payment security regulations do not provide for systematic checks on the name of the beneficiary of a transfer: currently, a transfer order can be executed as long as the beneficiary IBAN⁶ is valid and the beneficiary account exists and has not been closed, regardless of whether the name of the beneficiary provided by the payer matches the name of the actual account holder.

This situation is exploited by certain fraudsters, particularly in the so-called "IBAN substitution" scenario: the fraudster provides the IBAN of an account of which they are the

Recommendation 10:

Procedures for registering credit transfer beneficiary IBANs

Payment service providers are asked to clearly indicate, each time a beneficiary is added to a transfer, whether a concordance check between IBAN and beneficiary name has been implemented. If this is not the case, the user must be informed that the "beneficiary name" field is intended solely to facilitate the monitoring of transactions by the customer issuing the transfers, and that its content is not used to check whether it matches the identity of the holder of the beneficiary IBAN.

In addition, payment service providers established in France are encouraged to explore the possibility of implementing a beneficiary confirmation service as soon as possible, as envisaged by the European Commission in its proposal to revise the SEPA Regulation.

holder (or whose holder is complicit in the fraud) by associating it with the name of a beneficiary trusted by the victim (for example, the Treasury or a notary).

Because when adding a beneficiary account, the sender of the transfer is asked to enter the name of the beneficiary, and because some banks even claim to have an "IBAN validation" stage, which can take up to several days, the sender of the transfer may wrongly assume that there is a reconciliation check, and that the transfer will be cancelled if the true holder of the beneficiary account does not match the name entered when adding the IBAN for that account.

However, this situation should change over the next few years. In its proposal to revise the Single Euro Payments Area (SEPA) Regulation,⁷ the European Commission is planning to strengthen confidence in instant payments by requiring service providers to check that the IBAN and the name of the beneficiary provided by the payer match, in order to alert the payer to any errors or fraud risks before the payment is made.

2.6.3 Information and options presented to the payment service user at the time of strong authentication

In the case of fraud by manipulation, a fraudster uses their control over their victim to get them to ignore all the messages and alerts sent by the payment service provider. This manipulation is made easier when the messages and alerts are insufficiently precise regarding the nature and characteristics of the transaction to be validated. Reinforcing the precision and exhaustiveness of the information presented, as well as the choices given to the user during the authentication process, can therefore be effective measures in preventing fraud by manipulation.

Recommendation 11:**Information and options presented to the user at the time of strong authentication**

Payment service providers must ensure that, at each stage of the authentication process, the user is presented with explicit information as to the nature of the transaction. In particular, the user must be informed of (i) the amount, (ii) the beneficiary, (iii) whether the transaction is a one-off or a recurring transaction, (iv) the frequency of recurring transactions, and (v) the irrevocable nature of the validation of the payment order. Moreover, if the identity of the beneficiary and the IBAN provided have not been checked against each other for a given transaction, the authentication procedure should explicitly remind the user of this.

Payment service providers must also ensure that the authentication process explicitly offers an option to cancel the transaction.

to collect payment data without the user's knowledge. These techniques are varied: through emails (phishing) or SMS messages (smishing), misappropriating the identity of a legitimate sender, posting fake mirror sites, or displaying, during a malicious incoming call, of the telephone number of a legitimate caller (misappropriation).

Recommendation 13:**The role of service providers and information technologies**

Players in the information technology sector (telephony operators, content hosts, publishers of referencing sites, search engines, messaging service providers, etc.) should strive to protect users against the risks of identity theft and attacks on the integrity and confidentiality of their data, working to prevent the use of fraudulent techniques such as phishing, misappropriation and SIM-swapping.

2.6.4 Easy access to options for freezing payment instruments

If users detect abnormal activity on their accounts or payment instruments, or identify a breach in the protection of their data, they must be able to freeze the payment instruments concerned. This procedure must be easy to access to ensure the best possible responsiveness, in the same way as the current payment cancellation centre for payment cards.

Recommendation 12:**Easy access to options for freezing payment instruments**

Payment service providers should provide users with mechanisms to freeze each of their payment instruments and should ensure that they are easily accessible, free of charge and can be used at any time.

References: Articles L. 133-15 and L. 133-17 of the CMF (Code monétaire et financier, French Monetary and Financial Code).

2.6.5 The role of service providers and information technology in the fight against fraud

Telephone operators and digital service providers are key stakeholders in the security of remote payment transactions, for which they provide the link between the various parties and the exchange of data. They therefore have a responsibility to combat the techniques used by fraudsters

2.7 Conditions in the implementation of the recommendations

The Observatory's 13 recommendations, specifying the expectations of the French authorities with regard to the implementation of European regulations, constitute best practices for players in the payments market. They are not intended to replace the applicable regulations or case law in this area.

Payment service providers undertake to take account of Recommendations 1 to 6 in their practices for handling complaints about unauthorised payment transactions. For their part, all stakeholders undertake to play a proactive role in payment security by ensuring that they apply Recommendations 7 to 13 in their day-to-day.

In a context where fraud methods develop and change at a fast pace, the Observatory undertakes to review these recommendations and, if necessary, revise them within 18 months of their publication.

6 IBAN – international bank account number.

7 Proposal of 26 October 2022 – 2022/0341 (COD) – to make instant

payments in euro available to all individuals and businesses with a bank account in the European Union or in a country of the European Economic Area (EEA).

3

SMARTPHONE OR TABLET PAYMENT ACCEPTANCE SOLUTIONS

**Chapter 3 is available in French only in the original version of the report,
which can be found here:**

https://www.banque-france.fr/system/files/2023-09/rapport_annuel_de_lobservatoire_de_la_securite_des_moyens_de_paiement_2022.pdf

4

ACTIONS CONDUCTED BY THE OBSERVATORY IN 2022

This chapter reviews the actions and recommendations of the Observatory in the areas of strong customer authentication of card payments (4.1), payments by cheque (4.2) and technology monitoring (4.3).

4.1 Strong customer authentication of card payments

The deployment of strong customer authentication for internet payments, introduced by the second European Payment Services Directive (PSD 2), has been completed in France since 2021, as pointed out by the Observatory in its annual report last year. In addition to monitoring the positive effects of strong customer authentication in terms of fraud reduction (see Chapter 1), the Observatory remained committed in 2022 to ensuring that the security of internet payments remains sustainable. To this end, it provided clarifications on the application of exemptions and collaborated with the telecommunications sector, particularly with telephone operators, to identify additional ways of making authentication methods more secure.

4.1.1 Overview of cardholder devices with strong customer authentication solutions

Most cardholders were equipped with strong customer authentication between 2019 and 2021. At the end of 2022, the Observatory notes that strong customer authentication solutions are only marginally evolving:

- **Secure mobile applications** are still the primary strong customer authentication solution in France: 73% of cardholders are equipped with it (compared with 68% in 2021), but this type of solution is used in 81% of authenticated payments. A secure mobile application

is a solution that enables cardholders to authenticate themselves using a PIN or a biometric factor, via the banking application installed on their mobile phone.

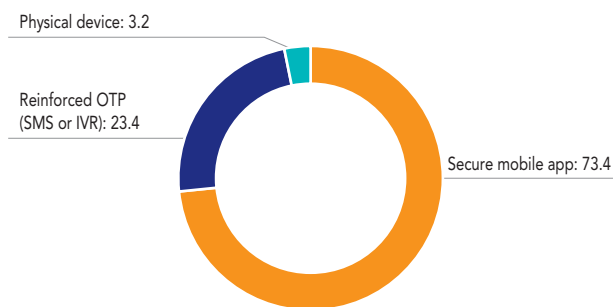
- **Reinforced OTP** combines a one-time password (OTP), received by SMS or voice message (IVS – interactive voice server), with a static password known by the cardholder. The proportion of cardholders equipped with this device had fallen by five points to 23% by the end of 2022.
- **Physical device**: made available to the cardholder by their payment service provider, it may be a code generator with an input keyboard, USB key or QR code reader. This device is specifically aimed at customers who consistently make their online purchases from their home computer. Only 3% of cardholders were equipped with them at the end of 2022, a percentage unchanged from 2021.

While all these solutions meet the regulatory requirements as compliant strong customer authentication solutions, the secure mobile application and the physical device are considered to be safer, as they rely on a physical device that cannot be remotely accessed by a fraudster. The secure mobile application is also seen as the most ergonomic and easy-to-use solution for customers. These two reasons combined explain why the secure mobile application is gaining ground among cardholders to the detriment of the reinforced OTP.

However, the Observatory points out that users must have the freedom to choose their authentication solution. Payment service providers are therefore invited to offer at least one free alternative method to the secure mobile application.

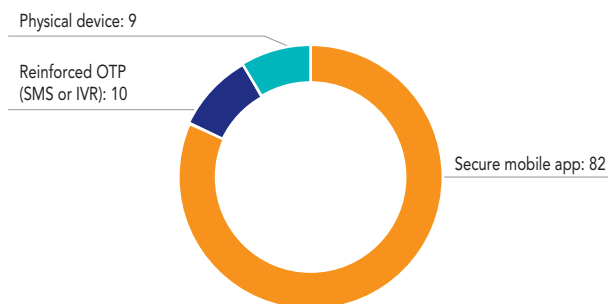
This overview does not cover strong customer authentication solutions delegated to a third party, such as mobile wallets or

C1 Distribution across cardholder's devices (in %)



Source: Observatory for the Security of Payment Means.
Note: OTP – one-time password; IVR – interactive voice response.

C2 Distribution in the use of strong customer authentication solutions among strongly authenticated payments (in %)



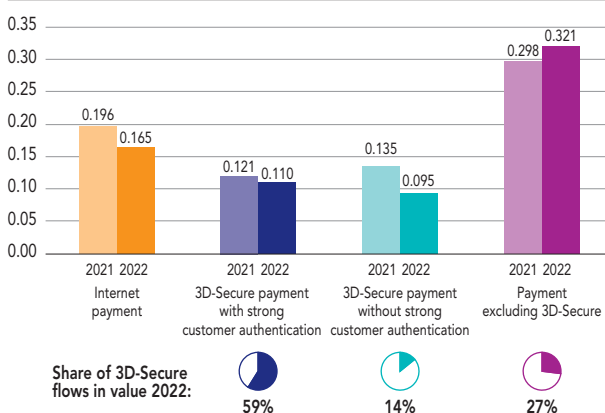
Source: Observatory for the Security of Payment Means.
Note: OTP – one-time password; IVR – interactive voice response.

e-wallets. In these cases, as the European Banking Authority (EBA) points out,¹ if the strong customer authentication is technically implemented by a third-party supplier, the issuer remains responsible for the regulatory compliance of the solution. The provision of services between the issuer and the solution provider must comply with the European Banking Authority's Guidelines on outsourcing arrangements of 25 February 2019 (EBA/GL/2019/02). In addition, the card enrolment operation in the mobile wallet must be subject to prior and systematic strong customer authentication under the direct responsibility of the issuer (EBA Q&A 5622).

4.1.2 Card payment fraud follow-up

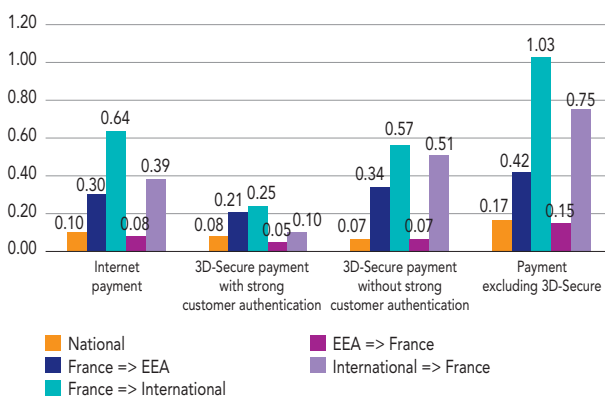
The strong customer authentication exemption provided for by PSD 2 for internet card transactions² considered more secure (based on their reduced amounts, risk, etc.), proves to be generally effective. The fraud rate of 3D-Secure payments exempt from strong customer authentication (0.095%) is very close to that of 3D-Secure payments with strong customer authentication (0.110%). By contrast, payments excluding 3D-Secure, which still represent 27% of card transactions on the internet in value, have a three times higher fraud rate of 0.321%, up from 2021.

C3 Internet transaction fraud rate for payments by card issued in France (in %)



Source: Observatory for the Security of Payment Means.

C4 Internet card payment fraud rate by authentication channel and geographic region in 2022 (in %)



Source: Observatory for the Security of Payment Means.
Note: EEA – European Economic Area.

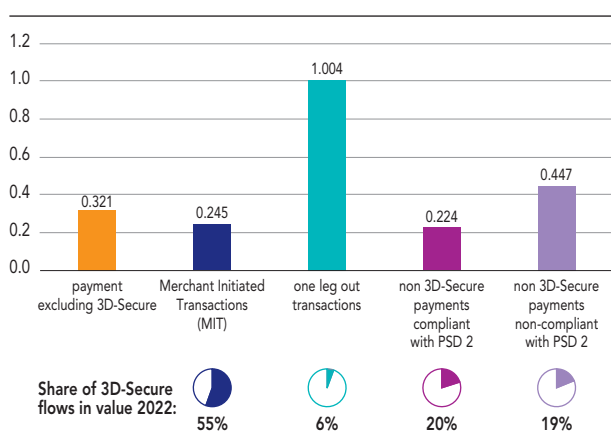
These general observations can be broken down by geographical area:

- At the national level, transactions using the 3D-Secure protocol are proportionally two times less defrauded than those not using it. Among 3D-Secure transactions, the fraud rate is particularly low for 3D-Secure transactions without strong customer authentication (0.07%), indicating a very successful application of exemptions at the domestic level.
- The application of exemptions is also successful at the level of the European Economic Area (EEA), for payments with cards issued in the EEA and accepted by French merchants (with a 0.07% fraud rate for exempted payments in 3D-Secure, compared to 0.05% for strongly customer authenticated payments). However, payments made by French cardholders to European merchants show

significantly higher rates of fraud. In particular, 3D-Secure payments without strong customer authentication remain more risky than those with strong customer authentication (0.34% compared with 0.21%). These figures reveal a less judicious use of exemptions or a less effective 3D-Secure infrastructure against fraud at the European level.

- At the international level, the PSD 2 strong customer authentication rules only apply on a voluntary basis and are subject to the counterparty's ability to support them. Internet payments accepted by French merchants therefore remain more secure than payments made by French cardholders to merchants established outside the EEA (0.39% compared with 0.64% fraud rates, respectively).

C5 Internet card payment fraud rate excluding 3D-Secure (in %)



Source: Observatory for the Security of Payment Means.

Note: Merchant Initiated Transactions (MIT) are transactions issued by the merchant without a user actively log in; one leg out transactions are transactions not subject to the strong customer authentication requirement, because they are carried out with a merchant or cardholder located outside the European Economic Area; PSD 2, second European Directive on payment services.

In 2022, non 3D-Secure (3DS) payments represent 27% of the amounts exchanged, yet represent 53% of the fraud affecting card payments on the internet. Because of their higher risk profile, the Observatory collected more detailed data on non 3D-Secure payments for the first time in 2022, drawing the following lessons:

- **Payments initiated by merchants** (MIT – Merchant Initiated Transactions), which account for most of the payment non 3DS flows (55%), have a fraud rate almost twice as high as payments initiated by the cardholder (CIT – Customer Initiated Transactions). The Observatory recalls that, under European regulations, MIT transactions must be linked to evidence of the cardholder's initial strong customer authentication. This must be requested at the time the cardholder consents to subsequent transactions (for example: subscription, purchase with deferred dispatch, payment associated with a reservation, etc.).
- **Payments that do not comply with PSD 2**, i.e. authorised without strong customer authentication even though there are no grounds for exemption, account for a significant proportion of these transactions (19% in terms of value). The Observatory will therefore pay particular attention in 2023 to the extinction of this category, given its elevated rate of fraud (0.447%).
- **Payments that are non 3DS, but are PSD 2-compliant** because they are authorised on the basis of an exemption accepted by the issuer, have a fraud rate twice as high as 3DS payments exempt from strong customer authentication (0.224% compared with 0.095% respectively). The Observatory will seek to understand this difference in performance for transactions that a priori present the same experience for the consumer.
- Finally, **so called "one leg out" payments** made to merchants established outside the European Economic Area, which are therefore not subject to PSD 2 rules, suffer from an elevated fraud rate (1.004%). However, very few of these operations do not use 3D-Secure.

4.1.3 Reminder of the principles applicable to strong customer authentication exemptions

The second European Directive on payment services (PSD 2)³ establishes strong customer authentication of the payer as a general rule to initiate an electronic payment. However, certain special cases are granted exemptions in the regulatory technical standards (hereinafter, referred to as "RTS") relating to strong customer authentication and account access interfaces.⁴

Exemptions come with strictly defined conditions of application, excluding the exemption referred to in Article 18 of the RTS concerning low-risk transactions (commonly known by the acronym "TRA" for transaction risk analysis). For this exemption, the eligibility of the transaction is based almost entirely on the payment service providers ("PSPs") judgement, which is therefore likely to lead to distortions in its application.

1 European Banking Authority, press release, 31 January 2023: "EBA clarifies the application of strong customer authentication requirements to digital wallets".

2 Internet card transactions cover any electronic payment made over the internet (merchant site or via a mobile application). Payments initiated by post, email, fax or telephone are therefore excluded, as they are classified in the separate category of "non-internet remote payments".

3 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

4 Delegated Regulation (EU) 2018/389 of the European Commission of 27 November 2017 complementing Directive (EU) 2015/2366 of the European Parliament and of the Council providing regulatory technical standards for strong customer authentication and common secure open standards for communication.

To provide greater clarity for all stakeholders (payment service providers, technical service providers, card payment systems, merchants and consumers), the Observatory has endeavoured to formalise the principles applicable to exemptions. Particular attention is paid to the TRA exemption, especially in light of the regulatory texts and in the clarifications provided by the European Banking Authority in its opinions⁵ and regulatory interpretation responses (Q&As)⁶.

General principles applicable to all exemptions from strong customer authentication

Non-mandatory nature and availability of the exemption

Although the exemptions are not mandatory, payment service providers (PSPs) are invited to implement them if they have the technical capacity to do so and if the conditions of application defined in the RTS are met.

Responsibilities of the payer's payment service provider regarding security

The payer's PSP, which is responsible under the PSD 2 for ensuring the security of payments initiated by its users, retains the right in all circumstances to require strong customer authentication if this is justified by the transaction assessment risk, even if the transaction meets the eligibility criteria for an exemption (EBA Q&A 4034 and 4480).

Equal treatment between payment service providers

At an assessed equivalent risk level, the payer's PSP ensures a fair response to exemption requests regardless of the identity of the payee's PSP. In particular, it ensures that other acquiring PSPs have access to the same exemptions granted to transactions for which it is the beneficiary PSP itself.

Specific principles applicable to the TRA exemption

Compliance with the reference fraud rate by the PSP requesting the exemption

The RTS provide that a PSP can only use the TRA exemption if the following two conditions are met:

- it has deployed a real-time transaction control mechanism, integrating the analysis factors specified in the regulations into a risk rating assigned to each individual transaction (Article 18 of the RTS, *EBA Q&A 4127*),
- and its fraud rate for the type of transaction concerned is sufficiently controlled. The reference fraud rates for accessing the TRA exemption are defined in the appendix to the RTS (*see table below*).

T1 Benchmark fraud rates set by the RTS

| PSP fraud rate | | Maximum unit amount of transactions eligible for TRA |
|-----------------------|-------------------|--|
| Internet card payment | Internet transfer | |
| ≤ 0.01% | ≤ 0.005% | 500 € |
| ≤ 0.06% | ≤ 0.010% | 250 € |
| ≤ 0.13% | ≤ 0.015% | 100 € |
| > 0.13% | > 0.015% | Not eligible |

Source: Delegated Regulation (EU) 2018/2389 of the European Commission of 27 November 2017 complementing Directive (EU) 2015/2366 of the European Parliament and of the Council providing regulatory technical standards for strong customer authentication and common secure open standards for communication.
Note: RTS – regulatory technical standards; TRA – transaction risk analysis (low risk transaction); PSP – payment service provider.

These fraud rates are calculated:

- at the level of the PSP as an authorised legal entity (EBA Q&A 4439),
- for each calendar quarter (Articles 19 and 20 of the RTS, EBA Q&A 4045),
- in accordance with the EBA's methodological guidelines on fraud (EBA/GL/2018/05), now included in the Banque de France's half-yearly statistical data collection on cashless payment fraud,
- and integrate all remote electronic payments linked to a card, with a global approach and not by range (EBA Q&A 4043 and 4702).

As a result, the fraud rate must be calculated globally in terms of value over the scope of application of the PSD 2. These are payments issued electronically on the initiative of the payer and for which both the PSP of the payer and the payee are located within the European Economic Area, all initiation channels, card payment systems and EEA countries combined. This calculation therefore excludes transactions (i) issued non-electronically (paper orders, faxes, etc.) or (ii) issued by the beneficiary (MIT transactions, etc.), as well as (iii) those where the counterparty is located outside the EEA (one leg out transactions).

According to the Observatory's statistics collected from card payment systems in 2022, the average fraud rate for card payments on the internet within the scope defined above was:

- 0.12% for payments by card issued in France,
- 0.09% for payments by card accepted in France.

These averages indicate that not all issuing or acquiring PSPs are currently eligible for the TRA exemption, as many will have fraud rates over the limits set by the

exemption. According to PSPs, the probability of being able to use the TRA exemption is low for transactions between EUR 100 and EUR 250, given a maximum fraud rate set by regulations of 0.06%, and very low for transactions between EUR 250 and EUR 500, given a maximum fraud rate of 0.01% set by regulations.

Fraud rates to be taken into account for card payments on the internet

In the case of card transactions over the internet, the TRA exemption may be requested either by the issuing PSP (referred to as issuer TRA) or by the acquiring PSP (acquirer TRA). Only the reference fraud rate of the PSP applying for the TRA exemption should be taken into account (EBA Q&A 4034):

- in the event of an acquirer TRA request, the issuing PSP has the option of validating the exemption even if its own fraud rate does not allow it to request an issuer TRA for the same transaction;
- in the event that the acquiring PSP's fraud rate does not allow it to request a TRA exemption, it retains the option of providing the issuing PSP with evidences of a low level of risk with a view to inviting such PSP to consider, in an informed manner, the possibility of using an issuer TRA exemption;
- checking the fraud rate against the reference rates is the sole responsibility of the PSP applying for the exemption.

Liability in case of fraud

In the event of fraud on a transaction that has benefited from a TRA exemption, the regulations stipulate that the financial responsibility is borne by the PSP that initiated the TRA request.⁷ In the event of fraud on a transaction associated:

- to a TRA (issuer or acquirer), the issuing PSP must immediately refund the unauthorised transactions in full to the holder of the means of payment;
- in addition, in the case of an acquiring TRA, the acquiring PSP is obliged to reimburse the financial loss to the issuing PSP.

Calculation of the fraud rates for card payments

The Observatory invites PSPs providing issuing and acquiring services to calculate separate fraud rates for these two activities, and to consider only the fraud rate relating to their respective role in a given transaction, i.e.:

- a fraud rate as issuing PSP to allow an issuing TRA exemption,
- a fraud rate as an acquiring PSP to apply for an acquiring PSP exemption.

Suspension of the right to use the TRA exemption and notification to the Banque de France

In accordance with Article 20 of the RTS, PSPs must immediately inform the Banque de France if:

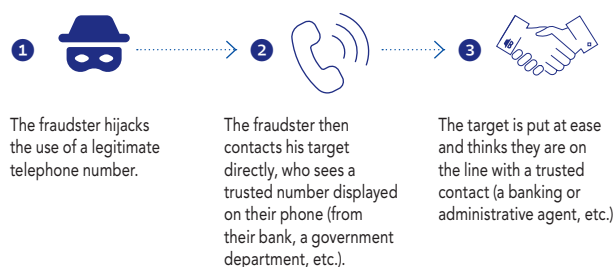
- their fraud rate, calculated for the purposes of the TRA, exceeds one of the reference rates set by the regulations, thus limiting their ability to use the TRA exemption;
- on the contrary, their fraud rate has once again become consistent with one of the reference rates, freeing up their ability to use the TRA exemption.

In accordance with the Banque de France letter of 19 December 2019, distributed to all PSPs through the *Comité français d'organisation et de normalisation bancaires* (CFONB – French Committee for Banking Organisation and Standardisation, Communication no. 20200002 of 8 January 2020), these two notifications are to be declared by the PSPs, in free format, by email to 2323-notifications-UT@banque-france.fr.

4.1.4 Work with telephone operators

With the dematerialisation of banking procedures, more and more exchanges between customers and their bank are taking place remotely. Despite the security measures implemented by banks to reduce online payment fraud, fraudsters are exploiting several vulnerabilities in the telecoms industry to establish new fraud scenarios. In light of this, the Observatory asked in 2022 the telecommunications sector to identify effective countermeasures.

Telephone number spoofing



Source: Observatory for the Security of Payment Means.

⁵ In particular, the following opinion of the EBA of June 2018: "EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04)".

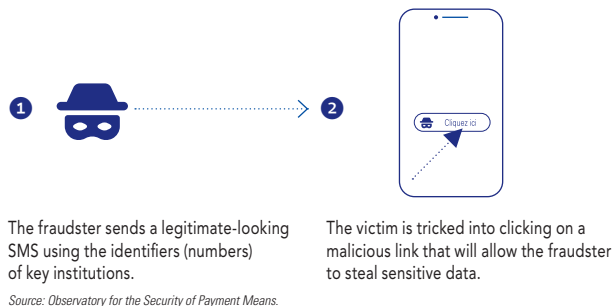
⁶ The EBA's Q&A can be accessed through its Single

Rulebook: <http://www.eba.europa.eu/single-rule-book-qa>

⁷ References: Articles 73 and 74 of the PSD 2, complemented by EBA Q&A 4042.

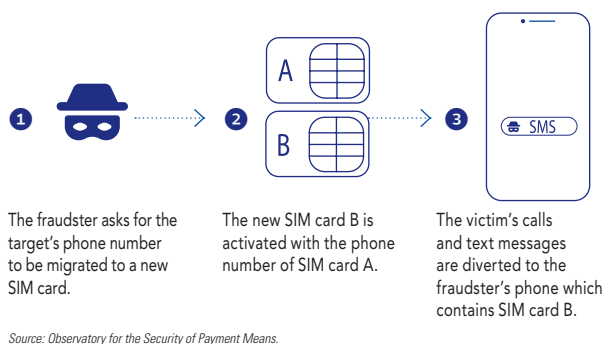
The so-called “Naegelen” law,⁸ passed in 2020, aims to make such practices impossible from its entry into force in July 2023. The telecoms industry is in the process of deploying a new infrastructure to ensure greater confidence in the numbers presented when making calls.

The theft of banking or other sensitive personal identification information in SMS numbers (smishing).



In October 2022, the French Mobile Multimedia Association (AF2M), which brings together the main telephone operators, launched a pilot action plan to protect the use of the phone numbers identifying sensitive institutions, coupled with the promotion of the 33700 short number to encourage consumers to report fraudulent SMS messages received.

Fraudulent SIM card swapping



One of the authentication solutions most commonly used by payment service providers is based on the use of the customer's mobile phone line to send them a one-time code (OTP) by text message. This is recognised as a possession factor of the telephone line and is used both to authenticate transactions and to secure sensitive operations (access to online banking, adding a trusted beneficiary, adding a card to a mobile wallet, etc.).

Unfortunately, the Observatory notes the persistence of fraudulent practices such as SIM swapping, used to divert calls and text messages from the legitimate cardholder to a fraudster. This phenomenon has taken on a new significance

in recent years with the development of digital SIM cards (or eSIMs), which enable several lines to be installed on the same phone, or the same telephone line to be used on several terminals (for example, on a multifunction mobile phone and a connected watch at the same time).

One corrective measure is the provision of an interoperator application programming interface (API), allowing users to obtain information about a SIM card associated with a given telephone number. This system, known as “SIM Verify”, is currently being tested by a number of operators to enhance strength of authentication solutions using SMS codes, although there is a charge for consulting the API.

Another corrective measure recommended by the Observatory is to make the procedures for issuing SIM cards by telephone operators more secure. These procedures should systematically use multi-factor authentication. As recommended by the Observatory in its 2021 annual report,⁹ telephone operators may use substantial or high-level electronic means of identification, or digital identity solutions providing an equivalent level of security, to secure SIM card changes and eSIM requests.

4.1.5 Outlook for 2023

The successful migration to the PSD 2 directive, with a significant drop in the fraud level involving card payments over the internet, is an illustration of the successful cooperation among the market actors. The Observatory is committed to this ongoing dialogue and collaboration, involving all the actors required in the fight against fraud, both financial players and merchants. It will continue to strengthen this dialogue and monitor the correct application of PSD 2 rules and the harmonisation of practices in the French market and at the European level. In 2023, the Observatory's “strong customer authentication” working group will continue to work on the following three areas:

- stepping up dialogue and cooperation with the telecommunications sector, including with the *Autorité de régulation des communications électroniques, des postes et de la distribution de la presse* (ARCEP – French Electronic Communications, Postal and Print media distribution Regulatory Authority), to help improve the security of telephonic operations and procedures;
- actively contributing to European regulatory work to ensure the harmonisation of rules and practices for strong customer authentication of payments, particularly with a view to the revision of PSD 2, with a focus on the rules applicable to the implementation of exemptions to strong customer authentication and tokenised cards;

- monitoring internet payment fraud rates by conducting comparative analyses with other European countries, based on the publication of the initial payment fraud indicators by European authorities.

4.2 Following up of Observatory's actions and recommendations against cheque fraud

This part is available in French only.

4.3 Reminder of the Observatory's primary recommendations on technology monitoring topics

As part of its annual monitoring work, the Observatory makes recommendations to market actors and users. The main recommendations issued in recent years are summarised in this section.

4.3.1 Recommendations relating to digital identity and payment security

The annual report for 2021 includes recommendations on digital identity and payment security. Identity theft, sometimes combined with document fraud techniques, can undermine the general security of payment methods.

More specifically, the Observatory identifies and distinguishes between three types of fraud: (i) identity theft at the time of entering into a contractual relationship, (ii) theft of the identity of the payer at the time of making a purchase and (iii) theft of the identity of the beneficiary of a payment. Some fraud schemes are still based on the impersonation of legal entities. However, the risks of identity theft primarily concern the identity of natural persons.

Digital identity solutions and secure trust services seeking to combat the risks of identity theft in the digital sphere, such as electronic signatures and stamps, can help improve the overall security of payment methods. With the publication in 2021 of the repository of requirements for remote identity verification (PVID) providers, and the ongoing revision of the European eIDAS regulation on electronic identification and trust services,¹⁰ the Observatory invites payment stakeholders to combat identity theft by using digital identity services that comply with PVID or eIDAS requirements.

⁸ Law 2020-901 of 24 July 2020 aimed at regulating telephone canvassing and combating fraudulent calls.

⁹ See Chapter 3, "Digital identity and payment security".

¹⁰ Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS – electronic Identification, Authentication and Trust Services).

T3 Observatory recommendations on digital identity and payment security

| Recommendations | Recipients |
|---|-------------------------------|
| Use, within the framework of the rules applicable to the fight against money laundering and terrorist financing (AML/CFT), substantial or high-level electronic means of identification within the meaning of Regulation (EU) 910/2014, qualified trust services and, more generally, services that comply with the requirements of the reference framework drawn up by the <i>Agence nationale de la sécurité des systèmes d'information</i> (Anssi) applicable to remote identity verification service providers. | Payment service providers |
| Use substantial electronic means of identification or digital identity solutions providing an equivalent level of security to authenticate their users for access to customer areas or for certain operations such as SIM card issuance with telephone operators. | Suppliers and traders |
| Use substantial or high-level electronic means of identification and recognised trust services within the meaning of eIDAS, such as advanced or qualified electronic signatures, to authenticate their users or counterparties more strongly at the time of certain sensitive transactions (communication or receipt of new bank details, signature of a direct debit mandate). | Administrations and companies |
| Use, where possible, secure digital identity solutions, for example those certified to a substantial or high level, to secure online uses with public authorities and companies and limit the risks of disclosure of personal identity and banking data. | Users |

Source: Observatory for the Security of Payment Means.

4.3.2 Recommendations relating to the security of real-time payments

The recommendations relating to the security of real-time payments were published in the 2020 annual report.

With the rapid development of instant transfers, which could gradually replace traditional transfers and even other means of payment, the Observatory remains particularly attentive to the security of real-time payments. In 2022, instant transfers represented 3.8% of the total number of transfers and 0.3% of the amounts exchanged by transfer (excluding large-value transfers processed by large-value payment systems). The number of instant transfers has risen by a further 84% since 2021. The increase is expected to continue over the next few years, supported by national and European payment strategies and legislative initiatives by European public authorities. In terms of security, the Observatory notes that fraud on real-time payments is increasing at a slower rate than flows, with the result that the fraud rate on instant transfers has remained relatively stable since 2020, at around 0.044%. With EUR 52 million in fraud involving instant

transfers in 2022, i.e. almost 17% of total recorded fraud involving transfers, the Observatory is renewing its call to the payments industry to continue its efforts and investment to enhance the security of instant transfers. The Observatory also reiterates its recommendations aimed at ensuring the rapid and secure development of this new payment method.

4.3.3 Payment data security recommendations

The recommendations on payment data security were published in the 2019 annual report.

The development of digital uses incorporating payment data – whether integrated into mobile applications, IoT devices, or personalised budgeting advice services – has resulted in the dissemination of this data, which is now shared with various players (banks, merchants, Fintech, etc.) in different environments.

In this context, the implementation of PSD 2 has strengthened the security of so-called “open banking” practices. Supervised third parties can access users’ payment accounts to provide

T4 Observatory recommendations on the security of real-time payments

| Recommendations | Recipients |
|--|---|
| Implement, under the conditions set out in PSD 2, strong user authentication for authorising payments in real time and for all sensitive peripheral transactions (adding a beneficiary, changing contact details, etc.). | Payment service providers (issuers) |
| Continuously improve fraud prevention tools in real time, in particular using machine learning-based technologies, to improve the performance of the risk analysis systems deployed. | Payment service providers (issuers and acquirers) |
| Where necessary, make use of rights management measures, such as caps and limitations, to limit the damage caused by the uncontrolled development of fraud. | Payment service providers (issuers) |
| Identify atypical incoming operations, especially when these precede other outgoing operations. | Payment service providers (acquirers) |
| Before validating a payment order, pay particular attention to the origin of the request and the identity of the contact person, and check the beneficiary's bank details. | Users |
| Enter banking data exclusively on reputable and trusted websites or mobile applications; favour referenced sites and applications and connect to them directly, considering with the greatest caution the links received by insecure means of communication, such as SMS and emails. | Users |
| Notify your bank of any suspicious unauthorised or fraudulent transaction as soon as possible after said transaction has taken place. | Users |
| Support user vigilance by providing tools for confirming beneficiaries, while actively informing them in real time of transactions carried out on their account. | Payment service providers |

Source: Observatory for the Security of Payment Means.

T5 Observatory recommendations on payment data security

| Recommendations | Recipients |
|---|---------------------------|
| Use strong user authentication for access to payment services and all sensitive data under the conditions set out in PSD 2 (in particular every 90 days for account consultation). | Payment service providers |
| Set up systems for detecting suspicious connections. | Payment service providers |
| Keep secret all elements used to make payments; in the case of payment cards, this care must not be limited to the confidential code alone, but to all the data present on the card that allows payments on the internet (card number, name of the holder, expiry date and cryptogram); in addition, the confidential code must never be communicated to a third party or stored on a digital medium. | Users |
| Enter banking data exclusively on reputable and trusted websites or mobile applications; favour referenced sites and applications and connect to them directly, considering with the greatest caution the links received by insecure means of communication, such as SMS and emails. | Users |
| In the specific case of access to payment services, use only trusted applications, in particular those published by their payment service provider or whose provider is duly authorised in France to provide payment services (i.e. listed in the Regafi directory or in the European Banking Authority register). | Users |
| Keep up to date with digital risks and developments, for example via the government website http://www.cybermalveillance.gouv.fr | Users |

Source: Observatory for the Security of Payment Means.

information aggregation or payment initiation services, through dedicated secure interfaces that do not require personal login information to be communicated. The level of security and performance offered by these interfaces and their ability to preserve data confidentiality will be decisive factors in the development of open banking services under optimum conditions of confidence and fluidity for the user.

The Observatory draws attention to the central role played by users in protecting their own payment data, urging them to develop the right habits, ensuring that this data is protected and only shared within trusted environments.

4.3.4 Recommendations relating to the security of mobile payments

The recommendations on mobile payments were published in the 2018 annual report.

Payments by card at the point of sale using a mobile solution have grown significantly over the last three years, boosted by the health crisis and the new option of contactless payment (up to a limit of EUR 50). The number of payments of this type has multiplied by just over 17.5 between 2019 and 2022, to represent, in 2022, 6% of the number of proximity card payments and 9% of contactless payments, compared with 0.5% respectively before the health crisis.

At the same time, the fraud rate in mobile contactless payments rose sharply in 2020, to 0.102%, and then was reduced to 0.064% by 2022, reflecting a strengthening of fraud risk management tools, particularly at the time of user enrolment in the solution, which the Observatory calls for to be continued. To avoid the risks of fraudsters using stolen card numbers in this type of solution, it is essential to implement strong customer authentication, as required by PSD 2 for sensitive transactions.

T6 Observatory recommendations on the security of mobile payments

| Recommendations | Recipients |
|--|---|
| Implement reliable mechanisms for the secure storage of confidential information in the mobile solution (sensitive payment data, identity data, authentication or biometric data). | Payment service providers and their technical service providers |
| Implement a strong customer authentication mechanism for users when they register their means of payment in the payment application. | Payment service providers |
| Provide users with corrective updates for mobile solutions whenever a security flaw is identified that could affect the integrity, confidentiality or availability of the system or data. | Operating system or application providers, manufacturers of smartphones |
| Give users sufficient visibility of the security measures built into their applications, while insisting on the need to deploy effective countermeasures to combat unauthorised use of these applications. | Payment service providers |
| Regularly assess the level of security of mobile payment solutions. | Payment service providers |
| Regularly update a mobile phone's operating system. | Users |
| Choose and regularly change confidential codes, passwords and any other personal data used for authentication procedures on a smartphone, at the very least for payment applications. | Users |
| Activate, if the operating system allows it, the remote data wiping option in case your mobile phone is lost or stolen. | Users |
| Use only trusted applications, including those recommended by payment service providers. | Users |
| Avoid making payment transactions on your mobile phone when the communication channel is unreliable (e.g. unsecured public wifi connection). | Users |

Source: Observatory for the Security of Payment Means.

APPENDICES

Appendix 1 is available in French only in the original version of the report, which can be found here:

https://www.banque-france.fr/system/files/2023-09/rapport_annuel_de_observatoire_de_la_securite_des_moyens_de_paielement_2022.pdf

Appendices 2, 3 and 4 are available in English in this report.

All tables in Appendix 5 can be downloaded in English at the following address:

https://www.banque-france.fr/system/files/2023-11/Dossier_statistique_2022_-_annexe_5_du_rapport_annuel_2022.xlsx

| | | |
|-----------|--|-----------|
| A1 | Precautionary advices for the use of means of payment | |
| A2 | Responsibilities and organisation of the Observatory | 52 |
| A3 | List of Observatory members by name | 54 |
| A4 | Methodology for measuring fraud involving cashless means of payment | 57 |
| A5 | Statistical file on payment card use and fraud | 67 |

A2

RESPONSIBILITIES AND ORGANISATION OF THE OBSERVATORY

The responsibilities, composition and operating procedures of the Observatory for the Security of Payment Means are set out in Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the French Monetary and Financial Code.

SCOPE

Under Article 65 of Law 2016-1691 of 9 December 2016 and according to the national strategy for means of payment, Article L. 141-4 of the French Monetary and Financial Code has been amended by extending the remit of the Observatory for Payment Card Security to all cashless means of payment. In addition to cards issued by payment service providers or similar institutions, the remit of the Observatory (now the Observatory for the Security of Payment Means) covers all other cashless means of payment.

According to Article L. 311-3 of the French Monetary and Financial Code, a means of payment is any instrument that enables a person to transfer funds, regardless of the medium or technical process used. The following are the payment methods covered by the Observatory:

- **Credit transfers** are made possible by a payment service provider holding the payer's payment account. The provider credits, after an instruction from the payer, the account of the indicated payee by means of a transaction or a series of payment transactions carried out from the payer's payment account.
- **Direct debits** are used to debit a payer's payment account when a payment transaction is initiated by the payee on the basis of consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.
- **Payment cards** are payment instruments that enable the holder to withdraw or transfer funds. There are different types of cards:
 - Debit cards are cards linked to a payment account enabling the cardholder to make payments or withdrawals that will be debited according to a timeframe set out in the contract for the card;
 - Credit cards are backed by a line of credit, with a rate and a limit negotiated with the customer, and can be used to make payments and/or cash withdrawals. They allow the holder to defer payment to the issuer for a certain period, while the payee is paid directly by the issuer, with no delay;
- Commercial cards, issued to companies, public bodies or self-employed individuals, are limited to business expenses, with payments made using this type of card billed directly to the account of the company, public body or self-employed individual.
- **Electronic money** is monetary value stored in electronic form, including magnetic form, representing a claim on the issuer, which is issued (by credit institutions or electronic money institutions) against the delivery of funds for payment transactions and which is accepted by a natural or legal person other than the electronic money issuer.
- **Cheques** are documents by which a person, the drawer, instructs a credit institution, the drawee, to pay a certain sum at sight to the drawer or to a third party, known as the payee.
- **Trade bills** are marketable securities that state that the bearer holds a claim for payment of a sum of money and serves for that payment. Trade bills include bills of exchange and promissory notes.
- **The remittance of funds** is a payment service where funds can be sent and received without creating a payment account in the name of the payer or payee. A remittance of funds has the sole purpose of transferring a corresponding amount to a payee or another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of the payee and made available to the payee.

RESPONSIBILITIES

According to Articles L. 141-4 and R. 141-1 of the French Monetary and Financial Code, the Observatory for the Security of Payment Means has three main responsibilities:

- To monitor the implementation of measures adopted by issuers, merchants and businesses to strengthen the security of means of payment;
- To compile statistics on fraud. Accordingly, issuers of means of payment send the information required to compile these statistics to the Observatory, following the recommendations given by the Observatory towards standardising the methods of calculating fraud on the various cashless payment methods;

- To monitor technological developments in non-cash means of payment, with the aim of proposing ways of combating breaches of security in means of payment. It therefore collects available information likely to enhance the security of means of payment and makes it available to its members, encouraging the exchange of information between its members, while respecting the confidentiality of certain information.

In addition, under the terms of Article R. 141-2 of the French Monetary and Financial Code, the French Minister for Economy and Finance may refer a matter to the Observatory for an opinion, setting a deadline for its response. These opinions may be made public by the minister.

COMPOSITION

Article R. 142-22 of the French Monetary and Financial Code sets out the composition of the Observatory. According to this text, the Observatory comprises:

- a member of the French Parliament and a French Senator;
- eight representatives of the French government;
- the Governor of the Banque de France or their representative;
- the Secretary General of the French Prudential Supervision and Resolution Authority;
- a representative of the French Data Protection Authority (*Commission nationale de l'informatique et des libertés*);
- fourteen representatives of issuers of payment instruments and operators of payment systems;
- five representatives from the consumer section of the *Conseil national de la consommation* (National Consumer Council);
- eight representatives of professional organisations of retailers and businesses in the retail, mass distribution, teleshopping and e-commerce sectors in particular;
- two people qualified by their expertise.

A list of the Observatory's members is given in Appendix 3.

The members of the Observatory, except the members of the French Parliament, those representing the government, the Governor of the Banque de France and the Secretary General of the French Prudential Supervision and Resolution Authority, are appointed for three years. Their mandate is renewable.

The Chairman is appointed from among these members by the French Minister for Economy and Finance. Their term of office is three years, renewable. François Villeroy de Galhau, Governor of the Banque de France, is the current chairman.

OPERATING PROCEDURES

According to Article R. 142-23 et seq. of the French Monetary and Financial Code, the Observatory is convened by its chairman at least twice a year. The sessions are not public. The measures proposed by the Observatory are adopted if an absolute majority is reached in a session. Each member has one vote; in the event of a tie, the chairman has the casting vote. The Observatory has adopted a set of internal rules setting out the conditions under which it operates.

The Observatory's administrative secretariat, provided by the Banque de France, is responsible for organising and monitoring meetings, centralising the information needed to compile statistics on fraud involving means of payment, and collecting and providing members with the information they need to monitor the security measures adopted and keep abreast of technological developments regarding means of payment. The secretariat also prepares the Observatory's annual report, which is submitted each year to the French Minister for Economy and Finance and sent to the French Parliament.

Working or study groups may be set up by the Observatory, in particular when the French Minister for Economy and Finance refers a matter to the Observatory for an opinion. The Observatory, acting with an absolute majority of its members, sets the terms of reference and composition of these working groups, which must report on their work at each meeting. Working or study groups may consult any person likely to be able to provide them with information useful for the accomplishment of their mandate.

Given the sensitivity of the data exchanged, the members of the Observatory and its secretariat are bound by professional secrecy under Article R. 142-25 of the French Monetary and Financial Code, and must therefore keep confidential any information brought to their attention in the course of their duties. To this end, the Observatory has included in its internal rules a requirement for members to express a commitment to the chairman that they will keep all working documents strictly confidential.

A3

LIST OF OBSERVATORY MEMBERS BY NAME

Pursuant to article R. 142-22 of the French Monetary and Financial Code, the members of the Observatory other than Members of Parliament, those representing the French government, the Governor of the Banque de France and the Secretary General of the French Prudential Supervision and Resolution Authority are appointed for three years by order of the French Minister for Economy and Finance. The last appointment order dates from 20 June 2023.

CHAIRMAN

François VILLEROY DE GALHAU

Governor of the Banque de France

MEMBERS OF PARLIAMENT

Éric BOCQUET

Senator

Michaël TAVERNE

Deputy

REPRESENTATIVE OF THE GENERAL SECRETARIAT OF THE FRENCH PRUDENTIAL SUPERVISION AND RESOLUTION AUTHORITY

- The Secretary General or their representative:
Nathalie AUFAUVRE
Grégoire VUARLOT

REPRESENTATIVES OF THE FRENCH GOVERNMENT

On the proposal of the General Secretariat
for Defence and National Security:

- The Director General of the National Cybersecurity Agency
of France or their representative:
Vivien MURA

On the proposal of the Minister of the Economy, Finance
and industrial and digital Sovereignty of France:

- The Senior Defence and Security Officer or their representative:
Samuel HEUZÉ

- The Director General of the Treasury or their representative:
Bastien LAFON

- The Chair of the *Institut d'émission des départements d'outre-mer* (IEDOM, Delegated central bank for the French overseas departments and territories) and
Director General of the *Institut d'émission d'outre-mer* (IEOM, the French overseas note-issuing bank):
Ivan ODONNAT

- The Director General for Competition, Consumer Affairs and
Fraud Prevention Directorate or their representative:
Marie-Hélène AUFFRET

On the proposal of the Minister for Justice:

- The Director of the Criminal Matters and Pardons Directorate
or their representative:
Étienne PERRIN
Léa OBADIA

On the proposal of the Minister of the Interior:

- The Deputy Director for the fight against financial crime at the
Central Directorate of the Judicial Police (DCPJ, *Direction
nationale de la police judiciaire*) or their representative:
Thomas DE RICOLFIS
Anne-Sophie COULBOIS

- The Director General of the national *Gendarmerie* or their representative:
Étienne LESTRELIN

On the proposal of the *Commission nationale de l'informatique et
des libertés* (National Commission on Informatics and Liberty):

- The head of the Economic Affairs department or
their representative:
Nacéra BEKHAT
Aymeric PONTVIANNE

REPRESENTATIVES OF ISSUERS OF PAYMENT INSTRUMENTS AND OPERATORS OF PAYMENT SYSTEMS

Thomas GOUSSEAU

Member of the Board of Directors

Association française des établissements de paiement et de monnaie électronique (Afepame, French Association of Payment and Electronic Money Institutions)

Amelia NEWSOM-DAVIS

Pay Services Director for Orange

Association française du Multimédia Mobile (AF2M, French Mobile Multimedia Association)

Corinne DENAEYER

Research Analyst

Association française des sociétés financières (ASF, French Association of Financial Companies)

Sébastien MARINOT

Director – Strategy and Market Relations, Cash Management
BNP Paribas (BNPP)

Mireille MERCIER

Director of Market Projects and Means of Payment

Office de coordination bancaire et financière (OCBF, Banking and Financial Coordination Office)

Caroline GAYE

General Director

American Express France (Amex)

Violette BOUVERET

Vice-Chairman, Cyber & Intelligence

MasterCard France

Philippe LAULANIE

Administrator

Groupement des cartes bancaires (GCB)

Jean-Paul ALBERT

Director of Electronic Payments

Société Générale

Évelyne BOTTOLLIER-CURTET

Card scheme relationships manager

Groupe BPCE

Romain BOISSON

Regional Director

Visa Europe France

Jérôme RAGUÉNÈS

Director of the Digital Department,

Payments and Operational Resilience

French Banking Federation (FBF)

Jean-Marie VALLÉE

General Director

STET

Marie-Anne LIVI

Director – Strategy and Market Relations

Crédit Agricole

COMPANY REPRESENTATIVES

Bernard COHEN-HADAD

Chairman of the *Commission financement des entreprises* (Business Financing Commission)

Confédération des petites et moyennes entreprises

(CPME, Confederation of Small and Medium Enterprises)

Émilie TISON

Confédération du commerce de gros et international

(Confederation of Wholesale and International Trade)

Mouvement des entreprises de France

(MEDEF, Movement of the Entreprises of France)

Isabelle CHARLIER

Chairman of the Commission monétique et moyens de paiement

(Electronic Payments and Means of Payment Commission)

Association française des trésoriers d'entreprise

(AFTE, French Association of Corporate Treasurers)

REPRESENTATIVES OF THE CONSUMER SECTION OF THE *CONSEIL NATIONAL DE LA CONSOMMATION* (NATIONAL CONSUMER COUNCIL);

Mélissa HOWARD

Lawyer

Association Léo Lagrange pour la défense des consommateurs
(ALLDC, Léo Lagrange Association for the Defense of Consumers)

Morgane LENAIN

Lawyer

Union nationale des associations familiales (Unaf)

Xavier KRUGER

Banking-insurance officer

UFC – Que choisir (association of consumers)

Hervé MONDANGE

Lawyer

Association Force ouvrière consommateurs
(Afoc, Force Ouvrière Consumer Association)

Bernard FILLIAT

Association pour l'information et la défense des consommateurs salariés CGT (INDECOSA-CGT, Association for Information and protection of CGT Consumers and employees)

REPRESENTATIVES OF PROFESSIONAL RETAILERS' ORGANISATIONS

Bertrand PINEAU

Executive Officer

Mercatel

Isabelle CLAIRAC

Managing Director of Market Pay

Fédération du commerce et de la distribution

(FCD, Trade and retail Federation)

Philippe JOGUET

Correspondent on financial matters

Conseil du commerce de France (CdCF, French Trade Council)

Marc LOLIVIER

Executive Officer

Fédération du e-commerce et de la vente à distance

(Fevad, Federation of e-commerce and distance selling)

Magalie CARRÉ

Paris Chamber of Commerce and Industry – Île-de-France (CCIP)

PROFESSIONALS QUALIFIED BY THEIR EXPERTISE.

Églantine DELMAS

Chief Operating Officer for France

Worldline

David NACCACHE

Professor

École normale supérieure (ENS)

A4

METHODOLOGY FOR MEASURING FRAUD INVOLVING CASHLESS MEANS OF PAYMENT

GENERAL FRAMEWORK

Definition of payment fraud

The Observatory's definition of cashless payment fraud is now aligned with that of the European Banking Authority (EBA), which is set out in its 2018 Guidelines on the reporting of fraud (EBA/GL/2018/05).¹ The guidelines define fraud as **the illegitimate use of a means of payment or the data attached to it, as well as any act contributing to the preparation or execution of such use:**

- **resulting in financial loss:** for the account-holding institution and/or issuer of the means of payment, the holder of the means of payment, the legitimate beneficiary of the funds (the acceptor and/or creditor), an insurer, a trusted third party or any party involved in the design, production, transport or distribution chain of physical or logical data that could incur civil, commercial or criminal liability;
- **regardless of:**
 - the means used to obtain (with no reasonable cause) the data or physical means of payment (theft, appropriation, hacking, etc.);
 - how the means of payment or associated data were used (remote or proximity payments, withdrawals, etc.);
 - the geographical region of issuance or use of the means of payment or related data;
- **and irrespective of the fraudster's identity:** a third party, the account-holding institution and/or issuer of the means of payment, the lawful holder of the means of payment, the legitimate beneficiary of the funds, a trusted third party, etc.

Transactions covered

The Observatory measures fraud by counting all payment transactions for which there has been made an entry in the account of at least one of the transaction's counterparties which has been rejected *a posteriori* on the grounds of fraud. Fraud does not include attempted fraud, where fraud is stopped before the transaction is carried out.

Also excluded from fraud are:

- irregular use of a means of payment due to a lack of sufficient funds, or a closed account resulting in an unpaid balance;
- using a false or assumed identity to open an account or obtain a means of payment in order to make payments;
- situations where the legitimate holder of the means of payment authorises a payment but then objects to its settlement, abusing lawful procedures by making a dispute in bad faith. These include commercial

disputes (such as the case of a bankrupt site not delivering sold products, or abusing the fact that an item purchased does not conform to its order);

- cases where a legitimate payer makes a payment to a beneficiary who is a swindler or an accomplice of a swindler, and the product or service purchased does not exist and is therefore not delivered (for example, illicit sale of financial products such as investment products or taking out loans).

The approach used to assess fraud is called "gross-fraud". It entails looking at the initial defrauded amount in a payment transaction without taking into account any measures that may subsequently be taken by the counterparties to reduce such loss (for example, interruption of the delivery of products or the provision of services, amicable agreement to reschedule payment in the event of improper payment rejection, damages to follow up legal action, etc.). The Observatory for the Security of Payment Cards, for example, estimated in its 2015 annual report² that the impact of measures of this kind reduced the gross estimate of fraud in card payments by 5%.

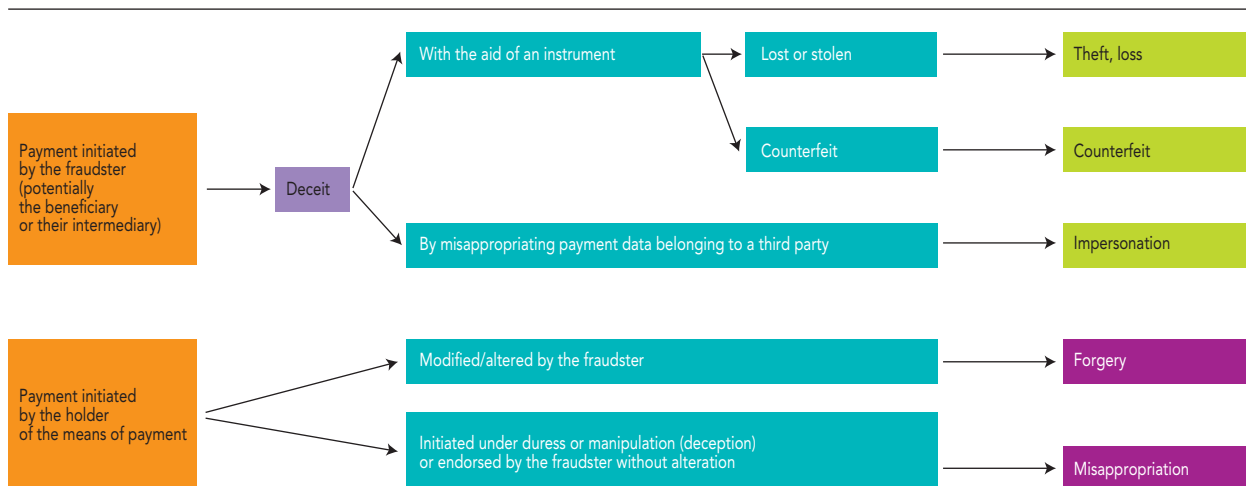
Sources of fraud data

Data on fraud is collected by the Observatory's secretariat from all the institutions concerned, following an approach according to means of payment (see below). Given the confidential nature of the individual data collected, only statistics consolidated at national level are made available to members of the Observatory to be presented in its annual report.

¹ This guideline has been drawn up under Article 96(6) of the Second European Directive on Payment Services in the Internal Market (EU Directive 2015/2366, known as "PSD 2").

² See the annual report of the Observatory for the Security of Payment Cards, 2015 (page 12).

Schematic presentation of the different types of fraud



Note: This schematic presentation should be read in conjunction with the Banque de France's official guides on the collection of statistics on payment fraud.

Types of payment fraud

As part of its analysis of payment fraud, the Observatory has identified three main types of fraud, although these do not apply in the same way to the various payment instruments:

- **fakes** (theft, loss, counterfeit): initiating a deceitful payment order, either by means of a physical payment instrument (card, chequebook, etc.) that has been stolen (whether it was stolen after it was received by the legitimate holder or before the legitimate beneficiary received it from their payment service providers – PSP), lost or counterfeited, or by misappropriating bank data or identifiers;
- **falsification**: alteration of a legitimate payment order given by the holder of the payment instrument, by changing one or more of its attributes (amount, currency, name of beneficiary, beneficiary's account details, etc.);
- **misappropriation**: transaction initiated by the payer under duress or manipulation (deception), without alteration or modification of an attribute by the fraudster.

Geographical breakdown of payment fraud

Fraud data is broken down into national, European and international transactions. Until 2020, European transactions were measured within the Single Euro Payment Area (SEPA), but since 2021, they have been measured within the European Economic Area (EEA), seeking to align the Observatory's methodology with that of the European Banking Authority (EBA). The United Kingdom is part of the SEPA, but since Brexit in 2020, is now outside the EEA.

MEASURING PAYMENT CARD FRAUD

Transactions covered

Payment card fraud, as measured in this report, concerns payment transactions (local and remote) and withdrawals made with payment cards and carried out in France and abroad whenever one of the

counterparties in the transaction is French, this includes cards issued by a French institution, or a merchant or ATM/ABM located in France that accepts the transaction. No distinctions are made according to the nature of the payment channel used (interbank³ or private⁴) or the category of card involved (debit card, credit card, commercial card or prepaid card).

Sources of fraud data

Payment card fraud data comes from data reported by payment systems, not payment service providers, and it is collected by the Banque de France on behalf of the Observatory from:

- members of *Groupe des Cartes Bancaires* CB, MasterCard, Visa Europe and UnionPay, through their intermediaries;
- the main private label card issuers operating in France.

Elements in the analysis of fraud

The analysis of payment card fraud takes several parameters into account: type of fraud, payment initiation channel, geographical areas where the card or the data attached to it is issued and used and, for remote payments, the business sector of the merchants involved, as well as internet payment method used.

³ The term "interbank" is used to describe card payment systems involving several card-issuing payment service providers and payment processors.

⁴ The term "private" refers to card payment systems involving a single payment service provider, who is both the card issuer and the payment processor.

| Types of payment card fraud | Types of fraud |
|-----------------------------|--|
| Lost or stolen card | The fraudster uses a payment card after it has been lost or stolen, without the legitimate holder's knowledge. |
| Card not received | The card was intercepted when it was sent by the issuer to its legitimate holder, in a type of fraud is similar to loss or theft, with the difference that in this case it is difficult for cardholders to realise that a fraudster is in possession of a card intended for them. The fraudster focuses on exploiting vulnerabilities in the card-sending procedures. |
| Counterfeit card | Forging a payment card involves either modifying the data in the magnetic, the embossing ^{a)} or in the programming of a genuine card, or creating a medium that gives the illusion of being a genuine payment card and/or is likely to deceive a merchant's automatic teller machine or payment terminal. In both cases, the fraudster makes sure that such a card carries the data required to fool the payment system. |
| Misappropriated card number | A cardholder's card number is taken without their knowledge, or created by random number generators, ^{b)} and used in remote sales. |
| Other | This category includes any other reason for fraud, such as the use of a card number that is consistent but not assigned to a cardholder and then used in remote sales, the fraudster's alteration of a legitimate payment order (forgery), manipulation of the payer to obtain a card payment (misappropriation), etc. |

a) Modification of the card numbers embossed on the card.

b) A fraud technique consisting in the use of an issuer's own rules for generating card numbers.

| Card use channel | Types of use |
|-------------------------------------|--|
| Proximity and ATM payment | Payment made at the point of sale or at a vending machine, including contactless payment. |
| Remote payment (excluding internet) | Payment made by post, electronic mail (email) or fax/telephone, often referred to as a MOTO payment by card payment systems, standing for "Mail Order, Telephone Order". |
| Internet payment | Payment made on the internet (on the merchant's website or via an application). |
| Withdrawal | Cash withdrawal at an automatic teller machine (ATM). |

| Types of payment on the internet | Description |
|--|--|
| 3D-Secure payment with strong authentication | Payment made over the internet using the 3D-Secure infrastructure with strong cardholder authentication. |
| 3D-Secure payment without strong authentication | Payment made over the internet using the 3D-Secure infrastructure without strong authentication by applying an exemption provided for by the European regulations resulting from the second European Payment Services Directive (PSD 2) or in the event of an incident that does not allow the implementation of strong authentication. Single-factor authentication (for example: SMS OTP – one time password – alone) are also included in this category. |
| Unauthenticated payment | Any payment made outside the 3D-Secure infrastructure, including: <ul style="list-style-type: none"> • payment not subject to European rules on strong authentication (PSD 2),^{a)} such as a payment initiated by the creditor on the basis of a pre-existing agreement between the payer and the creditor (e.g.: Merchant Initiated Transaction – MIT) and “One-leg” payments (where the issuer or the acquirer of the payment is located outside the European Union); • payment subject to European rules on strong authentication, but for which the reason for exemption is formalised in the authorisation flow; • payment subject to European rules on strong authentication, but not compliant. |

a) The European rules on strong authentication are set out in an act delegated by the PSD 2: Delegated Regulation (EU) 2018/389 detailing, for transactions subject to strong authentication, the various grounds for exemption and the conditions for implementing them.

| Geographical area | Description |
|---|---|
| National transaction | The issuer and the acquirer are both established in France. ^{a)} However, in remote payments, the fraudster can operate from abroad. |
| Outgoing European transaction | The issuer is based in France and the acquirer is based abroad in the European Economic Area (EEA). |
| Outgoing international transaction | The issuer is based in France and the acquirer is based abroad in the European Economic Area (EEA). |
| Incoming European transaction | The issuer is based in France and the acquirer is based outside of the European Economic Area (EEA). |
| Inbound international transaction | The issuer is based abroad in the European Economic Area (EEA) and the acquirer is based in French territory. |

a) For the purposes of this report, French territory includes mainland France, the overseas departments and regions (Guadeloupe, French Guiana, Martinique, Réunion, Saint-Pierre-et-Miquelon, Mayotte, Saint-Barthélemy and Saint-Martin) and the Principality of Monaco. French Polynesia, Wallis and Futuna and New Caledonia are not part of the French territory and are not members of the European Union. Transactions between France and these last territories are therefore accounted for as international transactions.

| Merchant's sector of activity for remote payments on and off the internet | Description |
|---|---|
| Food | Grocery stores, supermarkets, hypermarkets, etc. |
| Supplying an account, selling from one person to another | Online sales sites between individuals, etc. |
| Insurance | Subscription of insurance contracts. |
| Generalist and semi-generalist trade | Textile/clothing, general department store, catalogue sales, private sales, etc. |
| Home equipment | Sale of furniture and DIY products. |
| Online games | Online gaming and betting sites. |
| Technical and cultural products | Computer hardware and software, photographic material, books, CDs/DVDs, etc. |
| Health, beauty, hygiene | Sale of pharmaceutical, parapharmaceutical and cosmetic products. |
| Services for individuals and professionals | Hospitality, rental services, show ticketing, charity, office equipment, courier services, etc. |
| Telephony and communication | Telecommunication/mobile telephone equipment and services. |
| Travel, transportation | Rail, air, sea. |
| Other | Merchants that do not fit into any of the above categories. |

MEASURING TRANSFER FRAUD

Payment instruments covered

Transfer fraud, as measured in this report, concerns payment orders given by the payer (understood as the originator) to transfer funds from their payment or e-money account to the account of a third-party beneficiary. This category covers both credit transfers in SEPA format (SEPA credit transfer), including instant transfers (SEPA credit transfer Inst), and customer credit transfers issued via large-value payment systems (in particular the TARGET2 system operated by the Eurosystem national central banks, and the private pan-European Euro1 system).

Sources of fraud data

Data on credit transfer fraud is provided by the Banque de France and comes from the regulatory half-yearly fraud declarations made to it by approved payment service providers⁵ as contributions its "Census on cashless payment fraud". This data is reported by PSPs in their capacity as the institution servicing the payer in the transaction.

Elements in the analysis of fraud

Transfer fraud is analysed on the basis of the types of fraud, the geographical areas in which transfers are made and received, and the initiation channels used.

⁵ Institutions authorised to maintain payment accounts on behalf of their customers and to issue means of payment under the following statutes in accordance with French and European regulations: i) credit or similar institutions (institutions referred to in Article L. 518-1 of the French Monetary and Financial Code), electronic

money institutions and payment institutions governed by French law; ii) credit institutions, electronic money institutions and payment institutions governed by foreign law authorised to operate on French territory and established on French territory (i.e. present in France in the form of a branch).

| Types of transfer fraud | Types of fraud |
|-------------------------|---|
| Deceit | The fraudster counterfeits a transfer order or usurps the legitimate originator's online banking credentials to initiate a payment order. The credentials may be obtained by hacking (phishing, malware, etc.) or under duress. |
| Forgery | The fraudster intercepts and modifies a legitimate transfer order or file. |
| Misappropriation | The fraudster uses deception (in particular social engineering, by assuming the identity of one of the payer's contacts: line manager, supplier, bank technician, etc.) into regularly issuing a transfer to an account number that is not that of the legitimate creditor or that does not correspond to an economic reality. For example, cases of fraud involving the impersonation of a senior executive of a company, or fraud involving changes of bank details meet this definition. |

| Geographical area of transfer issue and destination | Description |
|--|--|
| Domestic transfer | Transfer from an account held in France ^{a)} to another account held in France. |
| European transfer (cross-border transfer within the EEA) | Transfer from an account in France to an account in another European Economic Area (EEA) country. |
| International transfer (cross-border transfer outside the EEA) | Transfer from an account held in France to an account held abroad in a country outside the European Economic Area (EEA). |

a) For the purposes of this report, French territory includes mainland France, the overseas departments and regions (Guadeloupe, French Guiana, Martinique, Réunion, Saint-Pierre-et-Miquelon, Mayotte, Saint-Barthélemy and Saint-Martin) and the Principality of Monaco. French Polynesia, Wallis and Futuna and New Caledonia are not part of the French territory and are not members of the European Union. Transactions between France and these last territories are therefore accounted for as international transactions.

| Initiation channel used | Types of use |
|--|---|
| Non-electronic means (post, courier, telephone) | Transfer orders sent by post, form, courier, fax or telephone. A common feature of these transfers is the need to re-enter the payer's payment instructions. |
| Online banking | Transfer order initiated by the payer from their online banking account (via a web browser or an online banking mobile application) or from an online payment initiation service (via their online banking account). |
| Transfer initiated by batch/file (telematic channels) | Transfer order sent via other electronic channels (excluding online banking and mobile payment applications), such as the EBICS system (Electronic Banking Internet Communication Standard, an interbank communication channel enabling companies to carry out automated file transfers with a bank). |
| Electronic transfer initiated by non-remote channel (ATM, counter) | Transfer order initiated at a branch's counter or from an automatic teller machine (ATM). |
| Payment Initiation Service Providers (PISPs) | Transfer order initiated via a PISP at the customer's request. |

MEASURING DIRECT DEBIT FRAUD

Payment instruments covered

Direct debit fraud, as measured in this report, concerns payment orders given by the creditor to their payment service provider to debit a debtor's account, having previously obtained an authorisation (or direct debit order) from the debtor. The category comprises direct debits in the SEPA European format (SEPA direct debit – SDD), and includes the standard direct debit (SDD Core) and the business-to-business direct debit (SDD B2B).

Sources of fraud data

Data on direct debit fraud is provided to the Observatory by the Banque de France and comes from the regulatory half-yearly fraud declarations made to it by approved payment service providers as contributions to the Banque de France's "Census on cashless payment fraud". The data is reported by PSPs in their capacity as the institution servicing the creditor.

Elements in the analysis of fraud

Direct debit fraud is analysed on the basis of the types of fraud, the geographical areas where the direct debit is issued and where it is sent, the format of the direct debit mandate, and the methods used to initiate it.

| Types of direct debit fraud | Types of fraud |
|-----------------------------|--|
| Deceit | The fraudster, acting as creditor, issues direct debits to account numbers that they have obtained illegally and without any authorisation or underlying economic reality ("unauthorised payment transaction" in the terminology of the European Banking Authority – EBA). |
| Misappropriation | The fraudster, acting as debtor, uses the identity and IBAN (international bank account number) of a third party to sign a direct debit mandate on an account that is not their own ("manipulation of the payer by the fraudster" in EBA terminology). |

| Geographical area of transfer issue and destination | Types of fraud |
|---|---|
| Domestic direct debit | Direct debit issued by a creditor whose account is domiciled in France to another account held in France. |
| European direct debit | Direct debit issued by a creditor whose account is domiciled in France to an account held in another European Economic Area (EEA) country. |
| International direct debit | Direct debit issued by a creditor whose account is domiciled in France to an account held abroad in a country outside the European Economic Area (EEA) country. |

| Format of a direct debit order | Description |
|--------------------------------|--|
| Paper | Direct debit issued on the basis of a mandate collected via letter, form, courier, fax or telephone. What all these channels have in common is the need to re-enter the order in the system. |
| Electronic | Direct debit issued on the basis of an order collected from an internet channel (online banking website, creditor's website or mobile application) or other telematic channels. |

| Initiation methods | Description |
|---|--|
| Direct debit initiated on the basis of a single payment | Electronically initiated direct debit that is independent of other direct debits. |
| Direct debit initiated from a file or batch | Direct debit initiated electronically as part of a group of direct debits initiated by the creditor. |

MEASURING CHEQUE FRAUD

Unlike other cashless means of payment, cheques are unique in that they only exist in paper format and use the payer's signature as the only means of authentication. These characteristics do not allow banks to implement automatic authentication systems prior to payment.

Scope of fraud

Cheque fraud, as measured in this report, concerns cheques payable in France, in euro or in foreign currency, subject to the legal regime set out in Articles L. 131-1 to 88 of the French Monetary and Financial Code and includes cheques drawn by a bank's customers on accounts held by the bank, as well as cheques received from the bank's customers to credit these accounts.

This definition includes the following categories: bank cheques, cashier's cheques, cheque-letters for companies, salary-cheques (TTS – *titre de travail simplifié*) for companies; it excludes travellers' cheques, as well as the special payment vouchers defined in Article L. 525-4 of the French Monetary and Financial Code and the specific payment instruments described in Article L. 521-3-2 of the same code, such as holiday vouchers, restaurant vouchers, culture vouchers or universal employment-service vouchers, which cover various categories of vouchers whose use is restricted either to the acquisition of a limited number of goods or services, or to a limited network of acceptors.

Sources of fraud data

Data on cheque fraud is provided by the Banque de France and comes from the regulatory half-yearly fraud declarations made to it by payment service providers as contributions to its "Census on cashless payment fraud". PSPs report this data in their capacity as institutions receiving cheques for collection from their customers (as remitting institutions).

Elements of fraud data analysis

Cheque fraud data is analysed on the basis of the main types of fraud defined by the Observatory. The table below summarises the most commonly observed forms of cheque fraud and the typology to which they belong.

Specificities of the gross-fraud approach for cheques

Until 2020, gross-fraud data for cheques included all cheque transactions cashed, presented for payment and rejected because of fraudulence (gross-fraud, former approach).

From 2021, gross-fraud data for cheques excludes fraud thwarted by an institution after the cheque has been paid (gross-fraud, new approach). These thwarted fraud attempts must meet the following two criteria to be excluded:

- 1) The cheque was rejected for fraudulence before the funds could be used by the remitter because the release of the funds to the customer's account was delayed or blocked (e.g. when a suspense or technical account is used, including declined orders, which are recorded in the remitting customer's account at the same time as credits).
- 2) The institution concerned had substantial evidence, supported by formalised indicators, that the cheque could be fraudulent, i.e. a cheque remitted with the aim of reaping fraudulent benefits, including when the cheque is remitted through an account used as an intermediary.

Cheque fraud totals are calculated using the new gross-fraud approach, which takes into account frauds detected after the cheque has been presented for payment. However, even from 2021 onwards, the breakdowns of cheque fraud by type are based on the old gross-fraud approach.

| Types of cheque fraud | Types of fraud |
|---------------------------|--|
| Deceit (theft, loss) | Use by the fraudster of a cheque lost or stolen from its rightful holder, bearing a forged signature that is neither that of the account holder nor that of their authorised representative. Illegitimate issue of a cheque by a fraudster using a blank cheque ^{a)} (including where the transaction was carried out under duress by the legitimate holder). |
| Counterfeit | The fraudster creates from scratch a counterfeit cheque, "issued" by an actual or fake bank . |
| Forgery | A fraudster intercepts a legitimate cheque and alters it by scratching, rubbing out or erasing the data. |
| Misappropriation or reuse | Cheque lost or stolen after clearing in a payment system and presented again for collection (reuse). Cheque duly issued, lost or stolen, intercepted on its way to the legitimate beneficiary and cashed in an account other than that of the legitimate beneficiary (misappropriation). The cheque is correct; the payee's name is unchanged and the magnetic line at the bottom of the cheque is valid, as is the customer's signature. |

a) Blank cheque, made available to the customer by the account-holding bank.

MEASURING COMMERCIAL PAPER FRAUD

Payment instruments covered

Commercial paper fraud, as measured in this report, is concerned with two payment instruments:

- *Lettre de change relevé* (LCR – bill of exchange): a document issued on paper or electronic form by which the issuer (usually the supplier) instructs the debtor (the customer) to pay a specific sum of money;
- *Billet à ordre relevé* (BOR – promissory note): a paperless payment order by which the payer acknowledges that they owe the beneficiary a certain sum of money and promises to pay it by a certain date, both specified on the note.

Typology and sources of fraud data

The types of commercial paper fraud are the same as those identified for cheques.

Fraud data on commercial paper is provided by the Banque de France and derived from the statutory half-yearly fraud reports made to it by payment service providers as contributions to its "Census on cashless payment fraud". PSPs report this data in their capacity as institutions receiving commercial paper for collection from their customers (as remitting institutions).

MEASURING FRAUD IN MONEY REMITTANCES

Payment services covered

Money remittances correspond to Payment Service 6 as defined in Article L. 314-1 of the French Monetary and Financial Code, in accordance with the provisions of the Second European Payment Services Directive (PSD 2), describing a payment service where funds are sent and received without creating payment accounts in the name of the payer or payee, for the sole purpose of transferring an amount to a payee or another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

Sources of fraud data

Fraud data on money remittances is provided by the Banque de France and derived from the half-yearly fraud declarations made to it by payment service providers as contributions to its "Census on cashless payment fraud". PSPs report this data in their capacity as the institution servicing the payer (originator), with a geographical breakdown identical to that used for credit transfers.

**MEASURING FRAUD ON TRANSACTIONS
VIA PAYMENT INITIATION SERVICE PROVIDERS (PISPs)**

Payment services covered

Payment initiation services are included in Payment Service 7 as described in Article L. 314-1 of the French Monetary and Financial Code, in accordance with the provisions of PSD 2. It is a service that initiates, via an approved PISP, a payment order at the request of the payment service user concerning a payment account held with a PSP. The transaction generally takes the form of a bank transfer.

Sources of fraud data

Fraud data on payment initiation services is provided by the Banque de France and derived from the half-yearly statutory fraud reports given as contributions to its "Census of fraud in cashless means of payment" by PSPs established or authorised to operate in France, with a breakdown by initiation channel.

| Initiation channel | Description |
|--------------------|--|
| Remotely | Payment initiated over the internet from a computer, mobile phone or similar terminal. |
| In proximity | Payment initiated at the point of sale, using an ATM or bank counter, with the payer physically present. |

**SPECIFIC PROVISIONS FOR FRAUD
INVOLVING ELECTRONIC MONEY TRANSACTIONS**

Payment instruments covered

Electronic money is monetary value stored in electronic form, representing a claim on the issuer that must be pre-funded by another payment instrument, and which may be accepted in payment by a natural or legal person other than the electronic money issuer (Article L. 315-1 of the French Monetary and Financial Code, in accordance with the provisions of Directive 2009/110/EC on electronic money institutions, known as "EMD2").

Sources of fraud data

The data on payment fraud is provided by the Banque de France and derived from the half-yearly reports on fraud made to it by electronic money issuers as contributions to its "Census on cashless payment fraud". Electronic money issuers provide this data with a breakdown by initiation channel (regardless of the medium used, whether a physical medium or an online account held by the institution).

There are two categories of electronic money media:

- physical media such as prepaid cards;
- online accounts held by the issuing institution.

| Initiation channel | Description |
|--------------------|---|
| Remotely | Payment initiated via the internet from a computer, mobile phone or other similar terminal. |
| In proximity | Payment initiated at the point of sale, using an ATM or bank counter, including using contactless systems, with the payer physically present. |

A5

STATISTICAL FILE ON PAYMENT CARD USE AND FRAUD



You can download the tables in this appendix and additional tables at the following address:
<https://www.banque-france.fr/dossier-statistique-2022-annexe-5-du-rapport-annuel>

OVERVIEW OF MEANS OF PAYMENT

T1 Map of cashless means of payment in 2022

(number in millions, value in EUR billions, average value in EUR, shares and changes in percentage)

| | Average number of transactions (volume) | | | Average daily transactions (value) | | | Average value |
|--|---|------------------|--------------|------------------------------------|------------------|--------------|---------------|
| | 2022 | Change 2022/2021 | Share | 2022 | Change 2022/2021 | Share | |
| Payment by card ^{a)} | 18,258 | 13.2 | 59.6 | 746 | 13.0 | 1.8 | 41 |
| <i>of which contactless</i> | 9,103 | 23.5 | 29.7 | 148 | 18.3 | 0.3 | 16 |
| <i>of which mobile payments</i> | 845 | 136.5 | 2.8 | 18 | 136.1 | 0.0 | 21 |
| Cheque | 1,008 | -8.8 | 3.3 | 540 | -8.3 | 1.3 | 536 |
| Credit transfer | 5,158 | 6.5 | 16.8 | 38,895 | 0.4 | 91.4 | 7,541 |
| <i>of which LVT^{b)}</i> | 19 | 114.1 | 0.1 | 15,908 | -19.1 | 37.4 | 825,710 |
| <i>of which instant transfers (SCT Inst)</i> | 198 | 84.8 | 0.6 | 119 | 137.7 | 0.3 | 601 |
| Direct debit | 4,914 | -2.1 | 16.0 | 2,041 | 7.7 | 4.8 | 415 |
| Commercial paper | 75 | 0.0 | 0.2 | 222 | 4.8 | 0.5 | 2,949 |
| Electronic money | 75 | 18.7 | 0.2 | 1 | -39.3 | 0.0 | 7 |
| Money remittance | 3 | 74.7 | 0.0 | 1 | -32.9 | 0.0 | 241 |
| Total | 29,491 | 8.3 | 96.3 | 42,445 | 0.9 | 99.7 | 1,439 |
| Withdrawals by card ^{a)} | 1,136 | 4.5 | 3.7 | 133 | 7.3 | 0.3 | 117 |
| Total transactions | 30,627 | 8.1 | 100.0 | 42,578 | 0.9 | 100.0 | 1,390 |

a) Cards issued in France only.

b) LVT: Large Value Transfers issued through large value payment systems (Target 2, Euro1), corresponding exclusively to institutional payments.

Source: Observatory for the Security of Payment Means.

T2 Historical evolution of cashless payments

a) By volume
(in millions of transactions)

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|--|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| Card | 11,134 | 12,581 | 13,179 | 14,485 | 13,852 | 16,129 | 18,258 |
| <i>of which contactless</i> | 635 | 1,300 | 2,374 | 3,779 | 5,159 | 7,369 | 9,103 |
| <i>of which by mobile</i> | 0 | 5 | 11 | 48 | 129 | 357 | 845 |
| Cheque | 2,137 | 1,927 | 1,747 | 1,587 | 1,175 | 1,106 | 1,008 |
| Credit transfer | 3,753 | 3,870 | 4,038 | 4,269 | 4,483 | 4,843 | 5,158 |
| <i>of which instant transfers (SCT inst)</i> | <i>n/a</i> | <i>n/a</i> | 0 | 14 | 45 | 107 | 198 |
| Direct debit | 3,963 | 4,091 | 4,211 | 4,370 | 4,622 | 5,020 | 4,914 |
| Commercial paper | 82 | 81 | 81 | 78 | 71 | 75 | 75 |
| Electronic money | 38 | 55 | 65 | 62 | 36 | 63 | 75 |
| Money remittance | 20 | 18 | 16 | 16 | 15 | 2 | 3 |
| Total cashless payments | 21,107 | 22,605 | 23,320 | 24,851 | 24,238 | 27,238 | 29,491 |
| Withdrawals by card | 1,491 | 1,481 | 1,439 | 1,392 | 1,064 | 1,086 | 1,136 |

b) In value
(EUR billions)

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|--|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| Card | 499 | 530 | 568 | 600 | 578 | 660 | 746 |
| <i>of which contactless</i> | 7 | 13 | 25 | 43 | 80 | 125 | 148 |
| <i>of which by mobile</i> | 0.005 | 0.1 | 0.2 | 1 | 3 | 8 | 18 |
| Cheque | 1,077 | 1,002 | 891 | 814 | 614 | 589 | 540 |
| Credit transfer | 23,697 | 24,069 | 24,296 | 25,164 | 32,712 | 38,723 | 38,895 |
| <i>of which instant transfers (SCT Inst)</i> | <i>n/a</i> | <i>n/a</i> | 0.086 | 7 | 27 | 50 | 119 |
| Direct debit | 1,492 | 1,579 | 1,645 | 1,711 | 1,684 | 1,895 | 2,041 |
| Commercial paper | 266 | 260 | 252 | 232 | 197 | 212 | 222 |
| Electronic money | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Money remittance | 0.8 | 1.6 | 2 | 2 | 2 | 1 | 1 |
| Total cashless payments | 27,032 | 27,440 | 27,653 | 28,522 | 35,786 | 42,081 | 42,445 |
| Withdrawals by card | 129 | 135 | 137 | 137 | 116 | 124 | 133 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available.

OVERVIEW OF FRAUD

T3 Breakdown of payment fraud in 2022

(value and average value in EUR; volume in units; share and change in percentage)

| | Volume | | | Value | | | Fraud rate 2022 | Average value |
|--|------------------|---------------------|--------------|----------------------|---------------------|--------------|--------------------|------------------|
| | 2022 | Change 2022/2021 | Share | 2022 | Change 2022/2021 | Share | | |
| Payment by card ^{a)} | 6,692,988 | -1.1 | 93.4 | 420,585,823 | -0.2 | 35.3 | 0.056 | 63 |
| <i>of which contactless</i> | 796,027 | 31.7 | 11.1 | 23,047,180 | 41.6 | 1.9 | 0.016 | 29 |
| <i>of which by mobile</i> | 162,869 | 95.6 | 2.3 | 10,942,984 | 95.1 | 0.9 | 0.061 | 67 |
| Cheque (new methodology) ^{b)} | 218,122 | -6.1 | 3.0 | 395,416,196 | -15.0 | 33.2 | 0.073 | 1,813 |
| Cheque (old methodology) | 266,216 | -2.5 | 3.7 | 556,796,815 | -11.0 | 46.7 | 0.103 | 2,092 |
| Credit transfer | 76,846 | 64.5 | 1.1 | 313,163,442 | 9.0 | 26.3 | 0.001 | 4,075 |
| <i>of which instant transfers (SCT inst)</i> | 33,193 | 157.1 | 0.5 | 52,768,218 | 135.5 | 4.4 | 0.044 | 1,590 |
| Direct debit | 49,453 | -80.3 | 0.7 | 19,853,012 | -21.6 | 1.7 | 0.001 | 401 |
| Commercial paper | 1 | 0.0 | 0.0 | 12,079 | 0.0 | 0.0 | 0.000 | 12,079 |
| Electronic money | 1,945 | -2.8 | 0.0 | 77,349 | -43.7 | 0.0 | 0.015 | 40 |
| Money remittance | 154 | -84.0 | 0.0 | 77,162 | -68.7 | 0.0 | 0.009 | 501 |
| Total payments | 7,039,509 | -3.5 | 98.3 | 1,149,185,062 | -4.2 | 96.4 | 0.003 | 163 |
| Withdrawals by card ^{a)} | 123,574 | -4.3 | 1.7 | 43,148,054 | 0.5 | 3.6 | 0.032 | 349 |
| Total transactions | 7,163,083 | -3.6 | 100.0 | 1,192,333,116 | -4.0 | 100.0 | 0.003 | 166 |

a) Cards issued in France only.

b) The new methodology towards measuring cheque fraud excludes fraud thwarted after a cheque has been cashed.

From 2021 onwards, totals for fraud involving cashless means of payment derive from a new methodology to measuring cheque fraud, which excludes fraud thwarted after the cheque has been cashed, and includes fraud involving electronic money and the money remittances.

Source: Observatory for the Security of Payment Means.

T4 Historical trends in payment fraud

a) By volume
(in units)

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|--|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| Card | 5,300,847 | 5,364,312 | 6,068,959 | 7,071,095 | 7,421,137 | 6,764,752 | 6,692,988 |
| <i>of which contactless</i> | 125,860 | 248,991 | 445,919 | 603,509 | 537,061 | 604,278 | 796,027 |
| <i>of which by mobile</i> | n/a | 22 | 2,070 | 3,494 | 33,761 | 83,266 | 162,869 |
| Cheque (new methodology) | n/a | n/a | n/a | n/a | 190,001 | 232,277 | 218,122 |
| Cheque (old methodology) | 120,295 | 114,906 | 166,421 | 183,488 | 220,685 | 272,970 | 266,216 |
| Credit transfer | 5,585 | 4,642 | 7,736 | 15,934 | 35,893 | 46,718 | 76,846 |
| <i>of which instant transfers (SCT inst)</i> | n/a | n/a | 5 | 729 | 7,131 | 12,913 | 33,193 |
| Direct debit | 1,176 | 25,801 | 309,377 | 43,519 | 6,485 | 251,010 | 49,453 |
| Commercial paper | 4 | 3 | 5 | 1 | 62 | 1 | 1 |
| Electronic money | n/a | n/a | n/a | n/a | n/a | 2,001 | 1,945 |
| Money remittance | n/a | n/a | n/a | n/a | n/a | 962 | 154 |
| Total cashless payment fraud | 5,427,907 | 5,509,664 | 6,552,498 | 7,314,037 | 7,684,262 | 7,297,721 | 7,039,509 |
| Withdrawals by card | 202,158 | 177,562 | 158,908 | 165,505 | 113,067 | 129,083 | 123,574 |
| Total fraudulent transactions | 5,630,065 | 5,687,226 | 6,711,406 | 7,479,542 | 7,797,329 | 7,426,804 | 7,163,083 |

b) In value
(EUR)

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|--|--------------------|--------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Card | 378,455,912 | 344,962,084 | 401,604,986 | 428,249,931 | 439,489,315 | 421,410,285 | 420,585,823 |
| <i>of which contactless</i> | 1,410,566 | 2,748,790 | 5,234,852 | 8,479,354 | 11,292,261 | 16,274,668 | 23,047,180 |
| <i>of which by mobile</i> | n/a | 1,227 | 73,682 | 216,236 | 2,792,574 | 5,610,270 | 10,942,984 |
| Cheque (new methodology) | n/a | n/a | n/a | n/a | 401,611,189 | 465,021,167 | 395,416,196 |
| Cheque (old methodology) | 276,716,554 | 296,072,847 | 450,108,464 | 539,215,175 | 538,059,139 | 625,703,442 | 556,796,815 |
| Credit transfer | 86,284,101 | 78,286,492 | 97,327,128 | 161,642,174 | 266,969,099 | 287,264,068 | 313,163,442 |
| <i>of which instant transfers (SCT inst)</i> | n/a | n/a | 29,800 | 2,203,240 | 10,562,419 | 22,406,942 | 52,768,218 |
| Direct debit | 39,935,882 | 8,726,403 | 58,346,253 | 10,990,025 | 1,891,051 | 25,318,677 | 19,853,012 |
| Commercial paper | 1,018,149 | 153,100 | 226,217 | 74,686 | 538,918 | 12,079 | 12,079 |
| Electronic money | n/a | n/a | n/a | n/a | n/a | 137,340 | 77,349 |
| Money remittance | n/a | n/a | n/a | n/a | n/a | 246,362 | 77,162 |
| Total cashless payment fraud | 782,410,598 | 728,200,926 | 1,007,613,048 | 1,140,171,991 | 1,246,947,522 | 1,199,409,978 | 1,149,185,062 |
| Withdrawals by card | 48,650,966 | 42,038,924 | 37,630,659 | 41,651,788 | 33,950,879 | 42,950,169 | 43,148,054 |
| Total fraudulent transactions | 831,061,564 | 770,239,850 | 1,045,243,707 | 1,181,823,779 | 1,280,898,401 | 1,242,360,147 | 1,192,333,116 |

Source: Observatory for the Security of Payment Means.

Notes: From 2021 onwards, totals for fraud involving cashless means of payment derive from a new methodology to measuring cheque fraud, which excludes fraud thwarted after the cheque has been cashed, and includes fraud involving electronic money and the money remittances.
n/a, not available.

CARD: ISSUANCE

T5 Payments by card issued in France (volume in thousands, value in EUR thousands)

| | 2017 | | 2018 | | 2019 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 10,969,923 | 428,693,263 | 11,222,954 | 443,193,792 | 12,171,755 | 459,066,750 |
| of which contactless payments (including mobile payments) | 1,300,071 | 13,204,448 | 2,374,029 | 25,219,537 | 3,778,756 | 42,903,452 |
| of which mobile payments | 4,600 | 93,204 | 11,399 | 200,876 | 47,885 | 850,983 |
| Remote payments (excluding internet) | 48,775 | 3,627,542 | 63,021 | 4,696,704 | 77,150 | 4,838,911 |
| Internet payments | 1,562,378 | 97,393,059 | 1,893,443 | 119,903,848 | 2,236,049 | 135,352,563 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 1,481,470 | 134,932,233 | 1,439,414 | 136,638,334 | 1,391,930 | 136,507,651 |
| Total | 14,062,546 | 664,646,097 | 14,618,833 | 704,432,677 | 15,876,884 | 735,765,875 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T5 Payments by card issued in France (continued) (volume in thousands, value in EUR thousands)

| | 2020 | | 2021 | | 2022 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 11,193,795 | 424,105,649 | 12,935,438 | 475,079,750 | 14,868,338 | 537,503,850 |
| of which contactless payments (including mobile payments) | 5,159,657 | 79,664,370 | 7,368,699 | 125,082,420 | 9,102,931 | 148,006,593 |
| of which mobile payments | 129,105 | 2,734,667 | 357,355 | 7,596,769 | 845,223 | 17,937,091 |
| Remote payments (excluding internet) | 134,114 | 7,567,877 | 76,931 | 7,995,010 | 105,781 | 16,994,865 |
| Internet payments | 2,524,317 | 146,563,476 | 3,116,285 | 177,056,237 | 3,283,604 | 191,418,128 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | 787,664 | 85,221,641 | 1,034,950 | 112,713,734 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | 444,723 | 19,267,910 | 781,313 | 27,091,534 |
| of which payments not using 3D-Secure | n/a | n/a | 1,883,898 | 72,566,685 | 1,467,342 | 51,612,860 |
| Withdrawals | 1,064,095 | 115,958,207 | 1,086,289 | 123,867,648 | 1,135,675 | 132,879,066 |
| Total | 14,916,322 | 694,195,208 | 17,214,942 | 783,998,644 | 19,393,398 | 878,795,909 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.



T5 bis Number of cards and supports

T6 Fraudulent transactions by card issued in France

(volume in units, value in EUR, rate in percentage)

| | 2017 | | | 2018 | | | 2019 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 969,674 | 59,046,770 | 0.014 | 1,142,861 | 64,546,992 | 0.015 | 1,203,233 | 64,992,145 | 0.014 |
| of which contactless payments (including mobile payments) | 248,991 | 2,748,790 | 0.021 | 445,919 | 5,234,852 | 0.021 | 603,509 | 8,479,354 | 0.020 |
| of which mobile payments | 22 | 1,227 | 0.001 | 2,070 | 73,682 | 0.037 | 3,494 | 216,236 | 0.025 |
| Remote payments (excluding internet) | 360,691 | 30,621,482 | 0.844 | 406,712 | 28,562,421 | 0.608 | 409,319 | 31,806,788 | 0.657 |
| Internet payments | 4,033,947 | 255,293,832 | 0.262 | 4,519,386 | 308,495,573 | 0.257 | 5,458,543 | 331,450,998 | 0.245 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 177,562 | 42,038,924 | 0.031 | 158,908 | 37,630,659 | 0.028 | 165,505 | 41,651,788 | 0.031 |
| Total | 5,541,874 | 387,001,008 | 0.058 | 6,227,867 | 439,235,645 | 0.062 | 7,236,600 | 469,901,719 | 0.064 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T6 Fraudulent transactions by card issued in France (continued)

(volume in units, value in EUR, rate in percentage)

| | 2020 | | | 2021 | | | 2022 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 972,228 | 47,994,762 | 0.011 | 942,376 | 52,426,587 | 0.011 | 1,055,575 | 62,861,464 | 0.012 |
| of which contactless payments (including mobile payments) | 537,061 | 11,292,261 | 0.014 | 604,278 | 16,274,668 | 0.013 | 796,027 | 23,047,180 | 0.016 |
| of which mobile payments | 33,761 | 2,792,574 | 0.102 | 83,266 | 5,610,270 | 0.074 | 162,869 | 10,942,984 | 0.061 |
| Remote payments (excluding internet) | 411,344 | 26,899,103 | 0.355 | 124,596 | 22,193,382 | 0.278 | 174,364 | 42,028,102 | 0.247 |
| Internet payments | 6,037,565 | 364,595,450 | 0.249 | 5,697,780 | 346,790,316 | 0.196 | 5,463,049 | 315,696,257 | 0.165 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | 496,017 | 103,029,680 | 0.121 | 624,473 | 124,258,815 | 0.110 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | 364,223 | 26,046,078 | 0.135 | 625,296 | 25,695,176 | 0.095 |
| of which payments not using 3D-Secure | n/a | n/a | n/a | 4,837,540 | 217,714,555 | 0.300 | 4,213,280 | 165,742,266 | 0.321 |
| Withdrawals | 113,067 | 33,950,879 | 0.029 | 129,083 | 42,950,169 | 0.035 | 123,574 | 43,148,054 | 0.032 |
| Total | 7,534,204 | 473,440,194 | 0.068 | 6,893,835 | 464,360,454 | 0.059 | 6,816,562 | 463,733,877 | 0.053 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T7 Types of fraud for payments by card issued in France in 2022

(volume in units, value in EUR, share in percentage)

| | Lost or stolen cards | | | | Cards not received | | | | Altered or counterfeit cards | | | |
|---|----------------------|-------------|-------------------|-------------|--------------------|------------|------------------|------------|------------------------------|------------|------------------|------------|
| | Volume | | Value | | Volume | | Value | | Volume | | Value | |
| | Number | Share | Value | Share | Number | Share | Value | Share | Number | Share | Value | Share |
| Proximity and ATM payments | 866,905 | 82.1 | 46,823,896 | 74.5 | 13,297 | 1.3 | 1,741,496 | 2.8 | 83,287 | 7.9 | 4,773,344 | 7.6 |
| of which contactless payments (including mobile payments) | 668,928 | 84.0 | 16,525,341 | 71.7 | 3,742 | 0.5 | 61,150 | 0.3 | 52,922 | 6.6 | 2,551,297 | 11.1 |
| of which mobile payments | 86,789 | 53.3 | 6,277,156 | 57.4 | 229 | 0.1 | 7,819 | 0.1 | 31,560 | 19.4 | 1,713,843 | 15.7 |
| Remote payments (excluding internet) | 1,370 | 0.8 | 479,506 | 1.1 | 47 | 0.0 | 13,687 | 0.0 | 427 | 0.2 | 132,809 | 0.3 |
| Internet payments | 76,819 | 1.4 | 4,743,859 | 1.5 | 3,180 | 0.1 | 151,727 | 0.0 | 55,226 | 1.0 | 3,525,928 | 1.1 |
| of which 3D-Secure payments with strong authentication | 6,791 | 1.1 | 1,147,008 | 0.9 | 294 | 0.0 | 64,074 | 0.1 | 510 | 0.1 | 227,034 | 0.2 |
| of which 3D-Secure payments without strong authentication | 3,428 | 0.5 | 144,810 | 0.6 | 305 | 0.0 | 6,999 | 0.0 | 204 | 0.0 | 14,171 | 0.1 |
| of which payments not using 3D-Secure | 66,600 | 1.6 | 3,452,041 | 2.1 | 2,581 | 0.1 | 80,654 | 0.0 | 54,512 | 1.3 | 3,284,723 | 2.0 |
| Withdrawals | 116,493 | 94.3 | 41,067,086 | 95.2 | 3,663 | 3.0 | 1,448,725 | 3.4 | 690 | 0.6 | 126,506 | 0.3 |
| Total | 1 061 587 | 15.6 | 93 114 347 | 20.1 | 20 187 | 0.3 | 3 355 635 | 0.7 | 139 630 | 2.0 | 8 558 587 | 1.8 |

Source: Observatory for the Security of Payment Means.

Note: ATM, automatic teller machine.

T7 Types of fraud for payments by card issued in France in 2022 (continued)

(volume in units, value in EUR, share in percentage)

| | Spoofed card number | | | | Other | | | | All sources | |
|---|---------------------|-------------|--------------------|-------------|---------------|------------|-------------------|-------------|------------------|--------------------|
| | Volume | | Value | | Volume | | Value | | Volume | Value |
| | Number | Share | Value | Share | Number | Share | Value | Share | | |
| Proximity and ATM payments | 15,936 | 1.5 | 1,904,050 | 3.0 | 76,150 | 7.2 | 7,618,678 | 12.1 | 1,055,575 | 62,861,464 |
| of which contactless payments (including mobile payments) | 9,153 | 1.1 | 462,310 | 2.0 | 61,282 | 7.7 | 3,447,082 | 15.0 | 796,027 | 23,047,180 |
| of which mobile payments | 4,061 | 2.5 | 311,402 | 2.8 | 40,230 | 24.7 | 2,632,764 | 24.1 | 162,869 | 10,942,984 |
| Remote payments (excluding internet) | 172,272 | 98.8 | 41,353,289 | 98.4 | 248 | 0.1 | 48,811 | 0.1 | 174,364 | 42,028,102 |
| Internet payments | 5,312,602 | 97.2 | 304,871,841 | 96.6 | 15,222 | 0.3 | 2,402,902 | 0.8 | 5,463,049 | 315,696,257 |
| of which 3D-Secure payments with strong authentication | 615,959 | 98.6 | 122,239,678 | 98.4 | 919 | 0.1 | 581,021 | 0.5 | 624,473 | 124,258,815 |
| of which 3D-Secure payments without strong authentication | 621,048 | 99.3 | 25,491,728 | 99.2 | 311 | 0.0 | 37,468 | 0.1 | 625,296 | 25,695,176 |
| of which payments not using 3D-Secure | 4,075,595 | 96.7 | 157,140,435 | 94.8 | 13,992 | 0.3 | 1,784,413 | 1.1 | 4,213,280 | 165,742,266 |
| Withdrawals | 325 | 0.3 | 39,063 | 0.1 | 2,403 | 1.9 | 466,674 | 1.1 | 123,574 | 43,148,054 |
| Total | 5,501,135 | 80.7 | 348,168,243 | 75.1 | 94,023 | 1.4 | 10,537,065 | 2.3 | 6,816,562 | 463,733,877 |

Source: Observatory for the Security of Payment Means.

Note: ATM, automatic teller machine.

T8 Geographical breakdown of fraud on cards issued in France in 2022

(volume in units, value in EUR, share in percentage)

| | Domestic transactions | | | | European transactions | | | |
|---|-----------------------|-------------|--------------------|-------------|-----------------------|-------------|--------------------|-------------|
| | Volume | | Value | | Volume | | Value | |
| | Number | Share | Value | Share | Number | Share | Value | Share |
| Proximity and ATM payments | 989,454 | 93.7 | 53,593,598 | 85.3 | 40,620 | 3.8 | 4,166,195 | 6.6 |
| of which contactless payments (including mobile payments) | 754,985 | 94.8 | 20,231,615 | 87.8 | 29,368 | 3.7 | 1,818,547 | 7.9 |
| of which mobile payments | 152,726 | 93.8 | 9,566,583 | 87.4 | 5,735 | 3.5 | 668,917 | 6.1 |
| Remote payments (excluding internet) | 120,708 | 69.2 | 24,857,056 | 59.1 | 30,063 | 17.2 | 10,076,248 | 24.0 |
| Internet payments | 1,874,565 | 34.3 | 145,299,292 | 46.0 | 2,287,025 | 41.9 | 102,735,078 | 32.5 |
| of which 3D-Secure payments with strong authentication | 314,967 | 50.4 | 72,922,674 | 58.7 | 220,335 | 35.3 | 39,127,248 | 31.5 |
| of which 3D-Secure payments without strong authentication | 342,714 | 54.8 | 17,460,124 | 68.0 | 204,976 | 32.8 | 5,721,496 | 22.3 |
| of which payments not using 3D-Secure | 1,216,884 | 28.9 | 54,916,494 | 33.1 | 1,861,714 | 44.2 | 57,886,334 | 34.9 |
| Withdrawals | 115,643 | 93.6 | 41,344,934 | 95.8 | 2,887 | 2.3 | 863,394 | 2.0 |
| Total | 3,100,370 | 45.5 | 265,094,880 | 57.2 | 2,360,595 | 34.6 | 117,840,915 | 25.4 |

Source: Observatory for the Security of Payment Means.

Note: ATM, automatic teller machine.

T8 Geographical breakdown of fraud on cards issued in France in 2022 (continued)

(volume in units, value in EUR, share in percentage)

| | International transactions | | | | Total | |
|---|----------------------------|-------------|-------------------|-------------|------------------|--------------------|
| | Volume | | Value | | Volume | Value |
| | Number | Share | Value | Share | | |
| Proximity and ATM payments | 25,501 | 2.4 | 5,101,671 | 8.1 | 1,055,575 | 62,861,464 |
| of which contactless payments (including mobile payments) | 11,674 | 1.5 | 997,018 | 4.3 | 796,027 | 23,047,180 |
| of which mobile payments | 4,408 | 2.7 | 707,484 | 6.5 | 162,869 | 10,942,984 |
| Remote payments (excluding internet) | 23,593 | 13.5 | 7,094,798 | 16.9 | 174,364 | 42,028,102 |
| Internet payments | 1,301,459 | 23.8 | 67,661,887 | 21.4 | 5,463,049 | 315,696,257 |
| of which 3D-Secure payments with strong authentication | 89,171 | 14.3 | 12,208,893 | 9.8 | 624,473 | 124,258,815 |
| of which 3D-Secure payments without strong authentication | 77,606 | 12.4 | 2,513,556 | 9.8 | 625,296 | 25,695,176 |
| of which payments not using 3D-Secure | 1,134,682 | 26.9 | 52,939,438 | 31.9 | 4,213,280 | 165,742,266 |
| Withdrawals | 5,044 | 4.1 | 939,726 | 2.2 | 123,574 | 43,148,054 |
| Total | 1,355,597 | 19.9 | 80,798,082 | 17.4 | 6,816,562 | 463,733,877 |

Source: Observatory for the Security of Payment Means.

Note: ATM, automatic teller machine.

T9 Payments by card issued and accepted in France – Domestic transactions

(volume in thousands, value in EUR thousands)

| | 2017 | | 2018 | | 2019 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 10,645,648 | 409,574,879 | 10,864,788 | 421,977,639 | 11,774,183 | 437,193,670 |
| of which contactless payments (including mobile payments) | 1,273,939 | 12,930,723 | 2,320,822 | 24,439,724 | 3,690,364 | 41,558,002 |
| of which mobile payments | 4,444 | 83,492 | 10,949 | 190,953 | 45,249 | 794,288 |
| Remote payments (excluding internet) | 26,290 | 2,072,306 | 34,893 | 2,707,270 | 34,859 | 2,773,069 |
| Internet payments | 1,268,072 | 80,134,150 | 1,515,988 | 97,756,554 | 1,768,890 | 109,593,147 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 1,428,580 | 128,325,480 | 1,385,723 | 129,786,224 | 1,339,625 | 130,198,441 |
| Total | 13,368,590 | 620,106,815 | 13,801,392 | 652,227,686 | 14,917,558 | 679,758,326 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T9 Payments by card issued and accepted in France – Domestic transactions (continued)

(volume in thousands, value in EUR thousands)

| | 2020 | | 2021 | | 2022 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 10,978,602 | 413,760,411 | 12,611,966 | 460,274,895 | 14,340,211 | 514,159,801 |
| of which contactless payments (including mobile payments) | 5,081,519 | 78,386,853 | 7,202,992 | 121,694,861 | 8,781,813 | 141,160,469 |
| of which mobile payments | 126,945 | 2,687,300 | 348,251 | 7,390,633 | 808,622 | 17,132,553 |
| Remote payments (excluding internet) | 60,243 | 5,428,918 | 56,236 | 5,540,339 | 87,602 | 13,259,829 |
| Internet payments | 2,011,431 | 122,128,921 | 2,399,865 | 142,184,895 | 2,393,161 | 146,642,890 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | 661,960 | 72,184,112 | 809,038 | 88,956,221 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | 389,530 | 15,797,723 | 717,916 | 24,981,800 |
| of which payments not using 3D-Secure | n/a | n/a | 1,348,375 | 54,203,060 | 866,207 | 32,704,868 |
| Withdrawals | 1,038,647 | 112,337,533 | 1,056,936 | 119,485,544 | 1,101,989 | 128,161,781 |
| Total | 14,088,924 | 653,655,783 | 16,125,003 | 727,485,673 | 17,922,963 | 802,224,301 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.



T9 bis Payments by card issued in France and accepted in the European Economic Area – European transactions



T9 ter Payments by card issued in France and accepted abroad outside the European Economic Area – International transactions

T10 Fraudulent card transactions issued and accepted in France – Domestic transactions

(volume in units, value in EUR, rate in percentage)

| | 2017 | | | 2018 | | | 2019 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 746,547 | 35,781,960 | 0.009 | 977,654 | 41,383,109 | 0.010 | 1,069,418 | 44,175,058 | 0.010 |
| of which contactless payments (including mobile payments) | 240,293 | 2,667,829 | 0.021 | 426,713 | 4,967,274 | 0.020 | 582,050 | 7,912,021 | 0.019 |
| of which mobile payments | 0 | 0 | 0.000 | 1,717 | 50,491 | 0.026 | 3,215 | 197,048 | 0.025 |
| Remote payments (excluding internet) | 99,860 | 7,406,798 | 0.357 | 159,916 | 9,512,197 | 0.351 | 64,113 | 7,498,207 | 0.270 |
| Internet payments | 2,279,763 | 148,652,859 | 0.186 | 2,180,379 | 163,824,893 | 0.168 | 2,630,697 | 183,067,879 | 0.167 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 121,686 | 34,181,829 | 0.027 | 109,924 | 30,893,412 | 0.024 | 122,260 | 35,935,625 | 0.028 |
| Total | 3,247,856 | 226,023,446 | 0.036 | 3,427,873 | 245,613,611 | 0.038 | 3,886,488 | 270,676,769 | 0.040 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T10 Fraudulent card transactions issued and accepted in France – Domestic transactions (continued)

(volume in units, value in EUR, rate in percentage)

| | 2020 | | | 2021 | | | 2022 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 793,350 | 36,280,495 | 0.009 | 825,325 | 43,515,617 | 0.009 | 989,454 | 53,593,598 | 0.010 |
| of which contactless payments (including mobile payments) | 522,873 | 10,502,092 | 0.013 | 576,537 | 14,002,613 | 0.012 | 754,985 | 20,231,615 | 0.014 |
| of which mobile payments | 29,807 | 2,447,707 | 0.091 | 75,039 | 4,801,997 | 0.065 | 152,726 | 9,566,583 | 0.056 |
| Remote payments (excluding internet) | 74,832 | 8,964,315 | 0.165 | 77,941 | 10,604,251 | 0.191 | 120,708 | 24,857,056 | 0.187 |
| Internet payments | 2,847,769 | 212,962,645 | 0.174 | 2,577,337 | 191,873,234 | 0.135 | 1,874,565 | 145,299,292 | 0.099 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | 267,556 | 69,544,332 | 0.096 | 314,967 | 72,922,674 | 0.082 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | 159,344 | 11,208,886 | 0.071 | 342,714 | 17,460,124 | 0.070 |
| of which payments not using 3D-Secure | n/a | n/a | n/a | 2,150,437 | 111,120,015 | 0.205 | 1,216,884 | 54,916,494 | 0.168 |
| Withdrawals | 102,962 | 32,477,429 | 0.029 | 121,642 | 41,437,842 | 0.035 | 115,643 | 41,344,934 | 0.032 |
| Total | 3,818,913 | 290,684,884 | 0.044 | 3,602,245 | 287,430,944 | 0.040 | 3,100,370 | 265,094,880 | 0.033 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.



T10 bis Fraudulent transactions using cards issued in France and accepted in the European Economic Area – European transactions



T10 ter Fraudulent transactions using cards issued in France and accepted abroad outside the European Economic Area – International transactions

T11 Breakdown of remote payment fraud by sector of activity on domestic transactions in 2022 (volume in units, value in EUR, rate in volume per thousand, rate in value in percentage)

| | Transactions | | Fraud | | Fraud rate | |
|--|----------------------|------------------------|------------------|--------------------|--------------|--------------|
| | Volume | Value | Volume | Value | Volume (‰) | Value (%) |
| Generalist and semi-generalist trade | 720,160,645 | 40,673,352,376 | 371,145 | 35,781,047 | 0.515 | 0.088 |
| Technical and cultural products (books, DVDs, IT, hi-fi, photo, video, household appliances, etc.) | 121,950,525 | 5,149,814,732 | 212,055 | 14,750,850 | 1.739 | 0.286 |
| Travel, transportation | 238,518,682 | 21,923,769,597 | 190,628 | 17,283,633 | 0.799 | 0.079 |
| Telephony and communication | 401,318,250 | 14,910,099,186 | 325,588 | 15,324,085 | 0.811 | 0.103 |
| Food | 32,482,983 | 2,109,085,070 | 13,718 | 1,029,111 | 0.422 | 0.049 |
| Household equipment, furnishings, DIY | 65,076,308 | 10,893,000,558 | 35,615 | 13,859,215 | 0.547 | 0.127 |
| Insurance | 12,266,930 | 2,497,700,204 | 3,564 | 529,667 | 0.291 | 0.021 |
| Health, beauty, hygiene | 37,868,213 | 2,428,226,279 | 25,961 | 2,307,096 | 0.686 | 0.095 |
| Services for individuals and professionals | 480,090,010 | 34,617,354,164 | 635,812 | 39,595,894 | 1.324 | 0.114 |
| Supplying an account, selling from one person to another | 121,276,878 | 11,359,213,472 | 102,306 | 20,160,930 | 0.844 | 0.177 |
| Online games | 113,174,813 | 3,697,908,887 | 49,613 | 3,588,319 | 0.438 | 0.097 |
| Other | 136,578,925 | 9,643,194,626 | 29,268 | 5,946,501 | 0.214 | 0.062 |
| Total | 2,480,763,162 | 159,902,719,151 | 1,995,273 | 170,156,348 | 0.804 | 0.106 |

Source: Observatory for the Security of Payment Means.

CARD: ACCEPTANCE

T12 Payments by card accepted in France (volume in thousands, value in EUR thousands)

| | 2017 | | 2018 | | 2019 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 11,076,238 | 440,943,480 | 11,286,513 | 453,608,003 | 12,277,149 | 468,895,511 |
| of which contactless payments (including mobile payments) | 1,302,753 | 13,537,550 | 2,370,247 | 25,007,584 | 3,802,953 | 42,931,374 |
| of which mobile payments | 6,120 | 113,383 | 11,911 | 209,710 | 56,169 | 1,014,657 |
| Remote payments (excluding internet) | 41,561 | 4,979,261 | 50,543 | 5,757,108 | 48,998 | 5,586,755 |
| Internet payments | 1,357,351 | 90,511,610 | 1,652,894 | 112,607,104 | 1,906,065 | 121,920,272 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 1,459,903 | 134,099,783 | 1,418,919 | 136,201,131 | 1,375,145 | 136,636,741 |
| Total | 13,935,054 | 670,534,135 | 14,408,869 | 708,173,346 | 15,607,358 | 733,039,279 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T12 Payments by card accepted in France (continued) (volume in thousands, value in EUR thousands)

| | 2020 | | 2021 | | 2022 | |
|---|-------------------|--------------------|-------------------|--------------------|-------------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value |
| Proximity and ATM payments | 11,284,433 | 428,180,387 | 13,031,098 | 480,804,099 | 15,093,611 | 551,753,133 |
| of which contactless payments (including mobile payments) | 5,187,488 | 79,877,184 | 7,437,197 | 125,344,168 | 9,248,429 | 149,971,446 |
| of which mobile payments | 145,527 | 2,979,437 | 388,175 | 8,403,747 | 897,307 | 19,846,999 |
| Remote payments (excluding internet) | 69,950 | 7,087,913 | 64,620 | 7,272,724 | 107,228 | 18,523,094 |
| Internet payments | 2,158,226 | 132,554,575 | 2,565,276 | 155,816,405 | 2,589,260 | 166,197,062 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | 708,194 | 78,650,830 | 871,961 | 99,937,461 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | 409,008 | 18,152,505 | 748,083 | 27,403,752 |
| of which payments not using 3D-Secure | n/a | n/a | 1,448,074 | 59,013,071 | 969,216 | 38,855,848 |
| Withdrawals | 1,062,376 | 116,986,747 | 1,083,643 | 125,105,264 | 1,134,543 | 134,637,455 |
| Total | 14,574,985 | 684,809,622 | 16,744,636 | 768,998,491 | 18,924,643 | 871,110,743 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

↓ T12 bis Payments by card issued in the European Economic Area and accepted in France – European transactions

↓ T12 ter Payments by card issued outside the European Economic Area and accepted in France – International transactions

T13 Fraudulent transactions using cards accepted in France

(volume in units, value in EUR, rate in percentage)

| | 2017 | | | 2018 | | | 2019 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 837,148 | 55,604,789 | 0.0126 | 1,064,889 | 58,485,280 | 0.0129 | 1,170,399 | 64,448,538 | 0.0137 |
| of which contactless payments (including mobile payments) | 243,839 | 2,734,977 | 0.0202 | 438,088 | 5,174,314 | 0.0207 | 602,309 | 8,534,090 | 0.0199 |
| of which mobile payments | 377 | 30,488 | 0.0269 | 1,915 | 64,599 | 0.0308 | 3,890 | 307,230 | 0.0303 |
| Remote payments (excluding internet) | 175,974 | 36,078,041 | 0.7246 | 206,957 | 27,274,865 | 0.4738 | 108,259 | 23,167,505 | 0.4147 |
| Internet payments | 2,597,284 | 204,928,799 | 0.2264 | 2,537,264 | 225,819,184 | 0.2005 | 2,989,333 | 232,763,441 | 0.1909 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| of which payments not using 3D-Secure | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Withdrawals | 127,560 | 35,741,778 | 0.0267 | 114,727 | 32,353,075 | 0.0238 | 127,005 | 37,354,814 | 0.0273 |
| Total | 3,737,966 | 332,353,407 | 0.0496 | 3,923,837 | 343,932,404 | 0.0486 | 4,394,996 | 357,734,298 | 0.0488 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.

T13 Fraudulent transactions using cards accepted in France (continued)

(volume in units, value in EUR, rate in percentage)

| | 2020 | | | 2021 | | | 2022 | | |
|---|------------------|--------------------|---------------------|------------------|--------------------|---------------------|------------------|--------------------|---------------------|
| | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value | Volume | Value | Fraud rate by value |
| Proximity and ATM payments | 841,280 | 42,883,367 | 0.0100 | 874,166 | 49,441,754 | 0.0103 | 1,084,701 | 67,409,965 | 0.0122 |
| of which contactless payments (including mobile payments) | 538,313 | 12,238,895 | 0.0153 | 601,803 | 15,600,613 | 0.0124 | 819,535 | 24,406,015 | 0.0163 |
| of which mobile payments | 35,968 | 3,640,684 | 0.1222 | 84,421 | 5,793,427 | 0.0689 | 170,752 | 12,007,511 | 0.0605 |
| Remote payments (excluding internet) | 105,972 | 17,644,315 | 0.2489 | 96,257 | 15,211,163 | 0.2092 | 144,965 | 35,446,137 | 0.1914 |
| Internet payments | 3,176,400 | 248,966,265 | 0.1878 | 2,885,920 | 227,162,875 | 0.1458 | 2,252,283 | 190,461,573 | 0.1146 |
| of which 3D-Secure payments with strong authentication | n/a | n/a | n/a | 306,265 | 76,891,633 | 0.0978 | 346,366 | 80,959,973 | 0.0810 |
| of which 3D-Secure payments without strong authentication | n/a | n/a | n/a | 213,403 | 20,406,481 | 0.1124 | 405,445 | 26,105,266 | 0.0953 |
| of which payments not using 3D-Secure | n/a | n/a | n/a | 2,366,252 | 129,864,761 | 0.2201 | 1,500,472 | 83,396,334 | 0.2146 |
| Withdrawals | 104,960 | 33,084,175 | 0.0283 | 124,077 | 42,256,276 | 0.0338 | 120,217 | 42,811,637 | 0.0318 |
| Total | 4,228,612 | 342,578,122 | 0.0500 | 3,980,420 | 334,072,068 | 0.0434 | 3,602,166 | 336,129,312 | 0.0386 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available; ATM, automatic teller machine.



Fraudulent transactions by card issued and accepted in France – Domestic transactions, see T10

 **T13 bis** Fraudulent transactions using cards issued in the European Economic Area and accepted in France – European transactions

 **T13 ter** Fraudulent transactions using cards issued in France and accepted abroad outside the European Economic Area and accepted in France – International transactions

 **T13 quater** Types of fraud for payments by card accepted in France in 2022

 **T13 quinquies** Geographic distribution of fraud on cards accepted in France in 2022

CHEQUE

T14 Cheques exchanged

(volume in millions, value in EUR billions, average value in EUR)

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|----------------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Volume | 1,926.8 | 1,746.9 | 1,586.5 | 1,175.5 | 1,105.8 | 1,008.0 |
| Value | 1,002.0 | 891.1 | 814.5 | 614.2 | 588.6 | 539.8 |
| Average value | 520.0 | 510.1 | 513.4 | 522.5 | 532.3 | 535.5 |

Source: Observatory for the Security of Payment Means.



T14 bis Detailed volume of cheques exchanged

T15 Cheque fraud

(volume in units, value and average value in EUR, volume rate per thousand, value rate in percentage)

a) Old methodology

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|----------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| Volume | 114,906 | 166,421 | 183,488 | 220,685 | 272,970 | 266,216 |
| Fraud rate (‰) | 0.060 | 0.095 | 0.116 | 0.188 | 0.247 | 0.264 |
| Value | 296,072,847 | 450,108,464 | 539,215,175 | 538,059,139 | 625,703,442 | 556,796,815 |
| Fraud rate (%) | 0.030 | 0.051 | 0.066 | 0.088 | 0.106 | 0.103 |
| Average value | 2,577 | 2,705 | 2,939 | 2,438 | 2,292 | 2,092 |

b) New methodology

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|----------------------|------------|------------|------------|--------------------|--------------------|--------------------|
| Volume | n/a | n/a | n/a | 190,001 | 232,277 | 218,122 |
| Fraud rate (‰) | | | | 0.162 | 0.210 | 0.216 |
| Value | n/a | n/a | n/a | 401,611,189 | 465,021,167 | 395,416,196 |
| Fraud rate (%) | | | | 0.065 | 0.079 | 0.073 |
| Average value | n/a | n/a | n/a | 2,114 | 2,002 | 1,813 |

Source: Observatory for the Security of Payment Means.

Notes: The old methodology took into account any cheque transaction settled and rejected for fraudulent reasons. The new methodology to cheque fraud excludes frauds that are thwarted after the cheque has been presented and settled.

n/a, not available.

T16 Types of cheque fraud

(volume in units, value in EUR, share in percentage)

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | |
|-------------------------|------------------|-------|------------------|-------|------------------|-------|------------------|-------|------------------|-------|------------------|-------|
| | Number/ value | Share | Number/ value | Share | Number/ value | Share | Number/ value | Share | Number/ value | Share | Number/ value | Share |
| Volume | | | | | | | | | | | | |
| Theft, loss | 89,988 | 78.3 | 138,358 | 83.1 | 154,211 | 84.0 | 196,754 | 89.2 | 244,750 | 89.7 | 237,854 | 89.3 |
| Forgery | 15,738 | 13.7 | 17,178 | 10.3 | 16,459 | 9.0 | 13,894 | 6.3 | 18,074 | 6.6 | 18,885 | 7.1 |
| Counterfeit | 7,234 | 6.3 | 8,092 | 4.9 | 9,574 | 5.2 | 7,207 | 3.3 | 5,119 | 1.9 | 5,969 | 2.2 |
| Misappropriation, reuse | 1,946 | 1.7 | 2,793 | 1.7 | 3,244 | 1.8 | 2,830 | 1.3 | 5,026 | 1.8 | 3,508 | 1.3 |
| Value | | | | | | | | | | | | |
| Theft, loss | 130,815,653 | 44.2 | 252,890,727 | 56.2 | 296,367,562 | 55.0 | 365,813,764 | 68.0 | 398,739,224 | 63.7 | 375,576,575 | 67.5 |
| Forgery | 127,157,212 | 42.9 | 145,737,424 | 32.4 | 145,881,745 | 27.1 | 102,801,337 | 19.1 | 100,395,756 | 16.0 | 93,152,894 | 16.7 |
| Counterfeit | 28,097,173 | 9.5 | 36,739,051 | 8.2 | 76,511,582 | 14.2 | 32,340,420 | 6.0 | 33,725,041 | 5.4 | 32,648,566 | 5.9 |
| Misappropriation, reuse | 10,002,809 | 3.4 | 14,741,262 | 3.3 | 20,454,286 | 3.8 | 37,103,618 | 6.9 | 92,823,421 | 14.8 | 55,418,781 | 10.0 |

Source: Observatory for the Security of Payment Means.

Note: The breakdown of cheque fraud by type is based on the old methodology, which covers any cheque transaction settled and flagged for fraudulent reasons.

CREDIT TRANSFER

T17 Breakdown of transfers issued by type of transfer

(volume in millions, value in EUR millions)

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | |
|--|--------------|-------------------|--------------|-------------------|--------------|-------------------|--------------|-------------------|--------------|-------------------|--------------|-------------------|
| | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value |
| Total | 3,870 | 24,069,448 | 4,038 | 24,211,142 | 4,251 | 25,879,217 | 4,483 | 32,713,128 | 4,843 | 38,722,734 | 5,158 | 38,894,879 |
| of which SEPA transfers – SCT | 3,801 | 9,259,478 | 3,974 | 10,846,914 | 4,174 | 9,602,866 | 4,384 | 10,029,108 | 4,668 | 12,980,883 | 4,689 | 9,655,892 |
| of which instant SEPA transfers – SCT Inst | n/a | n/a | 0 | 86 | 14 | 7,074 | 45 | 26,243 | 107 | 50,053 | 198 | 118,972 |
| of which large value transfers – LVT ^{a)} | 10 | 9,483,487 | 10 | 10,130,586 | 9 | 12,266,316 | 9 | 19,042,030 | 9 | 19,661,685 | 19 | 15,907,892 |
| of which other transfers | 59 | 5,326,483 | 53 | 3,233,556 | 54 | 4,002,960 | 45 | 3,615,748 | 59 | 6,030,114 | 252 | 13,212,124 |
| Total – excluding LVT | 3,860 | 14,585,961 | 4,028 | 14,080,556 | 4,242 | 13,612,900 | 4,474 | 13,671,098 | 4,834 | 19,061,050 | 5,138 | 22,986,988 |

a) These are large value transfers (LVT) made via Target 2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA – Single Euro Payments Area; n/a – not available.



T17 bis Breakdown of transfers issued by initiation channel



T17 ter Breakdown of transfers issued by geographic destination

T18 Breakdown of fraudulent transactions by transfer type

(volume in units, value in EUR, rate in percentage)

| | 2017 | | | 2018 | | | 2019 | | |
|--|--------------|-------------------|---------------|--------------|-------------------|---------------|---------------|--------------------|---------------|
| | Volume | Value | | Volume | Value | | Volume | Value | |
| | | Value | Fraud rate | | Value | Fraud rate | | Value | Fraud rate |
| Total | 4,642 | 78,286,492 | 0.0003 | 7,736 | 97,327,128 | 0.0004 | 15,934 | 161,642,174 | 0.0006 |
| of which SEPA transfers – SCT | n/a | n/a | n/a | 6,521 | 78,314,614 | 0.0007 | 13,302 | 127,572,549 | 0.0013 |
| of which instant SEPA transfers – SCT Inst | n/a | n/a | n/a | 5 | 29,800 | 0.0345 | 729 | 2,203,240 | 0.0311 |
| of which large value transfers – LVT ^{a)} | n/a | n/a | n/a | 14 | 4,622,598 | 0.0000 | 15 | 15,476,053 | 0.0001 |
| of which other transfers | n/a | n/a | n/a | 1,196 | 14,360,116 | 0.0004 | 1,888 | 16,390,332 | 0.0004 |
| Total – excluding LVT | n/a | n/a | n/a | 7,722 | 92,704,530 | 0.0007 | 15,919 | 146,166,121 | 0.0011 |

a) These are large value transfers (LVT) made via Target 2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA – Single Euro Payments Area.

T18 Breakdown of fraudulent transactions by transfer type (continued)

(volume in units, value in EUR, rate in percentage)

| | 2020 | | | 2021 | | | 2022 | | |
|--|---------------|--------------------|---------------|---------------|--------------------|---------------|---------------|--------------------|---------------|
| | Volume | Value | | Volume | Value | | Volume | Value | |
| | | Value | Fraud rate | | Value | Fraud rate | | Value | Fraud rate |
| Total | 35,893 | 266,969,099 | 0.0008 | 46,718 | 287,264,068 | 0.0007 | 76,846 | 313,163,442 | 0.0008 |
| of which SEPA transfers – SCT | 25,254 | 191,474,396 | 0.0019 | 33,199 | 246,527,533 | 0.0019 | 40,874 | 205,737,587 | 0.0021 |
| of which instant SEPA transfers – SCT Inst | 7,131 | 10,562,419 | 0.0402 | 12,913 | 22,406,942 | 0.0448 | 33,193 | 52,768,218 | 0.0444 |
| of which large value transfers – LVT ^{a)} | 51 | 2,439,224 | 0.0000 | 5 | 1,539,120 | 0.0000 | 49 | 1,934,774 | 0.0000 |
| of which other transfers | 3,457 | 62,493,060 | 0.0017 | 601 | 16,790,473 | 0.0003 | 2,730 | 52,722,863 | 0.0004 |
| Total – excluding LVT | 35,842 | 264,529,875 | 0.0019 | 46,713 | 285,725,443 | 0.0015 | 76,797 | 311,228,668 | 0.0014 |

a) These are large value transfers (LVT) made via Target 2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA – Single Euro Payments Area.



T18 bis Breakdown of fraudulent transactions by transfer initiation channel



T18 ter Breakdown of fraudulent transactions by geographical destination of transfers

T19 Totals for transfer fraud

(volume in units, value and average value in EUR, volume rate per thousand, value rate in percentage)

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|----------------------|-------------------|-------------------|--------------------|--------------------|--------------------|--------------------|
| Volume | 4,642 | 7,736 | 15,934 | 35,893 | 46,718 | 76,846 |
| Rate (‰) | 0.0012 | 0.0019 | 0.0037 | 0.0080 | 0.0096 | 0.0149 |
| Value | 78,286,492 | 97,327,128 | 161,642,174 | 266,969,099 | 287,264,068 | 313,163,442 |
| Rate (%) | 0.0003 | 0.0004 | 0.0006 | 0.0008 | 0.0007 | 0.0008 |
| Average value | 16,865 | 12,581 | 10,144 | 7,438 | 6,149 | 4,075 |

Source: Observatory for the Security of Payment Means.

T20 Breakdown of transfer fraud by type

(volume in units, value in EUR, share in percentage)

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | |
|----------------------------|--------------|-------------------|--------------|-------------------|---------------|-------------------|---------------|--------------------|---------------|--------------------|---------------|--------------------|
| | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value |
| Deceit | 3,803 | 42,008,522 | 5,525 | 51,069,661 | 13,769 | 98,525,485 | 28,211 | 87,061,255 | 35,865 | 87,370,131 | 57,443 | 120,006,990 |
| Share | 81.9 | 53.7 | 71.4 | 52.5 | 86.4 | 61.0 | 78.6 | 32.6 | 76.8 | 30.4 | 74.8 | 38.3 |
| Forgery | 57 | 1,304,143 | 151 | 485,131 | 125 | 3,438,923 | 203 | 3,377,807 | 875 | 5,387,862 | 179 | 2,838,371 |
| Share | 1.2 | 1.7 | 2.0 | 0.5 | 1.6 | 2.1 | 0.6 | 1.3 | 1.9 | 1.9 | 0.2 | 0.9 |
| Misappropriation | 464 | 32,966,084 | 1,037 | 40,250,639 | 1,534 | 56,514,755 | 5,731 | 157,318,883 | 8,523 | 168,094,274 | 16,991 | 148,732,203 |
| Share | 10.0 | 42.1 | 13.4 | 41.4 | 19.8 | 35.0 | 16.0 | 58.9 | 18.2 | 58.5 | 22.1 | 47.5 |
| Others^{a)} | 318 | 2,007,743 | 1,023 | 5,521,697 | 506 | 3,163,011 | 1,748 | 19,211,154 | 1,455 | 26,411,801 | 2,233 | 41,585,878 |
| Share | 6.9 | 2.6 | 13.2 | 5.7 | 3.2 | 2.0 | 4.9 | 7.2 | 3.1 | 9.2 | 2.9 | 13.3 |

a) For 2021, the "other" category includes fraud involving transfers initiated by non-electronic means (mail, telephone, etc.).

Source: Observatory for the Security of Payment Means.

DIRECT DEBIT

T21 Breakdown of direct debits by type of order

(volume in millions, value EUR in millions)

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | |
|---|--------------|------------------|--------------|------------------|--------------|------------------|--------------|------------------|--------------|------------------|--------------|------------------|
| | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value |
| Total | 4 091 | 1 578 653 | 4 211 | 1 644 553 | 4 370 | 1 710 931 | 4 622 | 1 684 258 | 5 020 | 1 895 098 | 4 914 | 2 040 963 |
| Breakdown of direct debits by type of order | | | | | | | | | | | | |
| of which direct debits granted by electronic order | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | 1,106 | 430,781 | 1,357 | 1,045,754 |
| of which direct debits granted by paper money order | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | 3,914 | 1,464,317 | 3,558 | 995,210 |
| Breakdown of direct debits by initiation method | | | | | | | | | | | | |
| of which direct debits initiated from a file/batch | 4,029 | 1,526,056 | 4,151 | 1,609,405 | 4,312 | 1,672,338 | 4,560 | 1,647,504 | 4,936 | 1,819,420 | 4,645 | 1,929,438 |
| of which direct debits initiated on the basis of a single payment | 63 | 52,596 | 60 | 35,148 | 58 | 38,593 | 61 | 36,754 | 84 | 75,678 | 269 | 111,525 |

Source: Observatory for the Security of Payment Means.

Note: n/a, not available.



T21 bis Breakdown of direct debits by geographic origin of the payer

T22 Totals for direct debit fraud

(volume in units, value and average value in EUR, volume rate per thousand, value rate in percentage)

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|----------------------|------------------|-------------------|-------------------|------------------|-------------------|-------------------|
| Volume | 25,801 | 309,377 | 43,519 | 6,485 | 251,010 | 49,453 |
| Fraud rate (‰) | 0.0063 | 0.0735 | 0.0100 | 0.0014 | 0.0500 | 0.0101 |
| Value | 8,726,403 | 58,346,253 | 10,990,025 | 1,891,051 | 25,318,677 | 19,853,012 |
| Fraud rate (%) | 0.0006 | 0.0035 | 0.0006 | 0.0001 | 0.0013 | 0.0010 |
| Average value | 338 | 189 | 253 | 292 | 101 | 401 |

Source: Observatory for the Security of Payment Means.



T22 bis Breakdown of fraudulent direct debits by geographic origin of the payer



T22 ter Breakdown of fraudulent direct debits by type of order

T23 Types of cheque fraud

(volume in units, value in EUR, share in percentage)




| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | 2022 | |
|-------------------------|---------------|------------------|----------------|-------------------|---------------|------------------|--------------|------------------|----------------|-------------------|---------------|-------------------|
| | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value | Volume | Value |
| Deceit | 23,943 | 6,141,836 | 309,302 | 58,329,283 | 14,601 | 3,961,260 | 6,011 | 1,388,326 | 250,493 | 25,201,709 | 43,788 | 14,206,533 |
| Share | 92.8 | 70.4 | 100.0 | 100.0 | 33.6 | 36.0 | 92.7 | 73.4 | 99.8 | 99.5 | 88.5 | 71.6 |
| Misappropriation | 1,832 | 2,305,112 | 72 | 16,703 | 26,223 | 6,677,467 | 62 | 10,720 | 517 | 116,968 | 5665 | 5,646,479 |
| Share | 7.1 | 26.4 | 0.0 | 0.0 | 60.3 | 60.8 | 1.0 | 0.6 | 0.2 | 0.5 | 11.5 | 28.4 |

Source: Observatory for the Security of Payment Means.

Note: Until 2020, direct debit fraud contained two other typologies, «Forgery» and «Other», which explains why the breakdown of the data in this report does not always represent 100% of fraud in the years before 2020.

OTHER



Electronic money

-  T24 Number of supports provided by service providers approved or established in France
-  T25 Use of electronic money by type of transaction
-  T26 Fraudulent electronic money transactions

Commercial paper: "*lettre de change relevé*" (LCR, statement of bill of exchange) and "*billet à ordre*" (BOR, promissory note)

-  T27 Payments by LCR and BOR
-  T28 Types of fraud in the use of LCR and BOR

Money remittance

-  T29 Money remittance transactions
-  T30 Fraud in money remittance transactions

Payment initiation services

-  T31 Transactions initiated by institutions as Payment Initiation Service Providers (Payment Service 7 of Article 314-1 of the French Monetary and Financial Code)
-  T32 Fraudulent transactions initiated via an institution acting as a Payment Initiation Service Provider (Section 7 of Article 314-1 of the French Monetary and Financial Code)

Published by

Banque de France

Managing Editor

Érick Lacourrège

Director General Cash and Retail Payments

Banque de France

Editor-in-Chief

Alexandre Stervinou

Director Cash and Retail Payments Policy and Oversight

Banque de France

Editorial Secretariat

Pierre Bienvenu, Aurélie Barberet, Véronique Bugaj,
Caroline Corcy, Yolaine Fischer, Anne-Marie Fourel,
Trần Huynh, Marc-Antoine Jambu, Julien Lasalle,
Ibtissam Lesca, Isabelle Maranghi, Marine Soubielle

Technical production

Studio Création

Press and Communication Directorate

Contact

Observatory for the Security of Payment Means

Internal mail code: S2B-2323

31 rue Croix-des-Petits-Champs

75049 Paris Cedex 01

Legal deposit

July 2023

ISSN 2557-1230 (online version)

ISSN 2556-4536 (printed)

Internet

www.observatoire-paiements.fr

The *Annual Report of the Observatory for the Security of Payment Means* can be downloaded for free on the Banque de France's website (www.banque-france.fr).



www.banque-france.fr

