OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2024

BANQUE DE FRANCE
EUROSYSTÈME

Observatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2024

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 Denis Beau,
First Deputy Governor of the Banque de France,
President of the Observatory
for the Security of Payment Means

SEPTEMBER 2025

CONTENTS

Chapter 3 is available in French only in the original version of the report, which can be found here: ***https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2024***

SUMMARY

The ongoing increase in the use of innovative payment methods, such as instant credit transfers (10% of transfers issued) and payments by mobile (15% of point-of-sale card payments), continued to drive the take-up of cashless payment means in 2024, which were up 5.2% in terms of number of transactions and up 3.4% in terms of total transaction value.

Chapter 1 of this OSMP report highlights that alongside this development, annual fraud in value terms has remained stable since 2022 at just under the EUR 1.2 billion threshold, while fraud levels on the most commonly used payment channels have been satisfactorily contained:

- The fraud rate for **payment cards**, which are the main means of payment for everyday use, stabilised at their lowest ever recorded level for the third consecutive year (EUR 53 of fraud per EUR 100,000 of payments), with a particular improvement in the fraud rate for digital payments (mobile and e-commerce).

- The fraud rate for **credit transfers** continues to be very low overall (EUR 1 of fraud per EUR 100,000 of payments on average). The general public remains structurally more exposed than businesses and government agencies (at EUR 43 of fraud per EUR 100,000 of payments for transfers made via online banking), but the fraud rate is still lower than the rate for payment cards, including for instant credit transfers (EUR 46 of fraud per EUR 100,000 of payments).

- **Cheque** fraud declined by more than 25% in value terms, while cheque use fell in value terms by 16%, bringing the fraud rate on cheques down to its lowest level since 2021, at EUR 69 of fraud per EUR 100,000 of payments.

After two years between 2021 and 2023 of very sharp rises in **fraud involving manipulation** (known as social engineering), its share of total fraud by value stabilised in 2024 at 32%, or EUR 382 million.[1]

Chapter 2 presents the assessment drawn up by the Autorité de contrôle prudentiel et de résolution (ACPR – the French Prudential Supervision and Resolution Authority) and the Banque de France on the application of the recommendations published in April 2023 on fraud prevention and reimbursement in cases of fraud. This assessment, supported by previously unseen statistics, notes in particular a general strengthening of the security of the payment journey on the one hand, and an improvement in dispute handling procedures to better take into account the various technical and contextual parameters on the other. However, the authorities will remain vigilant in correcting certain residual practices, which must comply with regulations or take better account of the recommendations.

Chapter 3 provides an overview of the actions undertaken by the Observatory in terms of fraud prevention, which mainly include:

- The roll-out of an action plan to secure remote card payments made without the authentication provided by the 3-D Secure technical protocol, which combines collective measures to restrict the use of the most vulnerable channels and individual measures targeting the merchants that are most exposed to fraud. This action plan, which already contributed to improving the fraud rate for card payments over the internet in 2024, is set to continue in 2025 and 2026.

- Actions taken by the telecommunications sector to prevent identity theft via their networks – in particular, the effective roll-out in late 2024/early 2025 of the MAN (number authentication mechanism) programme, intended to ensure that caller ID numbers displayed when a telephone call is received are authentic – and the promotion of services to prevent fraudulent text messages.

- The clarification of certain Observatory recommendations to strengthen cheque security, particularly with regard to the delivery of chequebooks by post and the simplification of reporting and stop payment procedures in the event of loss or theft.

Chapter 4 reports on the Observatory's monitoring of the use of artificial intelligence and transaction scoring techniques for fraud prevention purposes. *It notably sets out the conditions for the success of these types of solutions in terms of data management and control for payment industry professionals.*

Against a backdrop of rapidly evolving payment methods and fraud techniques, ***the Observatory remains committed to ensuring the security of all payment methods, thereby guaranteeing genuine freedom of choice for all users, both individuals and businesses, in their day-to-day transactions****. As part of its work programme for 2025-26, the Observatory will particularly direct its technology monitoring activities towards the security of payments using digital assets such as crypto-assets, including stablecoins. At the same time, it will pursue the fraud prevention initiatives undertaken in partnership with telecommunications sector players and, from a new perspective considering their importance, with digital sector stakeholders.*

[1] Fraud by manipulation, as measured by the Observatory, covers only scams involving the misappropriation of payment methods.
For the most part, these are cases where the fraudster manipulates the customer during a telephone conversation, often by impersonating the payment service provider (false bank advisor or fake anti-fraud service scams). The Observatory measures the extent of this fraud indirectly (through a proxy) through the sum of fraudulent transactions by payment card with strong authentication and by online bank transfer. However, scams in which the victim has authorised a payment to a fraudster (such as romance scams, fake e-commerce sites, subscription to a fake investment product or loan, etc.) are excluded from the Observatory's statistical scope.

THE USE OF MEANS OF PAYMENT IN 2024

EUR **34,864** BN EXCHANGED

+5.2%

INCREASE IN TRANSACTIONS USING CASHLESS MEANS OF PAYMENT COMPARED TO 2023

-16%

DECREASE IN PAYMENTS BY CHEQUE BY VALUE COMPARED TO 2023

62%

OF PAYMENTS MADE BY CARD

10%

OF CREDIT TRANSFERS MADE INSTANTLY

15%

OF POINT-OF-SALE CARD PAYMENTS ARE MADE USING A MOBILE WALLET

FRAUD TRENDS IN 2024

0.053%

CARD PAYMENT FRAUD RATE STABILISED AT A HISTORIC LOW

-74%

DECREASE IN THE FRAUD RATE FOR POINT-OF-SALE CARD PAYMENTS MADE USING A MOBILE WALLET SINCE 2022

-EUR 94 M

DECREASE IN FRAUDULENT CHEQUE TRANSACTIONS

EUR 1.189 BN

IN LOSSES

-0.6%

DECREASE IN FRAUD BY VALUE

0.046%

INSTANT CREDIT TRANSFER FRAUD RATE

EUR 382 M

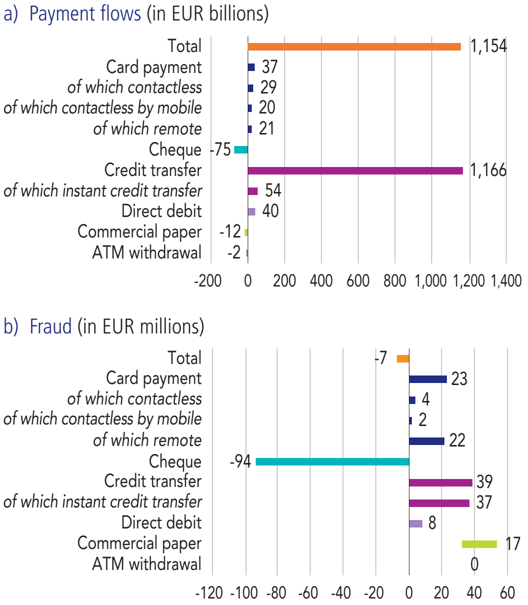
OF SOCIAL ENGINEERING FRAUD

1

FRAUD IN 2024

Key data

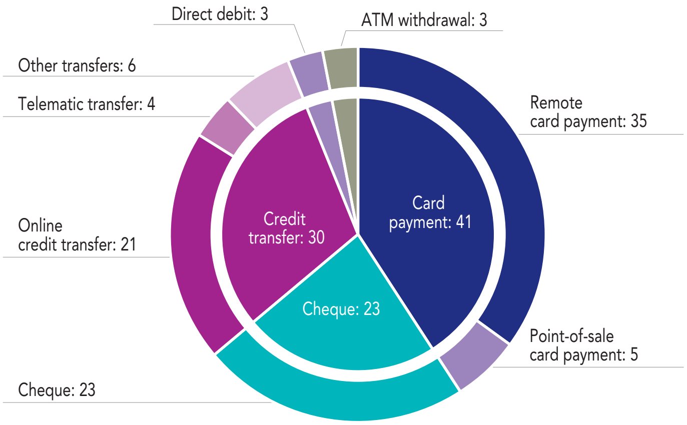
C1 Changes in means of payment between 2023 and 2024



Source: Observatory for the Security of Payment Means.

Note: ATM, automated teller machine.

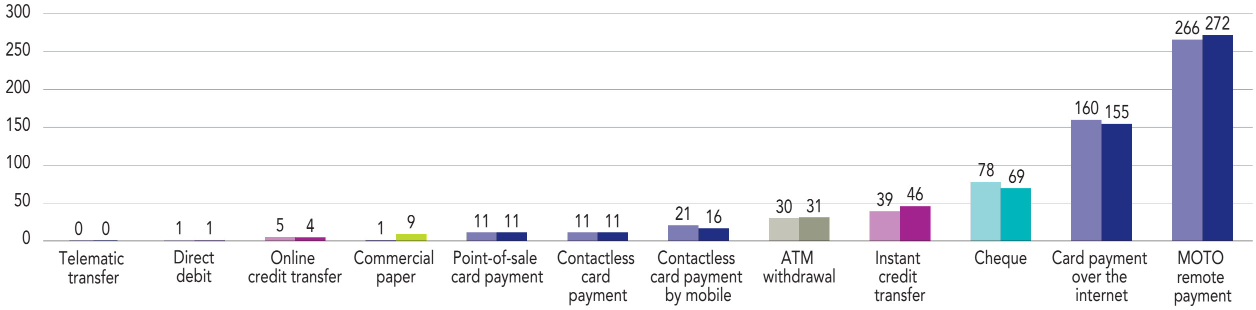
C2 Main sources of fraud in value terms (%)



Source: Observatory for the Security of Payment Means.

Note: ATM, automated teller machine.

C3 Vulnerability to fraud of the main payment channels in 2023 and 2024 (in EUR defrauded per EUR 100,000 of payments)



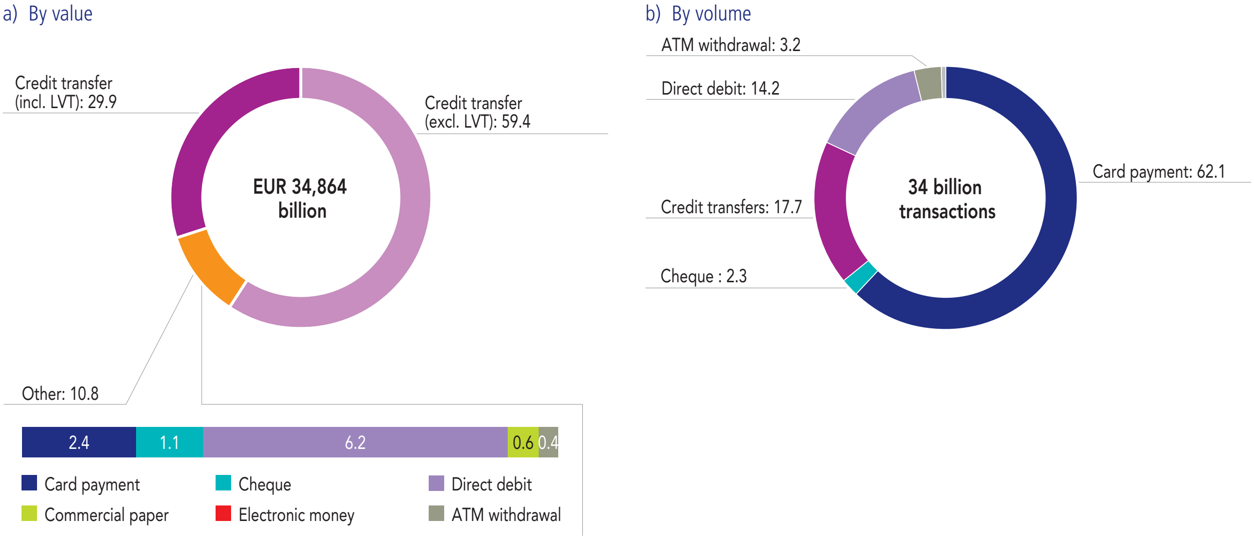
Source: Observatory for the Security of Payment Means.

Note: ATM, automated teller machine; MOTO, mail orders and telephone orders.

1.1 Overview

1.1.1 An overview of means of payment

C4 Use of cashless means of payment in 2024 (%)



a) By value

b) By volume

Source: Observatory for the Security of Payment Means.

Note: LVT, large-value transfer; ATM, automated teller machine.

Individuals, businesses and public authorities carried out 33.8 billion cashless payment transactions in 2024 (up 5.2% from 2023), with a total value of EUR 34,864 billion (up 3.4% from 2023).

While innovative approaches saw elevated growth rates, cheque use continued to fall: the value of cheque transactions decreased by 16%, and cheques accounted for just 2.3% of cashless transaction volumes.

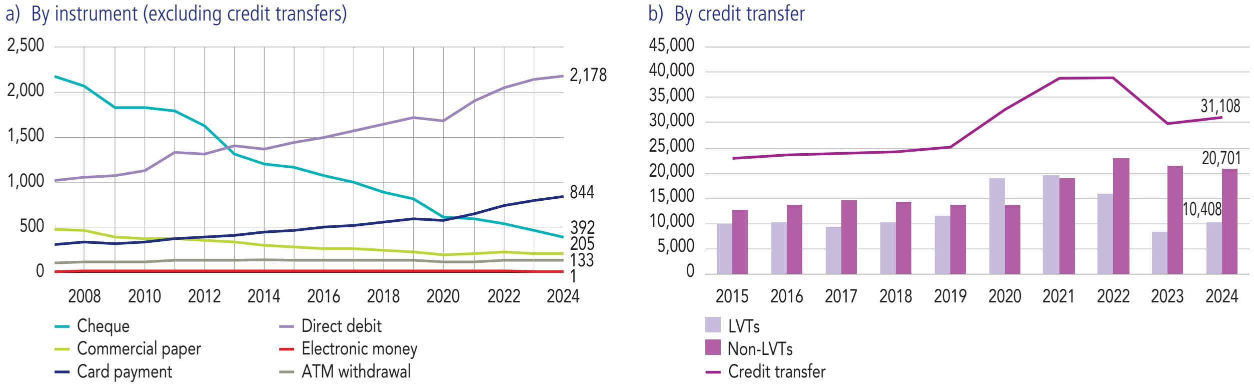
Credit transfers continued to account for the lion's share of total flows by value, retaining a steady share of 89%. Large-value transfers (LVTs) generated 30% of transferred values, but only 0.03% of transfer volumes. Instant credit transfers continued to increase rapidly (up 46% in volume terms and 31% by value) and accounted for 10% of all transfers by volume in 2024, compared with 7.3% in 2023.

Bankcards are still the preferred cashless payment method in France, and their use continues to increase. Their share of transaction volumes (excluding withdrawals) climbed from 61.4% in 2023 to 62.1% in 2024. Growth in the volume of contactless payment flows slowed, with an increase of 6% on 2023, compared with 19% between 2022 and 2023. However, payments by mobile phone continued to rise strongly as volumes expanded by 54% compared with 2023. As a result, mobile payments made up around 15% of point-of-sale (POS) payments in 2024, compared with 10% in 2023.

After years of stability, cash withdrawals by card fell slightly in 2024, decreasing by 4.2% in volume terms and 1.6% by value.

Direct debits followed the broad trend observed across all means of payment and rose by 3.7% in volume terms and 1.9% by value relative to 2023.

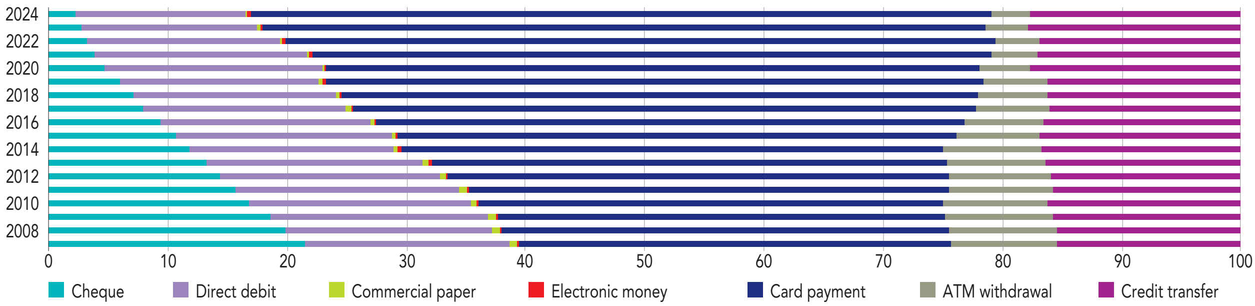
C5 Payment flows in value terms (in EUR billions)


a) By instrument (excluding credit transfers)

b) By credit transfer

Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine; LVT, large-value transfer.

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



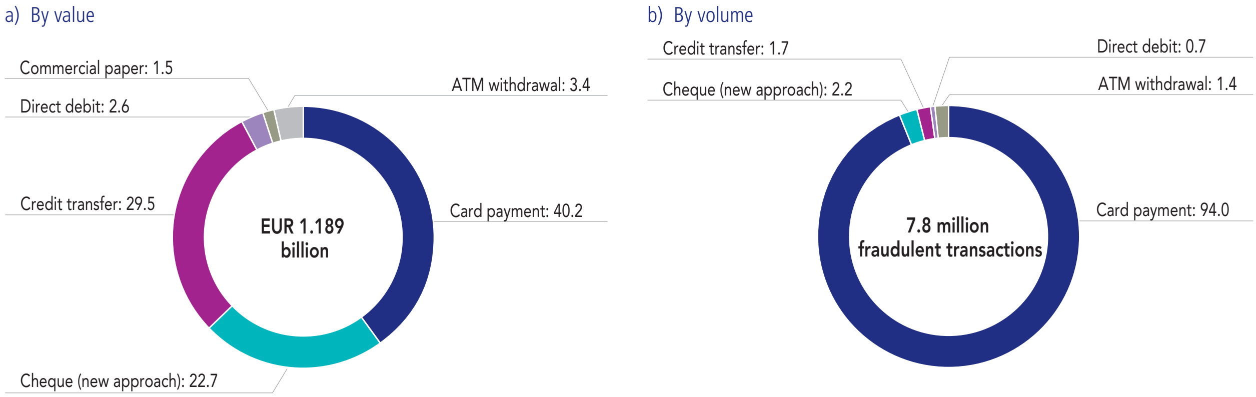
Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

1.1.2 Overview of means of payment fraud

Although cashless transactions increased in both volume and value terms, total fraud value was roughly steady at EUR 1.189 billion (down 0.6% compared with 2023). However, the number of fraudulent transactions rose by 9.3% to 7.8 million.

Based on the main trends observed, the main reasons for this stability were the EUR 93.6 million drop in cheque fraud, which far exceeded the decline in flows, offset by the EUR 39 million increase in credit transfer fraud (of which EUR 37 million for instant transfers) and the EUR 23 million increase in card fraud, essentially due to remote card payments (up EUR 22 million). Fraudulent cashing of trade bills (*lettres de change*), which targeted a few banks, accounted for the EUR 18 million in fraud in bills of exchange, which otherwise saw a 6% decrease in flows on 2023. Direct debit fraud rose by EUR 8 million, climbing by 36% compared with 2023.

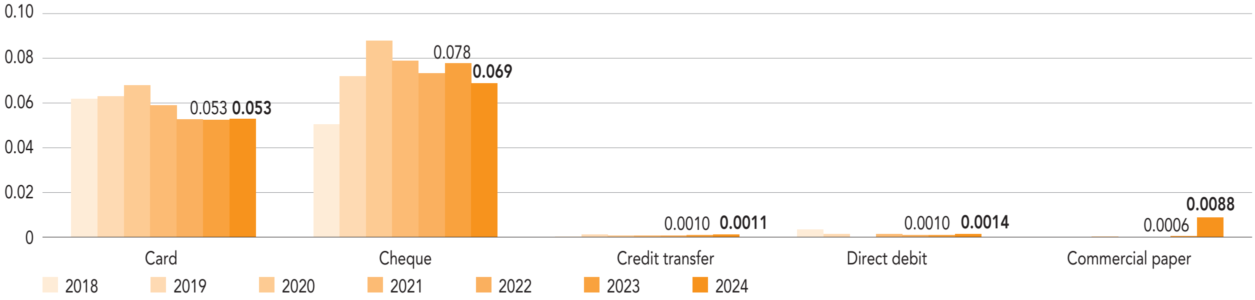
C7 Breakdown of fraud (%)


a) By value

b) By volume

Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

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



Source: Observatory for the Security of Payment Means.
Note: Since 2021, the cheque fraud rate has been calculated using a new approach, which excludes fraud that is thwarted after cheques have been presented and settled.

1.2 Payment card fraud

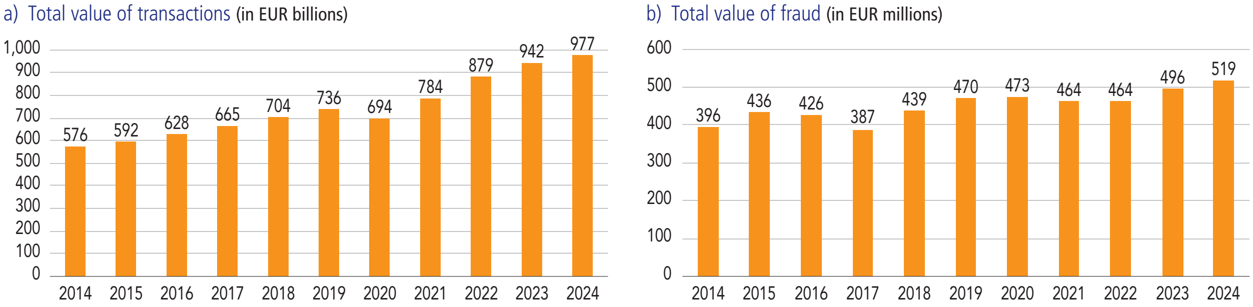
1.2.1 Overview – Cards issued in France

Payment cards remain the main means of payment for everyday use, with flows continuing to increase in 2024 in terms of both volume and value (6% and 4% respectively). Payments using mobile applications kept growing swiftly, increasing by 54% and accounting for 15% of POS payments.

Fraud totalled EUR 519 million, echoing the increase in flows and rising by 4.6% compared with 2023. Internet card payments remain the most exposed channel, representing 72% of fraud in terms of value, but only 25% of the total volumes exchanged.

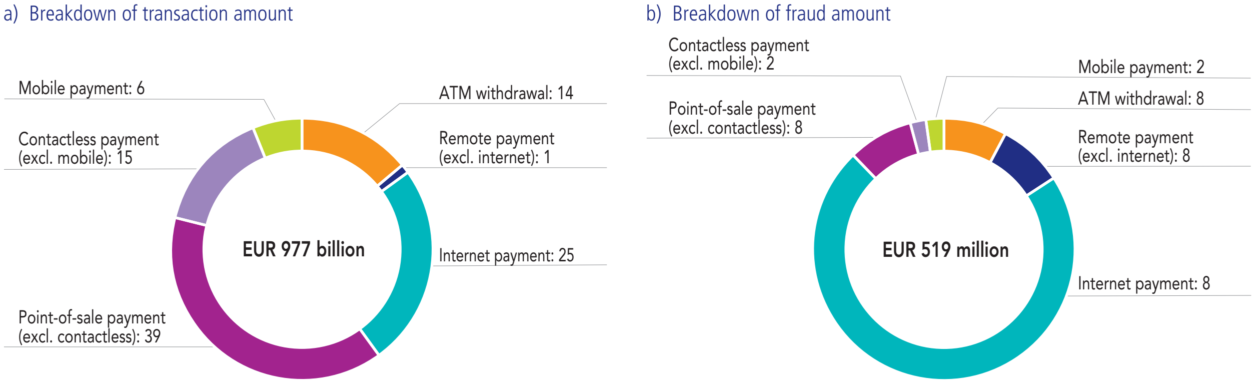
Card safety continues to benefit from the application of strong authentication to remote transactions as well as from ongoing improvements to the fraud detection tools used by members of the payment ecosystem. After falling by close to 10% over two consecutive years in 2021 and 2022, the fraud rate on card payments in France stabilised at 0.053% in 2024, remaining at its lowest level ever. Whereas POS payments and cash withdrawals continue to display low and stable fraud rates (0.011% for the former and 0.031% for the latter), the fraud rate for internet payments fell again, declining to 0.155% in 2024 from 0.160% in 2023.

C9 Cards issued in France in 2024



Source: Observatory for the Security of Payment Means.

C10 Use of cards issued in France by payment initiation channel in 2024 (%)

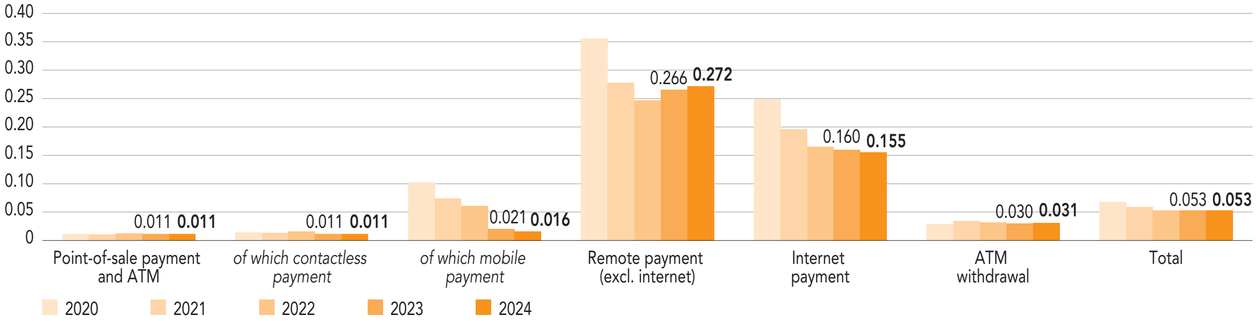


Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

This may reflect the first fruits of the Observatory's action plan in this area, together with efforts deployed by the payment ecosystem as a whole. The fraud rate for remote payments excluding the internet, which include payments for which customers share their payment card information via mail orders and telephone orders (MOTO), increased for the second year in a row (0.272% in 2024, compared with 0.266% in 2023 and 0.247% in 2022). The OSMP's plan has however driven a 6% decrease in the amounts exchanged via this channel, along with a virtually identical decline in fraud (down 4% to EUR 40 million).

The fraud rate for mobile payments fell again, declining by 22% in 2024 relative to 2023, after falling by two-thirds in 2023. Part of a long-term shift, this trend is directly linked to improved checks on user enrolment in mobile payment solutions through the systematic use of strong customer authentication, following a reminder about the regulatory requirements of the European Banking Authority and the Observatory in this area. These improvements are especially significant because this payment means has soared in popularity over recent years: its use has increased seven-fold since 2021 and it accounted for 15% of the total number of POS card payments in 2024.

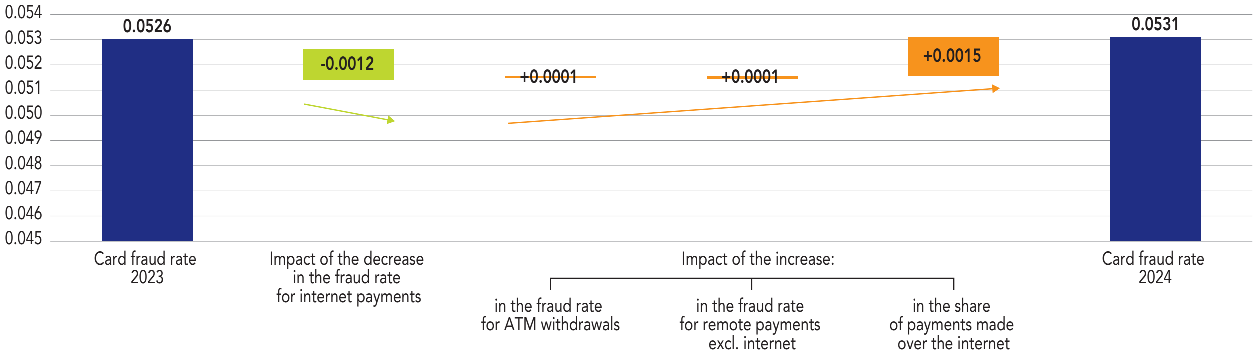
C11 Changes in fraud rates on French cards in value terms, by payment initiation channel (%)



Source: Observatory for the Security of Payment Means.

Note: ATM, automated teller machine.

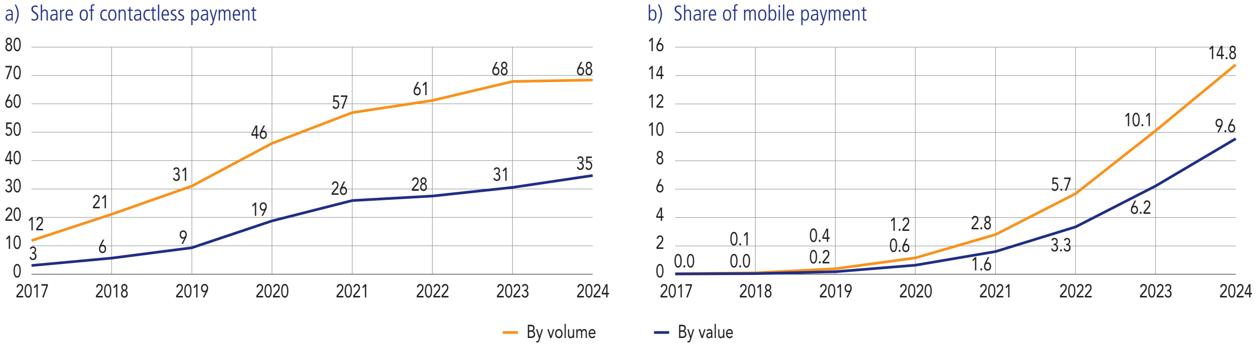
C11 *bis* Impact of changes in fraud rates by channel on the overall fraud rate (%)



Source: Observatory for the Security of Payment Means.

Note: ATM, automated teller machine.

C12 Card payment at point of sale (%)



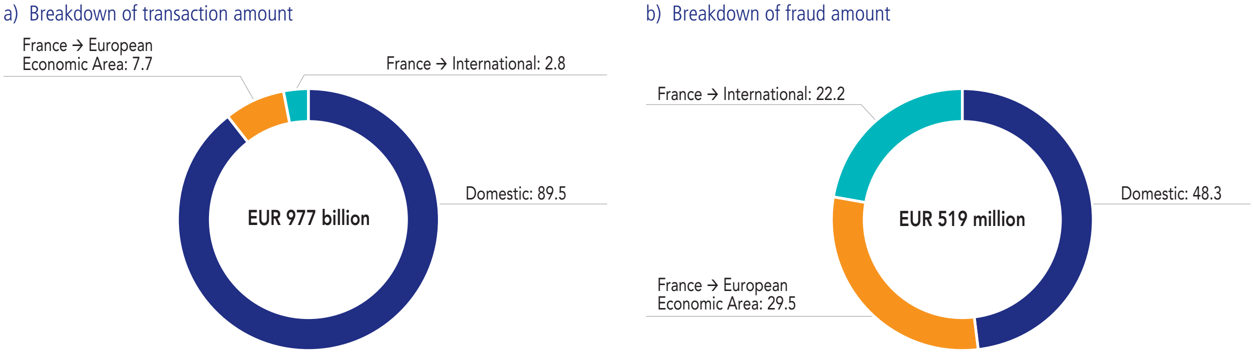
a) Share of contactless payment

b) Share of mobile payment

Source: Observatory for the Security of Payment Means.

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

C13 Cards issued in France by geographical area (%)

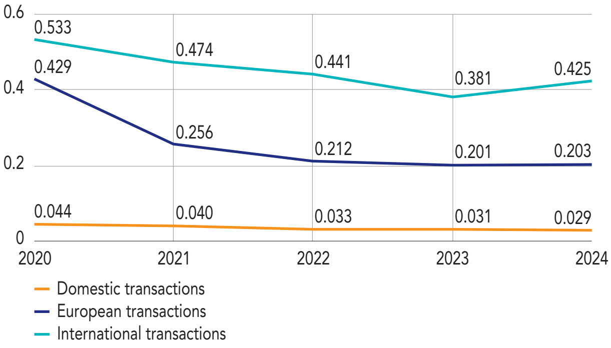


a) Breakdown of transaction amount

b) Breakdown of fraud amount

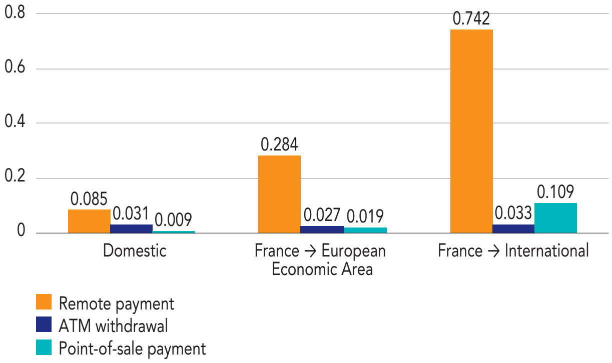
Source: Observatory for the Security of Payment Means.

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 (%)

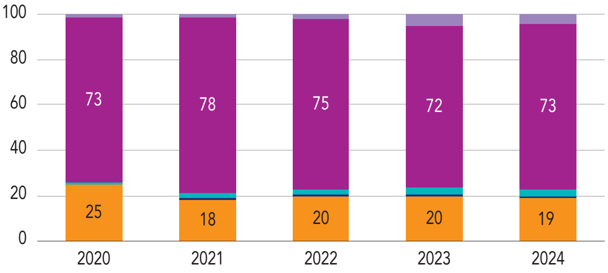


Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

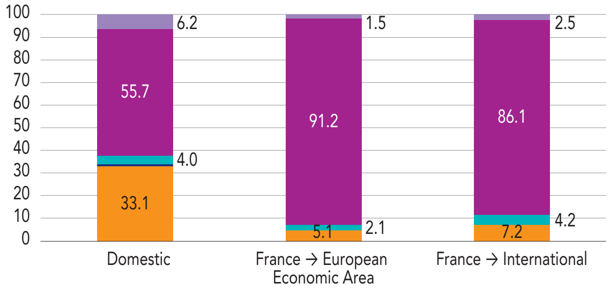
In 2024, international transactions (including transactions to the European Economic Area) accounted for approximately 52% of card payment fraud, compared with 47% in 2023. Whereas the fraud rate for domestic transactions reached an all-time low of 0.029%, the rate for international card transactions rose by 12%. These international transactions are mostly made up of remote payments (90%), which are historically more prone to fraud than domestic transactions and whose fraud rate increased to 0.74% in 2024 from 0.65% in 2023. International POS payments remain more exposed to fraud due to the use of less robust technologies (such as reading magnetic stripes or taking physical imprints of a card) that are therefore more vulnerable to counterfeiting.

1.2.3 Breakdown of fraud by method – Cards issued in France

C16 Changes in types of fraud since 2020 in value terms (%)



C17 Types of fraud by geographical area in value terms in 2024 (%)



Source: Observatory for the Security of Payment Means.

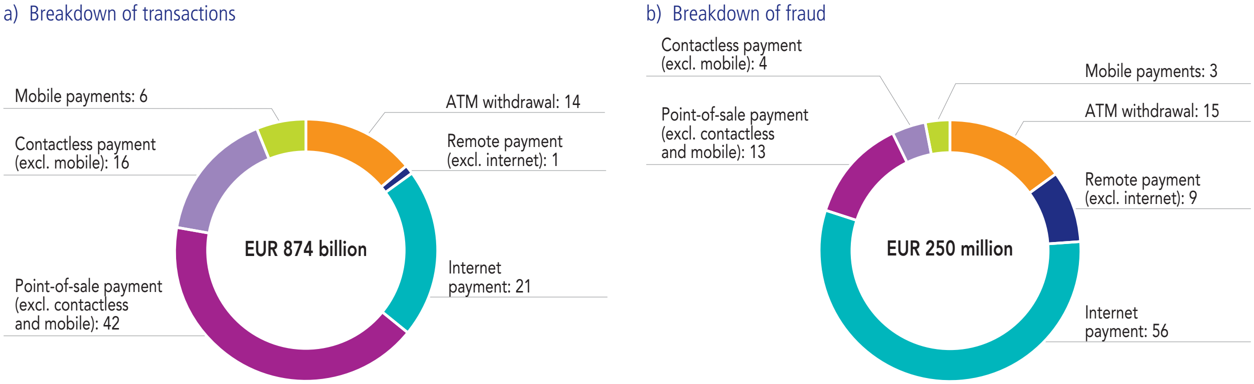
Card number theft using phishing techniques by email or SMS is still by far the most common type of fraud and its value share was steady in 2024 at 73% (72% in 2023).

The proportion of fraud linked to lost or stolen cards was also stable but remained at a low level (19% in 2024). Unsurprisingly, lost or stolen cards are used first and foremost on French territory (33% of fraud), while fraud involving card number theft takes place primarily over the internet with no regard to geographical location, although such fraud has a bigger presence in European and international transactions.

Other types of fraud, such as intercepted or counterfeit cards, continue to account for marginal shares of fraud.

1.2.4 Breakdown of fraud in domestic transactions

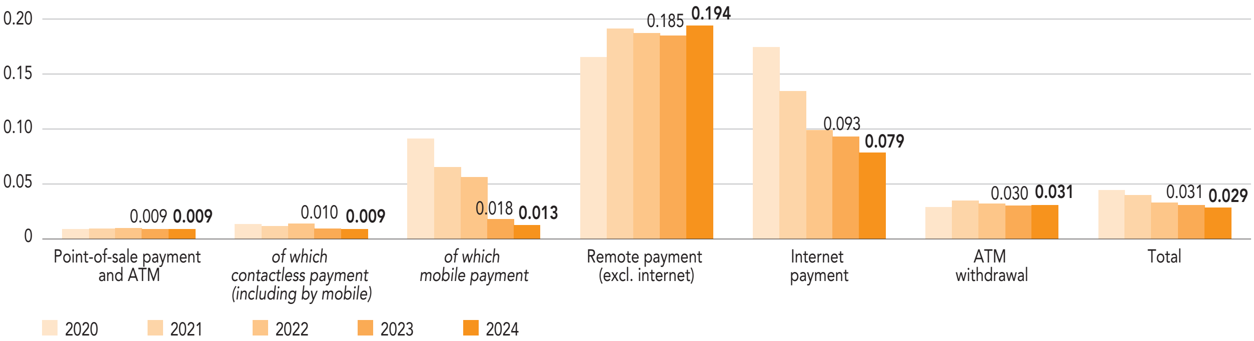
C18 Domestic card transactions in value terms (%)


a) Breakdown of transactions

b) Breakdown of fraud

Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

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



Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

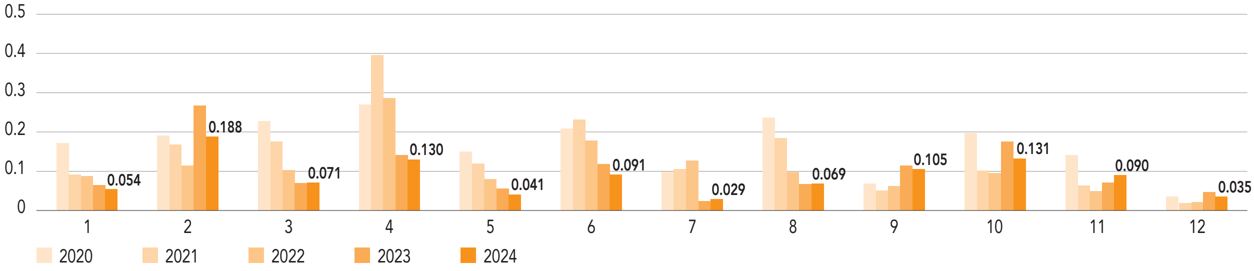
Domestic transactions are increasingly secure: the fraud rate has now fallen to an all-time low of 0.029%.

Remote payment transaction scams accounted for almost 65% of total fraud in France, leading to EUR 163 million in losses, despite making up just 22% of amounts exchanged.

However, internet payments continue to benefit from awareness-raising initiatives by members of the payment ecosystem. As a result, the fraud rate for these payments fell by a further 15% compared with 2023 to reach 0.079%, versus 0.093% in the previous year. In fact, this rate has more than halved since 2020.

1.2.5 Focus on domestic card payment fraud on the internet

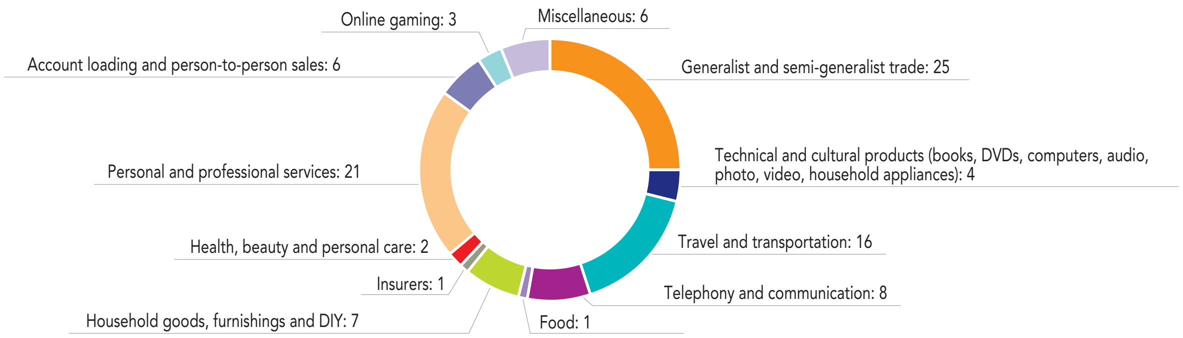
C20 Changes in fraud rates on domestic card payments over the internet, by sector (%)



1 Generalist and semi-generalist trade
2 Personal and professional services
3 Telephony and communication
4 Technical and cultural products
5 Travel and transportation
6 Account loading and person-to-person sales
7 Household goods, furnishings and DIY
8 Online gaming
9 Miscellaneous
10 Health, beauty and personal care
11 Food
12 Insurers

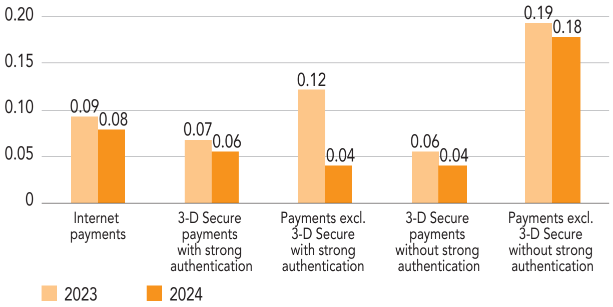
Source: Observatory for the Security of Payment Means.

C21 Breakdown of fraud on domestic card payments over the internet, by sector and in value terms in 2024 (%)



Source: Observatory for the Security of Payment Means.

C22 Fraud rates on domestic payments over the internet, by channel (%)



Source: Observatory for the Security of Payment Means.

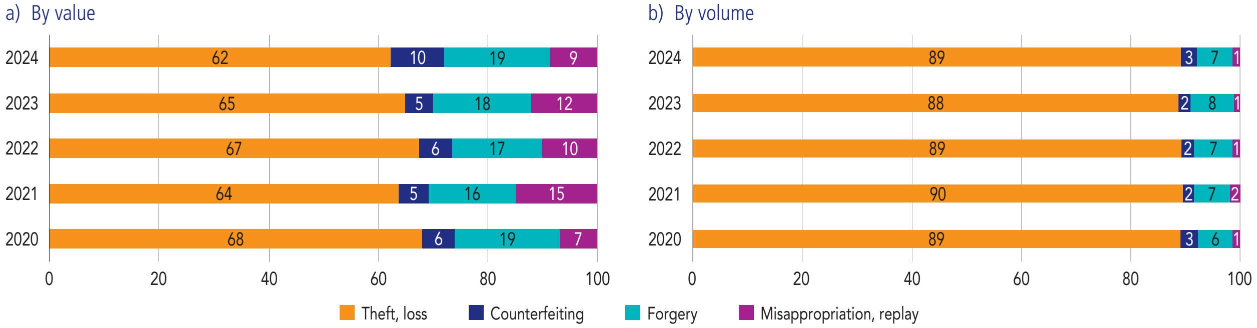
Domestic card payments over the internet that (i) do not use the 3-D Secure exchange protocol (or an equivalent proprietary protocol) and (ii) do not apply strong authentication are proportionally three times more exposed to fraud than other channels. The structurally higher fraud rate for non-3-D Secure remote payments warrants the measures introduced in June 2024 by the Observatory for this type of payment. Deployment of these measures will continue in 2025 and 2026 according to a specified roadmap *(see Chapter 3)*.

Merchant-initiated transactions (MITs), which are similar to direct debits but use a card as the payment means (e.g. subscriptions, deferred payments or reservations), account for the bulk of non-3-D Secure transaction flows (63%). Their fraud rate is more than twice as high as the overall rate for internet payments (0.179%, versus 0.079%).

Furthermore, solutions enabling exemptions from strong authentication are always effective when they use 3-D Secure. The fraud rate for transactions covered by these mechanisms is lower than that recorded for strongly authenticated transactions (0.04%, versus 0.06%). These indicators confirm that exemptions apply to the least risky transactions.

1.3 Current state of cheque fraud

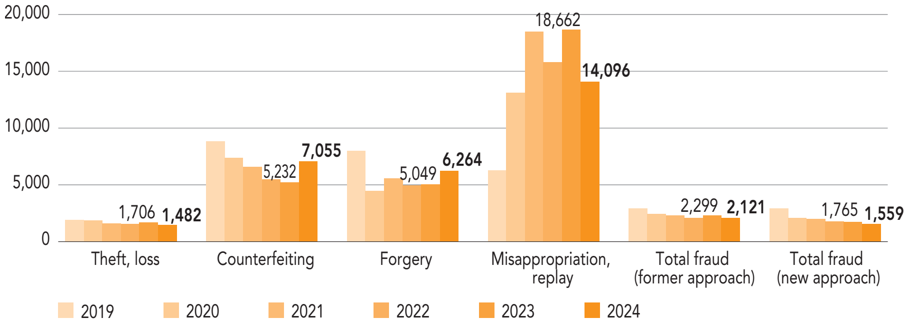
C23 Breakdown of cheque fraud by type of fraud (%)


a) By value

b) By volume

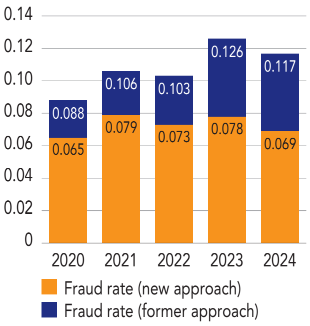
Source: Observatory for the Security of Payment Means.

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



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.

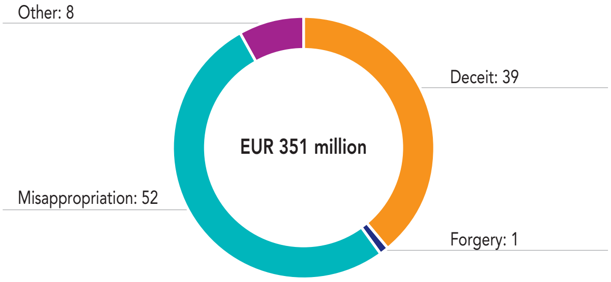
Cheque fraud continued to decline in 2024, falling to EUR 270 million (down 26% year-on-year). This significant decline is largely a result of the mechanisms introduced by banks to block or delay cheque payments, which neutralised 41% of fraudulent payments (EUR 187 million in fraud thwarted).

After excluding thwarted fraud under the new measurement approach, the cheque fraud rate dropped sharply, from 0.078% in 2023 to 0.069% in 2024. The main type of fraud by far remains the misappropriation of lost or stolen cheques, whether presented directly for payment by a fraudster or used as a means to pay merchants or private individuals. Shipment and delivery of chequebooks therefore remain a key area to watch in the cheque lifecycle.

These excellent results are tangible evidence of the long-term effects of the recommendations to prevent cheque fraud released by the Observatory in 2021. However, cheques still have the highest fraud rate of all means of payment. The Observatory therefore urges all participants in the cheque sector to keep up their progress and to focus especially on implementing the recommendations on (i) stepping up the security of chequebook shipment and delivery and (ii) making it easier to report loss or theft *(see Chapter 3 on follow-up on the Observatory's cheque recommendations)*.

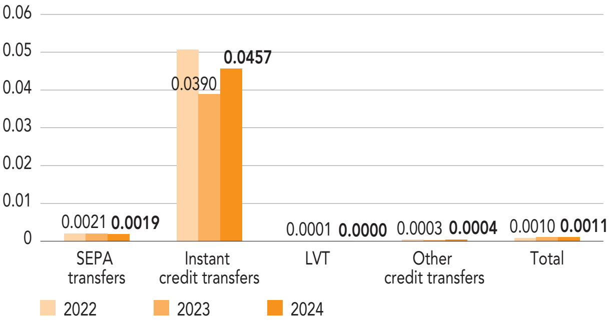
1.4 Current state of credit transfer fraud

C26 Breakdown of transfer fraud by type of fraud in value terms in 2024 (%)



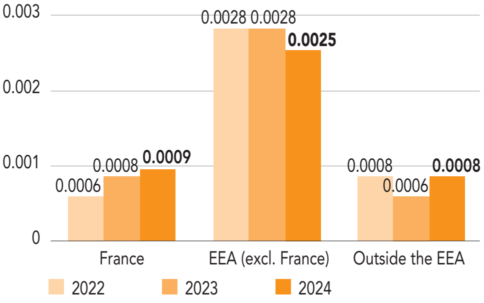
Source: Observatory for the Security of Payment Means.

C27 Fraud rate by type of transfer (%)



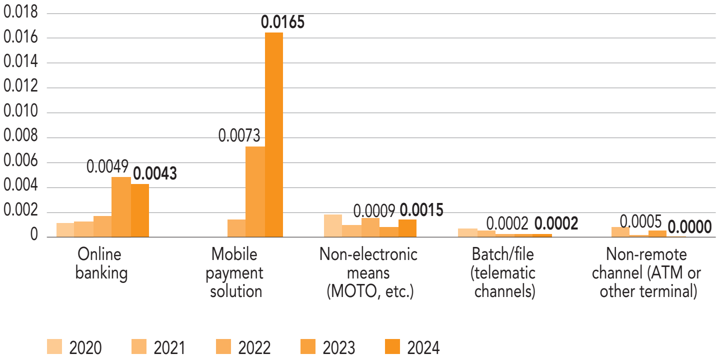
Source: Observatory for the Security of Payment Means.
Note: SEPA, Single Euro Payments Area; LVT, large-value transfer.

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



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

C29 Changes in transfer fraud rates by payment initiation channel (%)



Source: Observatory for the Security of Payment Means.
Note: MOTO, mail orders and telephone orders; ATM, automated teller machine.

Credit transfer fraud rose by 12% to EUR 351 million in 2024. This increase accompanied a structural change in credit transfer fraud: the telematic channels used by businesses continued to have very low exposure to fraud (fraud rate of just 0.0002%), while fraudster attacks tended to concentrate more on online banking solutions (fraud rate of 0.0043%) and mobile payments. Fraudsters use phishing techniques to gain access to online banking, and social engineering techniques to convince their victims to provide sensitive data or validate a transaction. Fraudsters are making greater use of accounts opened in France to retrieve their funds (13% increase in the domestic fraud rate), although European transfers are, compared with French domestic transfers, more than twice as exposed to fraud.

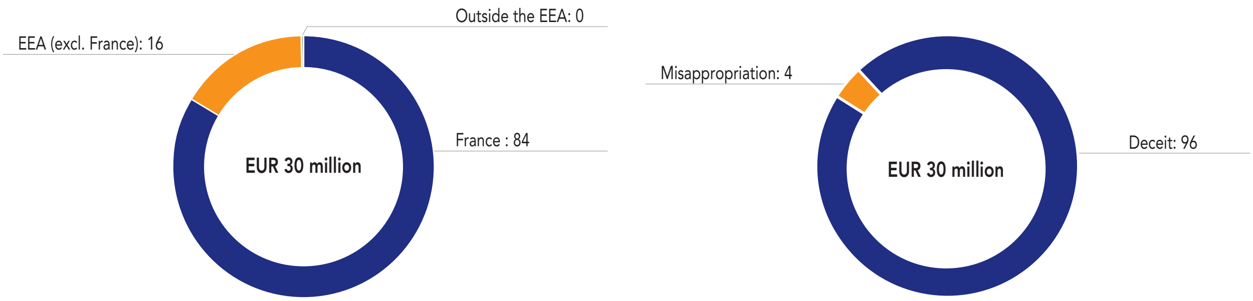
The instant credit transfer fraud rate edged up from 0.039% in 2023 to 0.046% in 2024. It is however still below the card fraud rate (0.053%), even though these two payment methods, which are both widely used by consumers, rely on similar security mechanisms, including the same strong authentication solutions for online payments.

1.5 Current state of direct debit fraud

C30 Breakdown of direct debit fraud in value terms (%)

a) By geographical area

b) By type of fraud

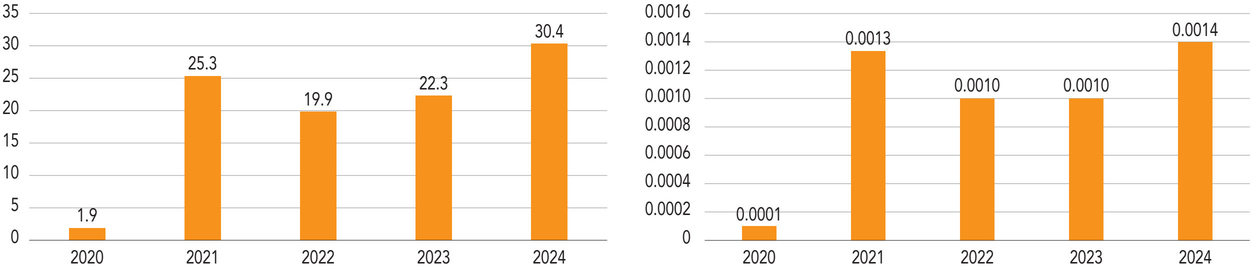


Source: Observatory for the Security of Payment Means.
Note: EEA, European Economic Area.

C31 Direct debit fraud

a) By value (EUR millions)

b) Rate (%)

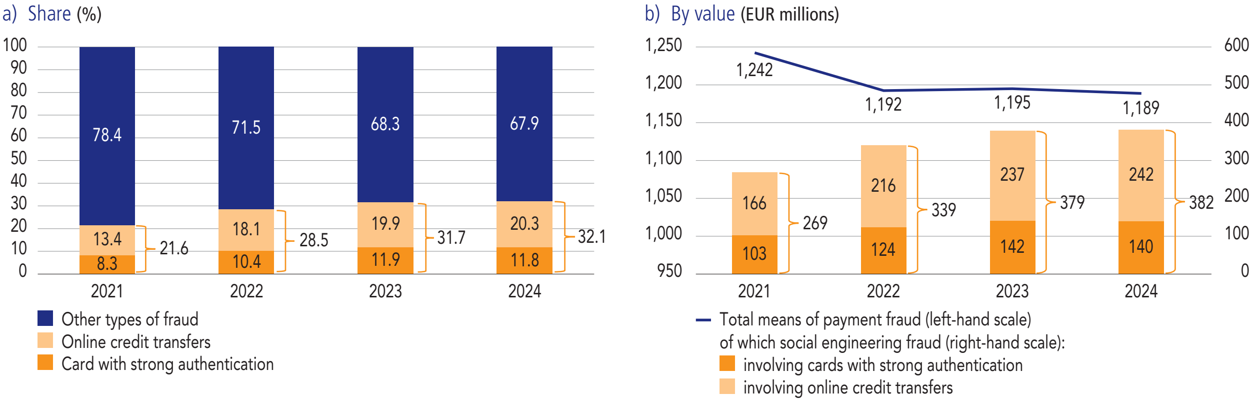


Source: Observatory for the Security of Payment Means.

While the amount of transaction flows was more or less stable (up 2%), direct debit fraud continued to increase, rising 36% to EUR 30.4 million. The fraud rate climbed automatically from 0.0010% in 2022 and 2023 to 0.0014% in 2024. This type of fraud is perpetrated almost exclusively by fraudsters issuing fake orders, without having a direct debit mandate or an economic relationship with the victim. Misappropriation fraud, where the fraudster steals the identity and international bank account number (IBAN) of a third party to sign a direct debit mandate, once again represented a tiny share of fraud in 2024 (4%).

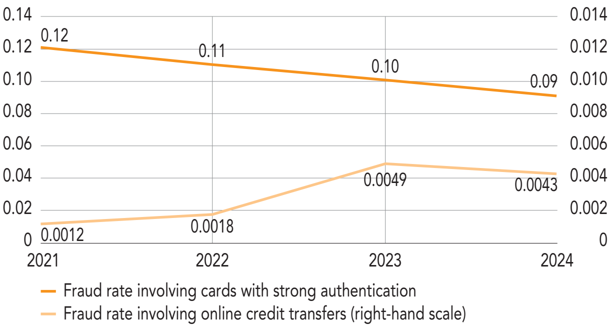
1.6 Current state of social engineering fraud

C32 Change in social engineering fraud, in value terms



Source: Observatory for the Security of Payment Means.

C33 Changes in social engineering fraud rates (%)



Source: Observatory for the Security of Payment Means.

Social engineering fraud includes cases where the customer is manipulated by the fraudster during a phone call. Often, the scammer poses as a payment service provider, such as a fake bank adviser or anti-fraud department. The Observatory measures the scale of this type of fraud using a proxy that sums fraudulent card transactions subject to strong authentication and fraudulent online banking credit transfers, which are the two channels targeted by fraudsters.

After increasing sharply between 2021 and 2023 (up 47%), social engineering fraud rose slightly in 2024, both by value (up 0.7% to EUR 382 million) and as a relative share of total fraud (from 31.7% in 2023 to 32.1% in 2024). The decrease in the share of fraud for strongly authenticated card transactions (0.8% by value) was offset by the increase in the share of online banking fraud (up 2.3%). However, owing to the increase in the underlying flows, fraud rates fell for both these channels.

The overall stability in the share of social engineering fraud is attributable to (i) widespread awareness-raising efforts by members of the ecosystem and (ii) the introduction by payment service providers of specific measures to prevent this type of fraud, including modifications to authentication procedures for online banking and banking apps, and enhancements to scoring tools. The number authentication mechanism required by the Naegelen Act and intended to prevent fraudulent calls has been deployed since October 2024. It should gradually stop fraudsters from misappropriating PSP phone numbers. Deployment of a service to check IBAN matches, beginning in October 2025, should likewise help to prevent social engineering fraud, especially those involving fraudulent IBAN switches.

❶

Indicators, lessons and recommendations from the French Ministry of the Interior on means of payment fraud in 2024

The French Ministry of the Interior is represented on the Observatory by the *Gendarmerie Nationale*'s cyber unit and the *Police Nationale*'s *Direction nationale de la police judiciaire* (DNPJ – National Judicial Police Directorate). In 2024, as they do every year, these two bodies reported their main observations on means of payment fraud to the Observatory.

1. Ministry of the Interior fraud statistics: a much broader scope than those of the OSMP, but with consistent and complementary findings

On 10 July 2025, the *Service statistique ministériel de la sécurité intérieure* (SSMSI – French ministerial statistical service for internal security) published its 2024 statistical atlas of crimes and offences, including scams and means of payment fraud.[1]

1.1 The Ministry's sources and methodologies differ from those of the Observatory

The SSMSI methodology for recording means of payment fraud, which is now systematically aggregated with other scams, differs significantly from that of the Observatory. By grouping means of payment fraud together with scams and other confidence tricks, the SSMSI applies a much broader scope than the OSMP. It includes all credit and investment scams, fake internet sales, ransomware attacks and romance scams, which are not counted as means of payment fraud by the OSMP. Furthermore, the SSMSI calculates the number of victims[2] on the basis of complaints filed, whereas the OSMP tallies the fraudulent transactions reported by payment service providers and card schemes. Lastly, the SSMSI's assessment of losses suffered is based on cross-referencing data recorded when a complaint is made with data from victimisation surveys.[3] The OSMP, on the other hand, uses the precise fraudulent transaction amounts reported by the institutions concerned. These differences in methodology and scope mean make it impossible to directly reconcile the data published by the SSMSI and the figures published by the Observatory.

1.2 Even so, the findings of the SSMSI and Observatory point to the same trends

The SSMSI's report and trends in means of payment fraud noted by the Observatory highlight a number of similarities.

Although the number of scam and means of payment fraud victims recorded by *Police Nationale* and *Gendarmerie Nationale* services continues to increase, rising from 411,700 people in 2023 to 417,300 in 2024, the pace has slowed markedly, with growth of just 1.4% between 2023 and 2024, compared with 6% between 2023 and 2022.

Means of payment fraud is increasingly based on manipulating victims (e.g. false bank adviser scams, CEO fraud, bank account details fraud, etc.) and targets individuals more than organisations. According to the SSMSI study, organisations accounted for 9% of victims of fraud in 2024, down from 16% in 2016.

The SSMSI report makes the point that in 2024, **half of all scams and means of payment fraud cases were linked to digital technology.** This share has surged since 2016, rising from 31% in 2016 to 50% in 2024. The soaring increase in these offences reflects digital's growing role in scams and means of payment fraud.

Young adults are the most common victims of scams and means of payment fraud. The number of scam and means of payment fraud victims known to law enforcement rises significantly from age 18 onwards, peaking at between 20 and 24 years of age, with a rate of 9 victims per 1,000 people in that age bracket.

[1] See Ministry of the Interior, "*Insécurité et délinquance en 2024*", 9th edition of the statistical report.

[2] According to the SSMSI's "*Vécu et ressenti en matière de sécurité*" (VRS) 2022 survey into people's experiences and feelings with regards to their security, around one in ten victims of fraud files a complaint.

[3] The victimisation survey is a statistical poll that questions a sample of the population on the crimes and offences they have suffered.

People aged between 18 and 44 alone account for around 45% of victims, while making up just 32% of the population.

Scams involving fake bank transfer orders and targeting organisations (companies, government agencies, local authorities) are watched particularly closely by law enforcement. According to law enforcement agencies, fake bank transfer order scams are a form of financial fraud in which the victim is coerced into making a transfer, which he or she believes to be legitimate, to a bank account managed by the perpetrator. There are two main methods.

- Bank account details fraud: fraudsters impersonate their target's supplier and tell the target that there has been a change in the bank account details that they should use to settle their bills, thus diverting the payment.

- CEO fraud: fraudsters assume the identity of a high-level company official or representative (lawyer, consultant, etc.) to trick employees into transferring money into a new account; the scammer will insist on the need to act urgently and in strict confidentiality.

In 2024, 649 cases against organisations were reported to the DNPJ, with losses totalling EUR 34 million, compared with 657 cases[4] and losses of EUR 49 million[5] in 2023.

Because they cover all victim profiles, i.e. individuals and organisations, the general trends measured by the Observatory, conversely, point to growth: bank transfer fraud by misappropriation increased by 20% in value terms and by 118% in volume terms in 2024.

2. Focus on the Perceval and Thésée reporting platforms

Since 2018, the *Gendarmerie*'s **Perceval platform** has been used to collect reports from users about the fraudulent use of payment cards on the internet. Its data can be more easily reconciled with the trends observed by the Observatory. There were 227,711 cases filed in 2024, down 12% from 258,700 in 2023. Note that one case reported on Perceval may actually cover several different fraudulent transactions initiated using the same stolen card details.

When considered alongside the Observatory's statistics, the percentage of frauds reported on Perceval continues to decrease. Only 37% of card fraud involving internet payments as quantified by the Observatory was reported on Perceval in 2024, compared with 44% in 2023 and 51% in 2022. Victims tend to report only the largest frauds: in 2024, the average value of a fraudulent transaction, according to the Observatory's statistics, was EUR 60, compared with EUR 168 according to Perceval (EUR 637 per complaint filed, which contained an average of 3.82 transactions).

The Thésée platform was launched in March 2022 and is managed by the *Office anti-cybercriminalité* (OFAC – the anti-cybercrime office of the *Police Nationale*). It allows individual victims of internet scams and frauds to lodge a complaint online.[6] In 2024, 53,300 complaints were made on the Thésée platform. This represents 11% of the total number of victims of means of payment fraud and scams recorded by the SSMSI, down from 14% in 2023.

The Observatory urges scam and fraud victims to report their cases on the Perceval and Thésée platforms, after first checking that they are eligible to do so. These reports provide law enforcement agencies with the information they need to dismantle fraud networks.

[4] The 2023 statistics reported here may be slightly higher than those contained in the OSMP's 2023 annual report. This is due to the lag between the date when a complaint is filed and the date on which the DNPJ receives the information. It may be that the DNPJ is informed about complaints several months after the incidents occurred, with the result that annual totals are regularly revised upwards.

[5] The cases reported to the DNPJ are a representative but non-exhaustive sample of fake bank transfer order scams committed against organisations in France.

[6] Filing a complaint online via the Thésée platform eliminates the need to do so in person at a law enforcement office. Thésée data are included in the number of victims of means of payment fraud published on 10 July 2025 by the SSMSI in its statistical study on insecurity and crime in 2024.

3. Hacking of payment and cash withdrawal terminals: fewer incidents each year

Hackers target payment or cash withdrawal machines (ATMs, automatic fuel dispensers, motorway vending machines, car park payment stations, 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.

Skimming[7] involves the use of tampered payment terminals to procure the bank details stored on a payment card's magnetic strip. The stolen card data are then re-encoded on counterfeit magnetic stripe cards, which are used for withdrawals or payments at points of sale where chip reading is not required, such as motorway toll booths, or in countries where smart cards are not yet widely used (countries in South America or South-East Asia, for example). The skimmed data can also be used in remote payments, mainly on non-European e-commerce sites that do not employ strong cardholder authentication solutions.

Shimming[8] relies on similar techniques to **skimming**, but targets the data stored in the card's chip. The high technical complexity involved means that attacks remain limited so far.

Figures from the *Groupement des cartes bancaires* (France's national interbank network) highlight a steep fall in skimming over the last few years. Nevertheless, service station managers, ATM managers and merchants alike must stay on their guard to prevent attempts to replace legitimate payment terminals with compromised terminals or to install fraudulent external devices such as readers, cameras or keypads.

[7] A skimmer is a device that slides into the slot of a machine or dispenser while leaving enough space for a bankcard to be easily inserted. The device then copies the data stored on the magnetic stripe, without interfering with the bankcard transaction.

[8] A similar device to a skimmer in that it is incorporated into a machine or dispenser, but which intercepts data, including the PIN code, from the bankcard's chip.

2

RESULTS OF RECOMMENDATIONS ON PREVENTING AND REIMBURSING FRAUDULENT PAYMENT TRANSACTIONS

2.1 Background

Amid a rise in fraud cases featuring social engineering techniques, the *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) issued a set of 13 recommendations in April 2023 to clarify the procedures used in applying the legislative framework for the reimbursement of disputed transactions and to strengthen fraud prevention mechanisms.

The Observatory tasked the Banque de France and the *Autorité de contrôle prudentiel et de résolution* (ACPR – Prudential Supervision and Resolution Authority) with assessing the results of the recommendations following their first 18 months of application. This chapter therefore reports on the work done in this regard by the two authorities.

In summer 2024, the **ACPR** conducted a questionnaire-based survey of 14 payment service providers that made up a representative sample of different PSP profiles (traditional banking networks, online banks, mutual banks, full-service banks and payment institutions). The survey was followed up by individual action at each of the institutions to assess implementation of the recommendations.

The **Banque de France** set up a programme to collect statistics on the handling of fraud-related disputes received by payment service providers. This programme covered the six main French banking groups, with data on each half during the 2023-24 period as well as the first quarter of 2025.

2.2 Summary

The recommendations have had positive results, according to assessments by the ACPR and the Banque de France.

- **Payment journeys – particularly online and in banking apps – have been made more secure overall** through the provision of better information to customers (about the type of transaction in process, the amount, the payee, reminders to exercise caution, etc.) and the deliberate introduction of frictions (via explicit questions or choices, for instance). This combination of measures has enabled users to respond more effectively to attempted manipulations.
- **Handling of fraud-related disputes has also improved, in line with the recommendations:** disputes are now handled by analysing the three categories of criteria recommended by the Observatory (technical parameters specific to the transaction, strong authentication methods used, and the circumstances) and by drawing on the enhanced information generated by new authentication processes. Reimbursement refusals are thus more fully supported, even if some institutions still need to work harder to provide technical evidence in response to customer requests.

- **Fraudulent card payments not covered by strong authentication are being systematically and immediately reimbursed.** But progress remains to be made in reimbursing fraudulent payments by credit transfer without strong authentication, which ought to receive similar treatment.

The ACPR and the Banque de France will continue to monitor practices at individual institutions, especially those that still have room for improvement in applying the recommendations. They will likewise keep tracking **statistical indicators on disputes and reimbursement** at the main institutions based in France.

2.3 Results of general recommendations for the handling of disputed payment transactions

Recommendation No. 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.

Recommendation No. 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.

Recommendation No. 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.

Work by the ACPR revealed a satisfactory level of compliance with these three recommendations: dispute handling procedures now build in the deadline requirements set by the regulations and by Recommendation Nos. 1 and 2.

The formal requirements for disputes demanded by institutions have been relaxed, making it possible to record disputes:

- without a complaint being filed by the injured party, at all institutions;
- and without a signed form being filed, at 12 of the 14 surveyed institutions.

However, some institutions still need to make progress on Recommendation No. 3.

- Specifically, 5 of the 14 institutions still report operational challenges in providing all required elements to customers when requested by the latter to do so.

The ACPR will continue to monitor those institutions individually.

2.4 Results of recommendations applicable to the treatment of specific cases

Recommendation No. 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 suspicion of fraud cannot be based solely on the use of the payment instrument.

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.

[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.

Recommendation No. 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.

Recommendation No. 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 delay to reimburse the transaction;
- or the payment service provider has good reason to suspect fraud by the user 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, or that the user was grossly negligent, 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.

Work by the ACPR revealed a satisfactory level of compliance with these three recommendations: in particular, institutions have properly integrated analysis of the three categories of criteria (technical parameters, strong authentication procedures and contextual elements) required by Recommendation No. 6 into their dispute handling processes.

However, the ACPR notes that some institutions still need to make progress.

- All institutions say that they can refund the expenses incurred as a result of recognising a fraudulent transaction, such as overdraft fees and loan interest, and pay late fees due in the event of delayed reimbursement. But 5 of the 14 institutions assessed do not have an automated system to do this.
- Regarding Recommendation No. 4, in the case of direct debits that are disputed more than eight weeks after the account was debited, 2 of 12 institutions[3] do not issue a refund until they have received the results of the mandate search. This conflicts with the principle of D+1 reimbursement written into the regulations and restated in Recommendation No. 4. These institutions should reimburse the customer immediately while giving notification that the funds could be recovered within 30 days if proof is obtained of a non-revoked mandate signed by the customer and authorising the disputed direct debit.

The ACPR will continue to monitor the affected institutions individually.

In addition, the statistics gathered by the Banque de France can be used to analyse how institutions handle incoming disputes, according to a process aligned with the decision tree provided in the introduction to the recommendations.

- The first filter consists in determining whether the transaction can be considered to have been authorised by the user. It particularly aims to screen out transactions resulting from a business dispute (e.g. a good or service that was undelivered or failed to meet the customer's expectations, or court-ordered liquidation of the merchant) as well as instances where the customer was scammed into agreeing to the transaction (e.g. fake site posing as an e-merchant, fake investments, emotional blackmail or ransomware payment). Because these payment orders were authorised by the user, the rules for reimbursement in cases of fraud do not apply.

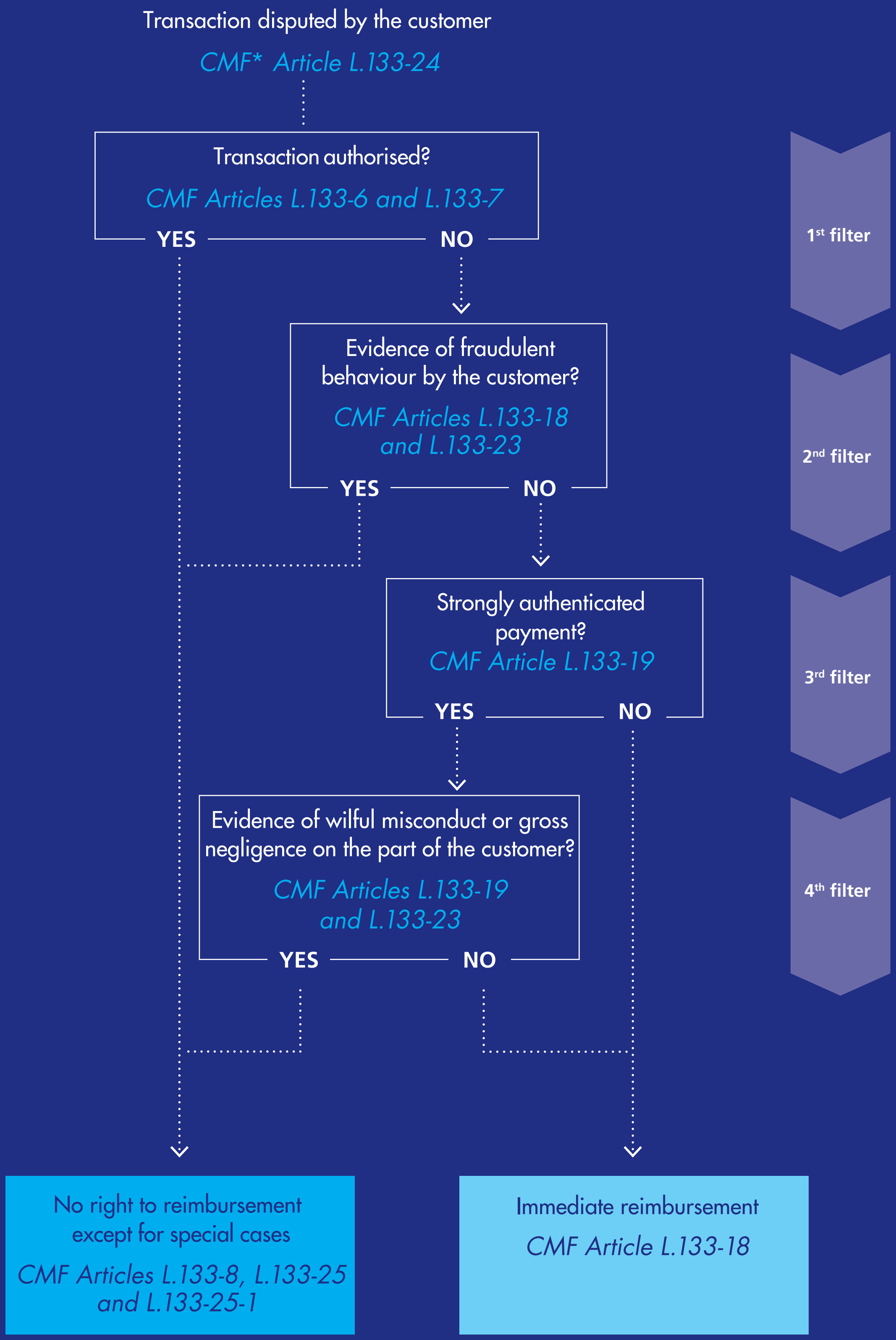
  ➡ By applying this filter, banks exclude 12% of disputes, or 26% of the total value covered by disputes.

- The second filter consists in identifying unfair disputes by customers, where either the customer or someone in their close circle did indeed instigate the transaction, such as a purchase by the customer's child made without the customer's knowledge and using their terminal and strong authentication tools.

  ➡ By applying this filter, banks exclude 4% of disputes, or 3% of their total value.

[3] Out of the 14 payment service providers assessed by the ACPR, two do not offer direct debit services.

PROCESS FOR HANDLING PAYMENT TRANSACTIONS DISPUTED BY THE CUSTOMER



Transaction disputed by the customer

CMF Article L.133-24*

Transaction authorised?

CMF Articles L.133-6 and L.133-7

YES NO

1st filter

Evidence of fraudulent behaviour by the customer?

CMF Articles L.133-18 and L.133-23

YES NO

2nd filter

Strongly authenticated payment?

CMF Article L.133-19

YES NO

3rd filter

Evidence of wilful misconduct or gross negligence on the part of the customer?

CMF Articles L.133-19 and L.133-23

YES NO

4th filter

No right to reimbursement except for special cases

CMF Articles L.133-8, L.133-25 and L.133-25-1

Immediate reimbursement

CMF Article L.133-18

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

Following application of the first two filters, the remaining disputes (84% of the total number of initially disputed transactions and 70% of the total value) are counted as fraudulent transactions for the purposes of the work of the Observatory. This is the base used to assess banks' effective reimbursement rates.

- The third filter seeks to identify disputes involving transactions that were not subject to strong authentication, which should always be reimbursed, pursuant to Recommendation No. 4.

  ➡ **Card payments without strong authentication have a reimbursement rate of 98% by value, which is in line with Recommendation No. 4.**

  ➡ **Credit transfers without strong authentication have a reimbursement rate of 20% by value, which is far too low. Insofar as banks may not claim gross negligence on the part of the user for this type of transaction, this indicator points to ongoing non-compliance. However, only a small proportion of disputes are affected (less than 10% of the total number of cases). The Banque de France will watch this indicator closely and will take action at the level of individual institutions.**

- The fourth filter aims to identify, among disputed transactions that were subject to strong authentication, those for which the bank can provide evidence that the customer was grossly negligent in protecting their personal login information or means of authentication, thereby providing grounds to refuse reimbursement.

  ➡ **Following application of these last two filters, the overall reimbursement rate for all payments was 91% by number of transactions and 62% by value.**

  ➡ **This overall rate has come down over the last two years, as measures to strengthen the customer journey ensure that customers are better informed throughout the authentication process, with a view to foiling attempted social engineering frauds more effectively.**

  ➡ **Institutions are therefore in a better position to determine to what extent users may have been negligent as regards the warnings sent to them and the options offered to them for the disputed transactions.**

2.5 Results of recommendations aimed at consumers and their representatives

<u>Recommendation No. 7:</u>

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.).

Recommendation No. 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 platforms 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.

The work done by the ACPR and the Banque de France with payment service providers (PSPs) cannot be used to assess the application of these recommendations by consumers. However, the Observatory notes that, following publication of its recommendations, PSPs have worked hard to make customers more aware of best security practices.

2.6 Results of recommendations aimed at preventing fraud

Recommendation No. 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.

Recommendation No. 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.

Recommendation No. 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.

Recommendation No. 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.

Recommendation No. 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.

The ACPR will continue to monitor the affected institutions individually.

In accordance with Recommendation No. 13, the Observatory continues to step up its constructive cooperation with the telecommunications sector. At the same time, cooperation with digital sector participants, especially messaging apps and platforms, could still be significantly increased *(see Chapter 3, Section 2).*

Work by the ACPR revealed a satisfactory level of compliance with Recommendation Nos. 9, 10, 11 and 12, with assessed institutions showing strong commitment to fraud prevention tools. In particular, in response to Recommendation No. 11, authentication processes at all institutions now display information that properly characterises transactions (type, amount, payee, etc.).

However, the ACPR notes that some institutions still need to make progress:

- regarding Recommendation No. 9, 3 out of 13 institutions[4] still do not conduct strong authentication when customers access accounts from a new device, preferring instead to base their analyses on internal risk assessment models;
- regarding Recommendation No. 10, 2 of 12 institutions are asked to provide more explicit information about the specific features of instant credit transfers at the time when the user has to choose between a standard credit transfer and an instant credit transfer;
- regarding Recommendation No. 12, the ACPR calls on institutions that do not yet offer them to develop solutions that can be used to set payment limits in order to prevent fraud, such as white or blacklists for direct debits (1 institution out of 12) or an online maximum amount for credit transfers (5 of 13 institutions), which is a regulatory requirement for instant credit transfers.[5]

[4] The number of institutions concerned by a particular recommendation may differ from the total number of institutions assessed (14), because some recommendations do not apply to the business models of certain institutions.

[5] Article 5 bis (6) of Regulation EU) No. 260/2012 of the European Parliament and of the Council of 14 March 2012.

3

WORK CARRIED OUT BY THE OBSERVATORY ON FRAUD PREVENTION

Chapter 3 is available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2024

4

ARTIFICIAL INTELLIGENCE'S CONTRIBUTION TO FRAUD PREVENTION: CHALLENGES AND OUTLOOK

4.1 Introductory remarks

Broadly, systems to protect means of payment against fraud are based on four fundamental pillars, written down in the Second European Payment Services Directive (PSD 2),[1] namely:

1. authentication of the parties to the transaction, to establish the legitimacy of both payer and payee;
2. the capability of payment chain participants to detect transactions at a high risk of fraud;
3. the physical and logical security of payment instruments and infrastructure, to ensure that payment data are always protected against the risks of being compromised or used to fraudulent ends;
4. awareness raising among users, so that they take steps to protect their payment instruments and data and know what to do when faced with attempted fraud.

While these four pillars form a solid foundation for fraud prevention, the ability of fraudsters to devise new fraudulent processes means that payment chain participants must harness technological advances to develop new fraud prevention capabilities. In particular, systems to detect at-risk transactions must be strengthened *(see point 2 above)*. These tools, which are the subject of this study, chiefly comprise scoring models for payment transactions. Such models rely on sophisticated algorithms developed by teams responsible for modelling and exploratory data analysis. Their role is to analyse transaction characteristics automatically and in real time in order to issue alerts if fraud is suspected. A transaction may thus be blocked while analysts run checks. The introduction of artificial intelligence (AI) modules to these systems is helping to significantly boost the performances of detection models. These systems may be deployed at different levels of the payment chain.

- They could be used autonomously by one participant in the chain:
  - For example, a payment service provider (PSP) could establish a user profile for each of its customers, based on payment habits, and assess a given transaction's risk of fraud as a function of its atypical characteristics (deviation from the customer's usual habits). For example, if a customer typically uses their card for small face-to-face payments or withdrawals, issuance of a large-value international online payment would be treated as riskier than it would be for someone who uses their card regularly to make payments on foreign websites,
  - Or, an e-merchant might deem a change to a regular customer's shipping address to constitute a risk factor warranting a verification call or a request for strong authentication at the time of payment;

- Other scoring mechanisms are shared by multiple payment chain participants via card payment schemes, such as *Cartes Bancaires* in France, or Visa and Mastercard, or via payment infrastructures, such as STET and EBA Clearing. A feature of these schemes and infrastructures is that they centralise the payment flows of many institutions, including information about mechanisms for fund recovery or reimbursement in the event of fraud. Once these data are processed, a score can be issued for the risk level associated with a given transaction, which is shared with the payer's PSP. The PSP may then adjust its own risk assessment, if it wishes.

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

By foiling attempted frauds, these models play a direct role in maintaining and improving confidence in means of payment and, by extension, in the stability of the banking and financial system. They also promote a smoother journey for customers. Specially, when these models are employed, some transactions are exempted from strong authentication requirements if the risk level is considered to be low (transaction risk analysis-based exemption).[2]

The purpose of this study is to describe the main types of models employed and the challenges associated with their use, their integration into the business processes of payment chain participants and compliance with the regulatory frameworks currently in force.

4.2 Technical challenges involved in optimising model performance

The quality of input data has a critical bearing on model performance. Payment participants face a twofold challenge in this respect: (i) that of continually improving data quality; (ii) and that of swiftly integrating new training data to reflect the latest identified fraud techniques. These issues are compounded by the requirement to strike a balance between the need for effective models and the risk of a significant increase in false positives, i.e. transactions that are wrongly identified as suspicious, as these are disruptive to customers.

4.2.1 Training data

The Delegated Regulation on Strong Customer Authentication supplementing PSD 2 specifies the type of data that may be used by payment transaction monitoring systems. These include the customer's habits in using the payment instrument, payment transactions, the location of the payer and payee, technical solutions and software used by the payer, and any signs of malware infection. Talks are being held on modifying this regulatory framework through a European Payment Services Regulation (PSR).[3] This draft regulation would still allow current data to be used in transaction monitoring systems, but would include additional data on the app session (IP addresses, etc.) and, more generally, information that may be helpful in recognising a legitimate user who is behaving in accordance with their payment habits.

4.2.1.1 Quality of training data

In machine learning, the set of training data is like the foundations of a building – it determines the strength and stability of any AI model. For a model to be robust over time, the data must be reliable (i.e. have consistent values and be in the correct format, with few missing or illogical values), non-biased, available over time and representative of the population to which the model applies.

A large proportion of this data is entered, transmitted and collected in authentication and authorisation message fields by each participant in the payment chain through to the information system (IS) of the issuer's PSP. The mandatory data required for the technical authorisation of payments are standardised in the payment instrument rulebook, such as the primary account number (PAN) for card schemes, or unique identifiers (IBAN) for SEPA[4] payment schemes. Other fields are provided to record optional data, such as the shipping address, the merchant's Siret number (French business ID), etc., but there are no guarantees as to their availability or quality in the absence of marketwide standards.

The software developments and integrations required to ensure the quality of the data exchanged in this manner may represent a cost that is hard for some participants, such as smaller merchants, to bear. Furthermore, PSP data collection and transmission practices are widely non-standardised, especially if one of the parties to the transaction is not located in France or the European Union.

➡ The exhaustiveness and accuracy of training data are thus directly affected by the length of the payment chain and the lack of properly defined and implemented standards. Stronger market standards for data quality across the entire payment chain would benefit the whole ecosystem and make fraud prevention solutions more effective.

To enhance data quality, PSPs are taking steps, either on their own or by delegating the task to specialised start-ups, to make their data more reliable, notably by cross-referencing multiple sources. AI modules can potentially perform this task. For example, when merchants' data are enhanced to include opening times and the geographical location of sales outlets, fraud alerts can be issued if discrepancies are detected, e.g. face-to-face card payments on electronic payment terminals taking place outside the usual hours or locations.

Fraud today comes in an extremely wide range of different types, including social engineering, hacking of online bank accounts, card frauds instigated by scammers posing as merchants, and unfair disputes by customers themselves. Detecting these frauds therefore requires different sets of data.

➡ Segmentation of the available data is a commonly used technique that consists in dividing the overall set of available data into several subsets based on objective criteria, in order to develop optimised detection modules for each fraud type.

4.2.1.2 Imbalance issue affecting the fraudulent transactions class

A statistical class is a group of values in which data are classified to calculate a frequency distribution. According to the Observatory's statistics, fraudulent transactions accounted for 0.0337% of the total number of card transactions in 2023 and 0.0016% of credit transfers.

➡ These minuscule shares pose challenges for statistical modelling because it is hard to train models to detect frauds using such tiny samples.

Two statistical techniques can be used to address this problem.

- **Oversampling**: this consists in randomly duplicating observations from the minority class (here, fraudulent transactions) until the desired proportion is reached. The effect is therefore to compile a set of observations in which fraudulent transactions have a larger share.
- **Undersampling**: this technique consists in randomly removing observations from the majority class (here, non-fraudulent transactions) until the desired proportion is reached for the minority class.

These adjustment techniques can have adverse effects, however.

- **With oversampling**: besides issues connected with data storage and increased computation time, this technique duplicates existing data and, accordingly, the associated observation errors. It also comes with a risk of overfitting, which can cause the model to detect only cases of fraud whose characteristics are identical to those contained in the training sample.
- **With undersampling**: since the absolute number of fraud cases is inherently very low, increasing their share of the total sample also implies considerably reducing the total number of transactions in the training sample. However, a minimum number of observations is required to calibrate and train a model properly. Furthermore, since the volume of legitimate transactions has been greatly reduced, there is a risk that the model might no longer see all the different types of legitimate payment, causing it to generate too many alerts (false positives).

➡ Pooling data among institutions, for example through schemes and interbank networks, offers another potential response to the issue posed by the small share of fraud cases in the samples. It is a way to increase the number of actual cases of fraud without having to use statistical methods that could be sources of distortions.

4.2.2 The three main categories of models

4.2.2.1 Expert models

Expert models (or heuristic models) comprise automatic rules, called scenarios, that experts create based on an analysis of data on fraudulent transactions. These rules are tailored to the business models of institutions and the characteristics of their customers' payment habits. Here are a few examples of rules that are typically used to issue alerts:

- a transaction whose amount is disproportionate, exceeding preset thresholds relative to the customer's typical incoming or outgoing transactions;
- an unusual transaction with a counterparty based abroad, especially in places or with institutions identified as being at-risk;
- transactions corresponding to the use of "mule"[5] accounts, where a recently opened account receives funds from multiple sources over a relatively short period followed by multiple cash withdrawals.

Heuristic models have the advantage of being swiftly adaptable to capture changes in the habits of customers and fraudsters. For example, some rules may be lifted if the customer tells the PSP that they are going abroad. These models are also easily interpretable: it is simple to identify the cause of an alert.

[2] This exemption is set out in Article 18 of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. The Observatory previously reiterated the principles applicable in this area in its 2022 annual report (Part 4.1.3).

[3] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market, 28 June 2023.

[4] SEPA – Single Euro Payments Area.

[5] Intermediary accounts, often manipulated by fraudsters, to allow money to be transferred from the accounts of victims to that of the fraudster.

➡ Unlike heuristic models, more sophisticated models using AI modules may be less responsive and are often harder to interpret, but at the same time open up broader fraud detection prospects at a time when frauds are also becoming increasingly sophisticated.

4.2.2.2 AI statistical models

Different types of AI models exist, but those whose purpose is to detect fraud fall mainly into the category of "supervised" models. Based on input data, they are designed to replicate a known response, such as delaying or blocking a transaction that has been identified as potentially fraudulent. The AI statistical models that are most widely used in this regard are as follows.

- **Logistic regression** estimates the probability of an event occurring based on a set of independent variables. The model generates a score $f(x)$, equivalent to a probability of between 0 and 1 for the fraudulent nature of a transaction, defined on the basis of its own characteristics x_i and their respective weightings w_i in the final score. It is a generalised linear model[6] using a logistic function[7] as link function.
  The problem of classification through logistic regression then becomes a simple question of optimisation where, based on the data, experts seek to obtain the set of parameters w_i that will enable the sigmoid curve to best fit the data.
- **A decision tree** is a machine learning (ML) algorithm used to make predictions or a classification. These models are used to partition the space in order to isolate cases of fraud (in red in Diagram 1) based on a series of simple logical rules applied to the transaction characteristics and summarised in Diagram 1 with two variables x_1 and x_2. These models are easy to interpret and train. Unlike with logistic regression, they make it possible to identify non-linear, and hence more complex, relationships, between the different characteristics of a fraudulent transaction.
- **A random forest** is an algorithm that combines the results of several decision trees trained on slightly different data subsets for a single result.

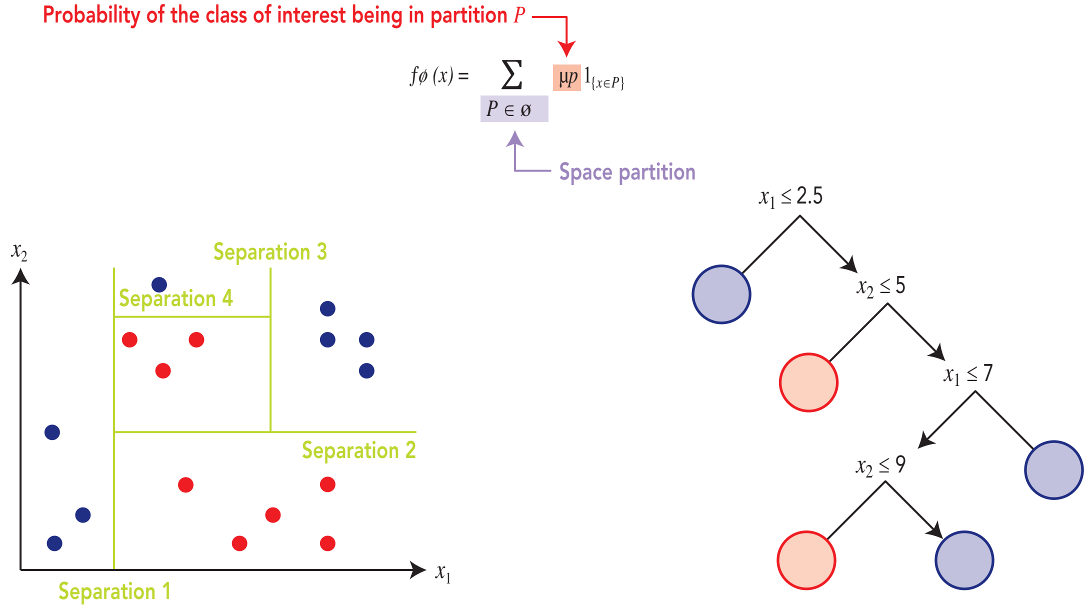
➡ The decision tree is one of the best types of ML algorithm. It offers real ease of interpretation and can be used to improve predictive models with precision. However, to detect fraud, some professionals believe that a logistic regression could be more effective than a decision tree and that a random forest is more effective than a logistic regression, because the relationships between the data are not linear.

- **Boosting** improves the precision and predictive performances of ML models by converting several weak models with low predictive capability into a single strong learning model with higher predictive accuracy.

D1 Statistical principle of the decision tree

a) Example of space partitioning

b) Decision tree associated with partitioning



Source: Observatory for the Security of Payment Means.

Although there are many different implementation variations, data scientists often use boosting with decision tree algorithms. An overall model is created by combining several weak decision trees sequentially. Data scientists assign output weights to individual trees, give a higher weighting to the incorrect classifications of the first decision tree, then modify the input weight in the next tree to correct these errors. After many cycles, the boosting method combines these weak rules into a single strong prediction rule.

➡ These models do a good job of capturing complex fraud schemes, but require special interpretability techniques, such as partial dependence plot (PDP) or accumulated local effect (ALE) approaches.

- **Deep learning neural networks** are ML statistical analysis models that use nodes, or interconnected neurons. This is a sub-set of ML, where the algorithms are variants of an ML algorithm called a neural network.

➡ Although these models should in theory do a better job of harnessing the many available data points, in practice they are less effective on structured payment data than in more traditional approaches.[8] In particular, they lack transparency in explaining transaction scores.

4.2.2.3 Graph Neural Network (GNN) AI models

The emergence of new types of data and the growing amount of unstructured data have spurred the creation of new ML models that are capable of adapting to unstructured data such as graphs.[9] They include GNNs, which build on the deep learning neural networks used to process structured data.

➡ GNNs make it possible to combine the scenarios used by expert models with a statistical approach. They can be used to obtain precise scores for transactions, while the results are more usable.

[6] The function *f(x)* is determined by a weighted linear combination: $f(x) = \sum_{i=1}^{n} w_i . f(x_i)$.

[7] In mathematics, logistic functions are functions with the expression: $f(t) = \frac{k}{1+ae^{-rt}}$ where k and r are positive real numbers and a is a real number. These functions provide values of between 0 and 1 for the dependent variable, irrespective of the values of the independent variable.

[8] See "Why do tree-based models still outperform deep learning on tabular data?", Léo Grinsztajn (Soda), Édouard Oyallon (*Institut des systèmes intelligents et de robotique*, ISIR, and *Centre national de la recherche scientifique*, CNRS) and Gaël Varoquaux (Soda), July 2022.

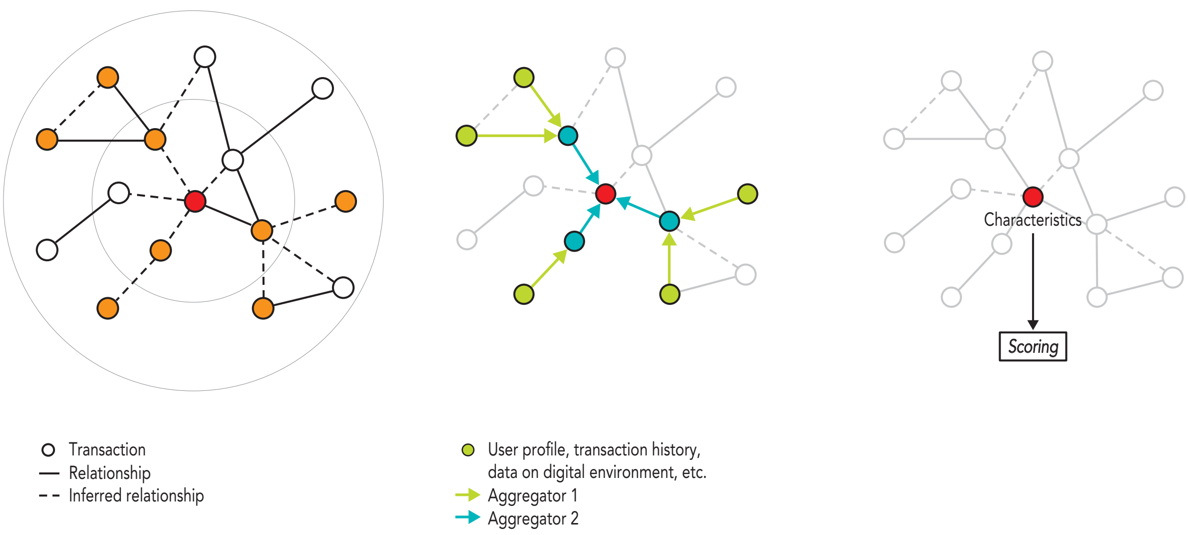
[9] A graph is a complex data structure used to represent objects and the relationships between them. A graph is comprised of a set of nodes and edges (or links).

D2 Illustration of a graph neural network applied to payment

a) Analyse the neighbourhood

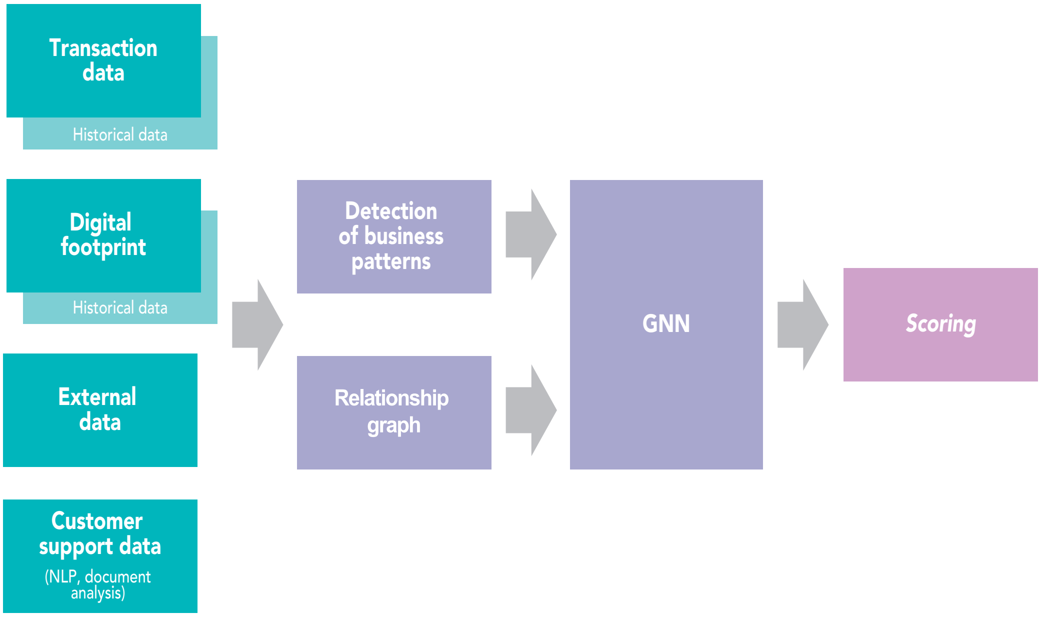
b) Aggregate information using neighbouring nodes

c) Determine scoring based on aggregate data (node classification)


Characteristics
Scoring
○ Transaction
— Relationship
- - Inferred relationship
● User profile, transaction history, data on digital environment, etc.
→ Aggregator 1
→ Aggregator 2

Source: Observatory for the Security of Payment Means.

D3 Simplified architecture of graph neutral network models associated with business scenarios



Source: Observatory for the Security of Payment Means.
Note: GNN, Graph Neural Network; NLP, Natural Language Processing.

➡ As a rule, ML models are powerful but also challenging to interpret. The usability of results may be facilitated by developing interpretive methods, such as the SHapley Additive exPlanations (SHAP) tool,[10] or the PDP and ALE approaches mentioned above. These methods make it possible to interpret non-linear models in the same way as linear models (sum of factor weights) and to better understand the effect of the model's characteristics on predictions.

4.2.3 Statistical performances in terms of fraud detection

4.2.3.1 Tools to measure model performance

Specific indicators are required to assess the ability of fraud detection models to generate meaningful alerts.

Another way to express false positives is to consider the number of legitimate transactions reported as alerts by the model to ultimately identify a single actual case of fraud: **the Receiver Operating Characteristic (ROC) curve is one of the most widely used measures in detection models**.

To represent the ROC curve, the first step is to classify all the transactions in a sample as either legitimate or fraudulent, according to the scores sent by the model. Beyond a given score, also called the classification threshold, transactions are the subject of an alert.

The true positive rate, called the **detection rate** in Table 1, is equal to the number of true positives divided by the sum of true positives and false negatives. True positives are transactions that are correctly classified as fraudulent, while false negatives are those that are incorrectly classified as legitimate.

The **false positive rate** is equal to the number of false positives divided by the sum of false positives and true negatives. False positives are transactions that are incorrectly classified as fraudulent, while true negatives are those that are correctly classified as legitimate.

For each threshold, the true positive rate and the false positive rate are calculated and reported on the ROC curve. The ROC curve shows the change in actual cases of fraud detected by the model's alerts, when the percentages of false positives with the most at-risk scores are taken into account.

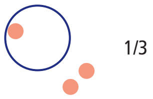
➡ There is an inverse relationship between the improvement in the recall rate and the improvement in the precision rate, creating a trade-off between the risk of not detecting a fraudulent transaction (recall rate too low) and the risk of generating too many alerts (precision rate too low).

T1 Main performance measures used with real-time fraud detection models

Recall (detection) rate: target of 100%

$$\frac{\textit{Number of fraudulent transactions that were the subject of alerts}}{\textit{Number of fraudulent transactions}}$$

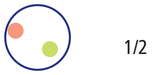
A recall rate of 33% means that 1 fraud out of 3 was detected by the model.



Precision rate: target of 100%

$$\frac{\textit{Number of fraudulent transactions that were the subject of alerts}}{\textit{Number of alerts raised by the model}}$$

A precision rate of 50% means that 1 alert out of 2 is an actual case of fraud.



F-score: target of 100%

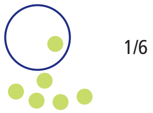
$$F = 2 * \left(\frac{\textit{precision rate} \ * \textit{recall rate}}{\textit{precision rate} + \textit{recall rate}} \right)$$

The F-score (or F1 score) computes an average of precision and recall, but note that the precision rate decreases as the recall rate rises.
It is a widely used measure by payment fraud detection models.

False positive rate: target of 0%

$$\frac{\textit{Number of legitimate transactions identified as high risk by the model}}{\textit{Number of legitimate transactions}}$$

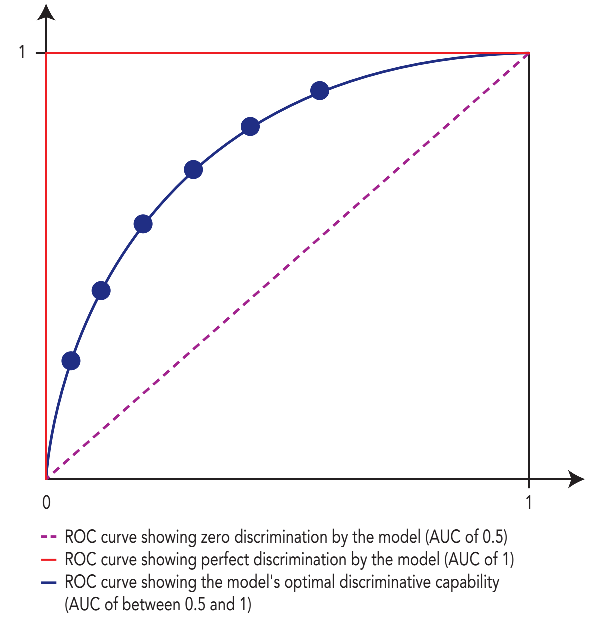
A false positive rate of 16.6% means that the model raises an alert about an event that is not an actual case of fraud for every six legitimate transactions.



Source: Observatory for the Security of Payment Means.

D4 Guide to understanding the ROC curve

(x-axis: false positive rate; y-axis: detection rate)



Source: Observatory for the Security of Payment Means.

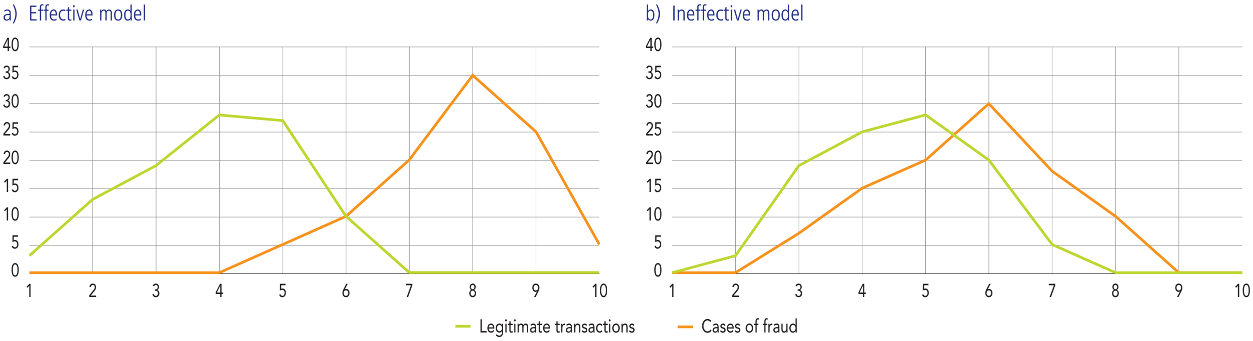
Guide: A perfect model can identify 100% of actual cases of fraud, with a zero false positive rate. A model that does not offer any particular discrimination detects as many fraudulent transactions as it generates false positives.
Two models can be compared by looking at the area under their respective ROC curves (AUC-ROC). The model is perfect if its AUC is equal to 1.
Note: Receiver Operating Characteristic (ROC); Area Under Curve (AUC).

➡ In addition, the precision indicator faces a paradox: in the event of a structural decrease in an institution's fraud rate, the precision rate may go down even though the recall rate stays constant, causing the F-score to collapse. Yet it would be a mistake to stop using the model, since its performance will recover in the event that fraud picks up again.

Besides these measures, a direct approach based on studying statistical distributions could prove highly complementary: the graphical representation of scores assigned by the model to legitimate transactions and instances of fraud can be used to intuitively assess the model's discriminatory performance. Chart 1 llustrates this approach with a model that discriminates ten scores, from 1 to 10 (10 being the riskiest score): a larger overlap between the curves for cases of fraud and legitimate transactions denotes a less efficient model.

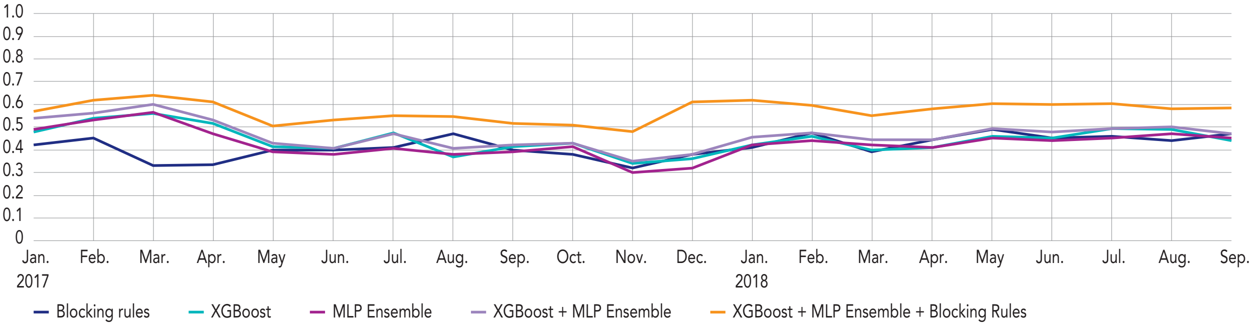
10 See "A unified approach to interpreting model predictions", Scott Lundberg and Su-In Lee, Conference on Neural Information Processing Systems (NeurIPS), 2017.

C1 Two cases of model performance (x-axis: model score, from 1 (low risk) to 10 (high risk); y-axis: probability density as a %)



Source: Observatory for the Security of Payment Means.

C2 Performance of different card fraud detection models (calibrated F-score)



Source: Observatory for the Security of Payment Means.

Note: Blocking rules show the F-score of the expert model; XGBoost and Multi-Layer Perceptron (MLP) – artificial intelligence models.

4.2.3.2 Fit between expert and AI models

The predictive capability of expert and AI models is cumulative. Practice has shown that using expert models as an initial filter for transactions and inputting the result to AI-based statistical models is a way to detect fraud more effectively.

The example shown in Chart 2 illustrates the value added of AI relative to an already relatively effective expert model based on statistics provided by a contributor to this study between January 2017 and September 2018. The F-score of the expert model (Blocking Rules) is comparable to those of XGBoost and Multi-Layer Perceptron (MLP) AI models. Combining two AI models does not deliver significantly better performances than the expert model. But combining the expert model with AI models (orange curve) boosts the F-score by up to 50%: here, it increases from 40% to 60% between November and December 2017.

4.2.3.3 Backtesting and retraining models

After being trained on a specific set of data, a model may prove effective in a given setting but then see its performances fall off when it is applied to an environment that has changed. The most commonly observed types of model drift are as follows.

- **Covariate shift**, also known as data drift: this refers to a shift in the distribution of the data input to the model, which tend to change as a function of users' payment habits and the new processes employed by fraudsters.
- **Concept drift**: in predictive analysis and ML, concept drift occurs when the statistical properties of the target variable, which the model is trying to predict, change over time in an unforeseen manner. The relationship between the target and the model's characteristics changes, and predictions become less accurate over time. This could happen, for example, when fraudsters find ways to circumvent countermeasures put in place by a PSP after detecting a new fraud scheme.

There are several possible actions that may be taken to maintain the ML model's performance.

- If the drift is due to a covariate shift, correcting and improving data quality should rectify the situation;

- By using backtesting processes to regularly monitor model performances, it is possible to conduct model retraining sessions.

However, if correcting the data or retraining the model is not enough, a new model may have to be built.

4.3 Business challenges

A team of modellers is required to set up advanced scoring systems. This team could be integrated within the company itself or outsourced to a specialist provider. Whatever the case, **it is essential that the teams responsible for modelling and those in charge of managing payment transactions communicate and cooperate closely** to design and implement effective models.

➡ As a rule, human judgement is quicker at identifying a new and unexpected type of attack and at proposing an adequate countermeasure. But once the attack type has been established, AI-driven fraud detection models will be better at spotting future fraud attempts.

4.3.1 Selecting the decision threshold (or alert threshold)

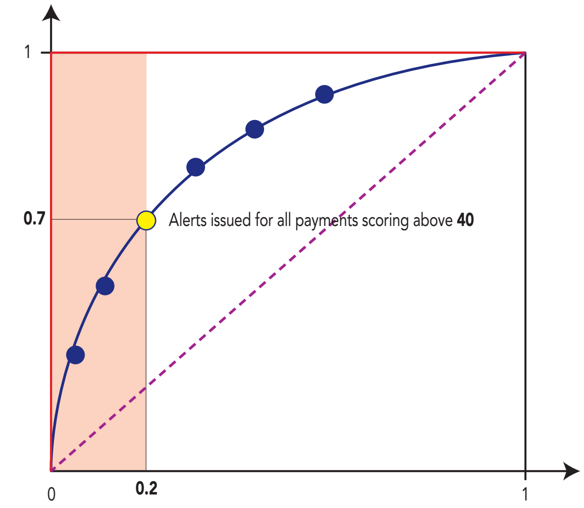
The **decision threshold** is the scoring threshold that, when crossed by transactions, triggers an alert. To facilitate business choices, tools have been developed that cater to operational challenges. One of the most widely used is directly inspired by the ROC curve *(see Section 4.4.1)* and is shown in Diagram 5:

- the x-axis shows the challenge rate, which is the percentage of alerts to be processed by the back office divided by the total number of transactions;
- the y-axis shows the recall rate, which is the total number of fraudulent transactions subject to an alert divided by the total number of fraudulent transactions.

4.3.2 Close collaboration between modelling and business teams to promote system agility

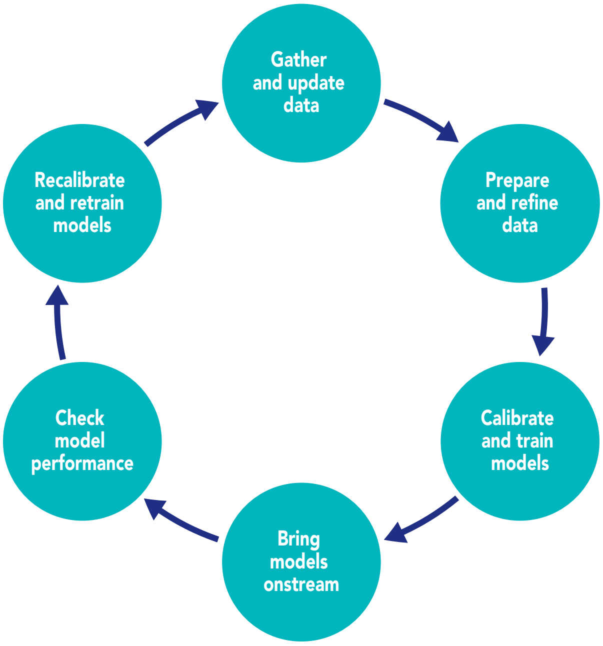
Faced with the constantly evolving techniques employed by fraudsters, close collaboration is needed between the teams responsible for modelling and those in charge of payment transactions, to ensure that the fraud detection system is sufficiently agile.

D5 Alert threshold as a function of the challenge rate and recall rate
(x-axis: challenge rate; y-axis: recall rate)



Source: Observatory for the Security of Payment Means.
Guide: The higher the alert threshold rises, the lower the point moves on the blue curve.
In this example, by setting an alert threshold at 40/100, the back office must challenge 20% of orders, making it possible to cover 70% of fraudulent transactions.

D6 ModelOps approach



Source: Observatoire de la sécurité des moyens de paiement.
Note: Approach describing governance of the lifecycle of an AI model.

To rationalise the development and implementation of appropriate models, modelling teams could adopt the principles of the ModelOps approach *(see Diagram 6)*, a method for managing model lifecycles devised by Gartner, a research and consulting firm. To do this, they need to build their knowledge of fraud. This entails (i) understanding the different payment processes, the source and significance of available data as well as trends in the various techniques employed by fraudsters, and also (ii) communicating effectively with the operations business line.

In addition, to manage time constraints more effectively, having close ties between modelling and business teams can facilitate database enrichment and help in monitoring model performances. When a new alert is received, back-office analysts study the transaction to determine whether it is an actual case of fraud. While some cases are clear-cut, others may require further investigation. The complexity of AI models may be such that analysts have to make repeated information requests to the modelling team in order to better understand the source of alerts.

Furthermore, once the model has been designed, and certainly before it comes into use, modelling teams must check with IT teams that servers have the requisite resources to allow information to be conveyed securely and comply with the maximum risk score computation times set by sector standards. Specifically, the total time allowed for payment IT processing is governed by international standards set by EMVco[11] for cards and the European Payments Council[12] for SEPA instruments.

4.4 Compliance challenges

The compliance of real-time fraud detection models lies at the confluence of several regulations, including Europe's General Data Protection Regulation (GDPR), the Artificial Intelligence Regulation, and the Second European Payment Services Directive (PSD 2) supplemented by regulatory technical standards and prudential rules for the management of operational risk.[13]

4.4.1 Absence of new regulatory restrictions for operational processes

Compliance with the GDPR[14] is a key challenge for the payment sector. The regulation's application to the data of real-time fraud detection models, while requiring material precautionary measures, does not raise major obstacles from an operational perspective:

- **Lawfulness of collecting data from customers:**
  – GDPR Article 6, paragraph 1 (f) states that collection is lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller […]";
  – as regards the processing of sensitive data (biometrics, health services payment data, etc.), GDPR Article 9, paragraph 2 (g) states that their use is not prohibited if "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued […]".

In both cases, preventing fraud is a purpose that aims to achieve legitimate interests. This is explicitly confirmed by PSD 2, whose Article 94 permits "processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud".[15]

- **Anonymisation of databases**:[16] the European Data Protection Board (EDPB) considers that "the processing of personal data strictly necessary for the purposes of preventing fraud could constitute a legitimate interest of the payment service provider concerned, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject".

➡ Modelling teams do not need to process databases including non-anonymous personal data. These bases should therefore be anonymised following guidance from the *Commission nationale de l'informatique et des libertés* (CNIL – French Data Protection Agency).

- **Permission to use data**: GDPR Article 13, paragraph 2 (f) states that the controller shall, at the time when personal data are obtained, provide the data subject with information about the logic underpinning the algorithm used, as well as the significance and the envisaged consequences of such processing for the data subject. In the event of a request, only the broad principles need to be explained; the algorithm itself may remain confidential. Accordingly, disclosures to persons about the use of their data to detect attempted fraud are generally provided in contracts and agreements linked to the account and means of payment.
- **Data retention**: according to the European Data Protection Board (EDPB), the principle that models to detect fraudulent transactions should be auditable, expressed in Article 3 of Commission Delegated Regulation 2018/389 on strong authentication,[17] may, by virtue of its explicit legitimacy, be invoked against GDPR Article 17 on the right to erasure and Article 18 on the right to restriction of processing.
- **The full impact of the European Artificial Intelligence Regulation of 13 June 2024** is not yet clear, but no major obstacles to using scoring algorithms for payment transactions were noted by the contributors to this Observatory study.

4.4.2 Issues arising in connection with PSD 2

PSD 2 encourages PSPs to implement real-time fraud detection models, in particular to be able to apply a strong authentication exemption. In its draft Payment Services Regulation (PSR), the European Commission seeks to support and clarify this stance by identifying transaction monitoring mechanisms as a central component of payment security and a key supplement to strong authentication.[18] Accordingly, the future European regulation may facilitate the sharing of fraud-related data between PSPs, which is currently bound by certain aspects of the GDPR and banking secrecy legislation.[19] Data sharing by PSPs could enrich their respective fraud detection models.

4.4.2.1 Strong authentication exemption as a factor in making payments smoother

As part of the application of PSD 2, Article 18 of Commission Delegated Regulation 2018/389 allows PSPs to be exempt from strong authentication if they conduct a transaction risk analysis (TRA), provided that those PSPs requesting an exemption report a fraud rate below the threshold set out in the annex to the regulation. The Observatory detailed the exact requirements for implementing the TRA exemption in its 2022 annual report *(see Section 4.1.3)*.

➡ TRAs conducted for the purpose of strong authentication exemption may be conducted using AI modules by some participants and have the practical effect of facilitating the execution of transactions by customers within a secure framework.

4.4.2.2 Sharing of fraud notes on transactions subject to strong authentication by the issuing PSP

PSD 2 gives the payer's PSP responsibility for the security of payment transactions, including responsibility for reimbursement in the event of an unauthorised transaction. Accordingly, a transaction must be assessed as having a low level of risk in order to be exempted from strong authentication; such assessment must be able to draw on information about the transaction provided by the merchant and the acceptor.

➡ Issuing PSPs must strive, as far as possible, to inform other payment chain participants, including acceptors and merchants, about cases of fraud that involve them directly so that they can improve the performances of their own fraud detection models. This cooperation may also encourage acceptors and merchants to monitor the quality of data conveyed in payment flows to PSPs.

4.5 Recommendations

Following this study, the Observatory for the Security of Payment Means is issuing three recommendations for the use of AI modules in fraud prevention systems by payment chain participants.

[11] EMVco was set up in 1999 to provide worldwide management of Europay Mastercard Visa (EMV) specifications, which are international standards for payment cards and their security.

[12] The European Payments Council (EPC) is an association that was set up in June 2002 to help implement and promote the European Union's Single Euro Payments Area (SEPA).

[13] According to the French decree of 3 November 2014 on the internal control of companies in the banking, payment services and investment services sector, institutions are required to manage their operational risks, which include the risks of internal and external fraud defined in Article 324 of Regulation (EU) No. 575/2013.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[15] PSD 2 Article 94 was transposed into Articles L. 521-5 and L. 521-6 of France's Monetary and Financial Code.

[16] European Data Protection Board, Guidelines 06/2020 on the Interplay of the Second European Payment Services Directive and the GDPR, June 2020.

[17] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

[18] Recital (100) of the Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (PSR), 28 June 2023.

[19] Banking secrecy is the legal obligation placed on banks to refrain from sharing customer data with third parties. Banking secrecy was introduced in France by Banking Act No. 84-46 of 24 January 1984 and is now laid down by Article L. 511-33 of the French Monetary and Financial Code.

Recommendation No. 1:

Explore, for the purpose of fraud prevention, the contribution of AI modules to models used to monitor and score payment transactions

The Observatory calls on members of the payment chain to assess the value of supplementing their existing approach by integrating AI technologies into their systems to analyse the risks of fraud in real time.

Recommendation No. 2:

Optimise the scope of data used in models to monitor and score payment transactions

The Observatory urges members of the payment chain to harness all usable data in their risk analysis systems:

- (i) by monitoring in particular the quality and exhaustiveness of data exchanged in payment messages, in accordance with applicable standards (EMVco, EPC, etc.);
- and (ii) by integrating information derived from existing sharing mechanisms (such as risk scores generated by interbank payment systems or information provided by telephone companies via shared interfaces) and future mechanisms (such as the payee verification service or fraud data sharing schemes provided for under forthcoming future domestic and European regulations).

Recommendation No. 3:

Set up a system to steer AI-driven models to monitor and score payment transactions

The Observatory calls on members of the payment chain to employ backtesting methods to assess, at least once a year, the effectiveness of scoring models integrating AI modules, based on quantitative indicators (of the types described in Part 2.3), supplemented by qualitative expertise that involves analysts with responsibility for operations. To this end, it is essential to make sure that the methodologies, assessments and checks associated with models are documented, understandable and explainable.

APPENDICES

Appendices 1 and 3 are available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2024

Appendices 2 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/2025-11/OSMP_2024_EN_Appendix-5-Statistical-data.xlsx

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 (*Code monétaire et financier*).

SCOPE

Under Article 65 of Law No. 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 was amended to extend 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 payment methods are covered by the Observatory.

- **Credit transfers** are facilitated by a payment service provider (PSP) holding the payer's payment account. The PSP credits, after 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 linked to a payment account enabling the cardholder to make payments or withdrawals that will be debited according to a time frame 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 magnetically), 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.

- **Commercial papers** are marketable securities that state that the bearer holds a claim for payment of a sum of money and serve for that payment. Commercial papers include trade bills 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.

- Monitoring the implementation of measures adopted by issuers, merchants and businesses to strengthen the security of means of payment.

- Compiling statistics on fraud. Accordingly, issuers of means of payment send the data 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.

- Monitoring 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, and encouraging the exchange of information between its members, while respecting the confidentiality of certain information.

The Observatory's proposals for analysing and combating breaches of payment means security are issued in the form of recommendations. In addition, under the terms of Article R. 141-2 of the French Monetary and Financial Code, the French Minister for the 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 French state government;
- the Governor of the Banque de France or a representative;
- the Secretary General of the ACPR (French Prudential Supervision and Resolution Authority);
- a representative of the French Data Protection Authority (*Commission nationale de l'informatique et des libertés*);
- eight representatives of issuers of payment instruments;
- seven representatives of payment systems operators;
- five representatives of consumer associations;
- eight representatives of retailers and businesses in the retail, mass distribution, teleshopping and e-commerce sectors in particular;
- two representatives from electronic communications operators;
- two representatives from associations working with and for persons with disabilities;
- two people qualified on the basis of their expertise.

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

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

The chairman is chosen from among these members by the French Minister for the Economy and Finance and appointed for a renewable term of three years. Denis Beau, First Deputy 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 in closed session. The measures proposed by the Observatory are adopted if an absolute majority is reached. 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 the 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 the 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 any information brought to their attention in the course of their duties confidential. To this end, the Observatory's internal rules include a requirement that all members express their commitment to keep all working documents strictly confidential to the chairman.

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 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.),
  - the procedures for using the means of payment or related data (payment/withdrawal, in person or remotely, via physical use of the payment instrument or related data, etc.),
  - the geographical area 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 an entry in the account of at least one of the transaction's counterparties which was subsequently rejected on the grounds of fraud. Fraud does not include attempted fraud, where fraud is stopped before the transaction is carried out.

Also excluded from the definition of 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 disputing the payment 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 the accomplice of a swindler, and the product or service purchased does not exist and is therefore not delivered (for example, the illicit sale of financial instruments such as investment products or loan subscriptions).

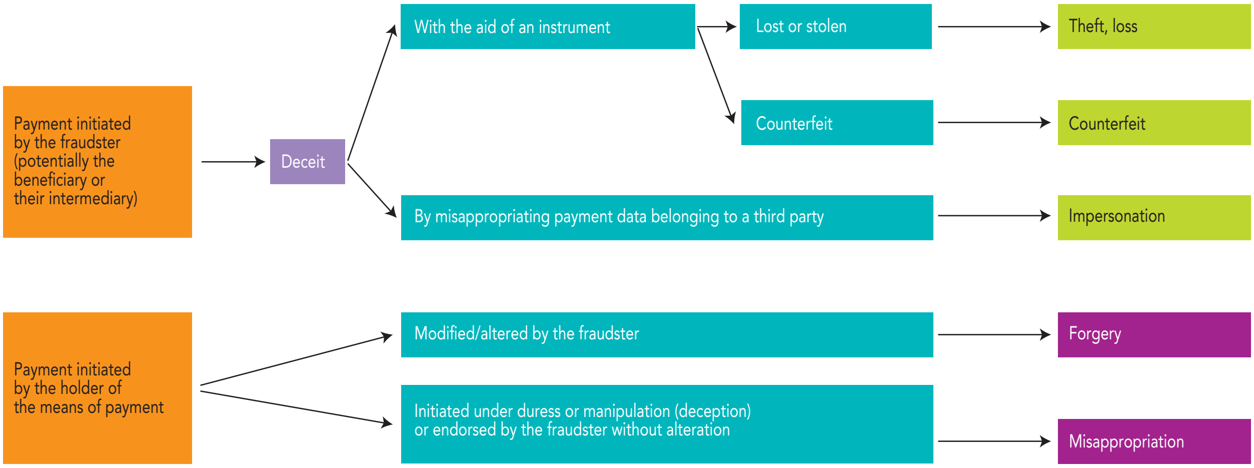
Fraud is assessed using the "gross-fraud" approach. It takes the initial defrauded amount in a payment transaction without taking into account any measures that may subsequently be taken by the counterparties to reduce the loss (for example, interrupting the delivery of products or the provision of services, amicable agreements to reschedule payment in the event of improper payment rejection, damages following legal action, etc.).

Source of fraud data

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

[1] Guideline drawn up under Article 96(6) of the Second European Payment Services Directive in the Internal Market (EU Directive 2015/2366, known as "PSD 2").

Schematic presentation of the different types of fraud


Payment initiated by the fraudster (potentially the beneficiary or their intermediary)
Deceit
With the aid of an instrument
Lost or stolen
Theft, loss
Counterfeit
Counterfeit
By misappropriating payment data belonging to a third party
Impersonation
Payment initiated by the holder of the means of payment
Modified/altered by the fraudster
Forgery
Initiated under duress or manipulation (deception) or endorsed by the fraudster without alteration
Misappropriation

Note: This schematic presentation should be read in conjunction with the Banque de France's official guidance 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, whose application differs depending on the payment instrument:

- **deceit** (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 provider – PSP), lost or counterfeited, or by misappropriating bank data or identifiers (spoofing);
- **forgery**: 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 a payer acting under duress or manipulation (deception) without alteration or modification of an attribute by the fraudster.

Geographical breakdown of payment fraud

Fraud data are broken down into domestic, European and international transactions. Until 2020, European transactions had been measured within the Single Euro Payment Area (SEPA). Since 2021, however, 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 fell outside the EEA in 2020 as a result of Brexit.

MEASURING PAYMENT CARD FRAUD

Transactions covered

Payment card fraud, as measured in this report, concerns payment transactions (in person 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 with regard to the nature of the payment channel used (interbank[2] or private[3]) or the category of card involved (debit card, credit card, commercial card or prepaid card).

Source of fraud data

Data on payment card fraud come from the payment systems, not payment service providers, and are collected by the Banque de France on behalf of the Observatory from:

- members of *Groupement des Cartes Bancaires CB*, MasterCard, Visa Europe, American Express, UnionPay and Japan Credit Bureau (JCB);
- the main private label card issuers operating in France.

Elements in the analysis of fraud

Payment card fraud is analysed on the basis of several parameters: types of fraud, payment initiation channels, geographical areas where the card or the data attached to it are issued and used and, for remote payments, the business sectors of the merchants involved, as well as the internet payment method used.

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

[3] The term "private" refers to card payment systems involving a single payment service provider, which operates as both the card issuer and the payment processor.

Types of payment card fraud	Fraud method
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 is intercepted when it is sent by the issuer to its legitimate holder, in a fraud method similar to loss or theft, with the difference that in this case cardholders are not sure 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	Counterfeiting a payment card involves either modifying the data in the magnetic strip, 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 – with or without manipulation of the payer with the aim of obtaining their confidential codes or performing strong authentication.
Other	This category includes any other method of fraud, such as the use of a card number that is consistent but not assigned to a cardholder and then used in remote sales, alteration of a legitimate payment order (forgery), etc.

a) Modification of the card numbers embossed on the card.
b) A fraud technique whereby an issuer's own rules are used to generate card numbers.

Card use channels	Methods of use
Point-of-sale payment and ATM	Payments made at the point of sale or at a machine, including contactless payments.
Remote payment (excluding internet)	Payments made by post, electronic mail (email) or fax/telephone, often referred to as a MOTO ("Mail Order, Telephone Order") settlement, by card payment systems.
Internet payment	Payments made on the internet (on the merchant's website or via an application).
Withdrawal	Cash withdrawals at an automatic teller machine (ATM).

Types of payment on the internet	Description
3-D Secure payment with strong authentication	Payments made over the internet using the 3-D Secure infrastructure with strong cardholder authentication.
Payment excl. 3-D Secure with strong authentication	Payments made online over the internet, outside the 3-D Secure infrastructure, with strong authentication delegated to a third party, in accordance with the outsourcing requirements applicable under PSD 2 (e.g. an X-Pay-type mobile wallet offered under the responsibility of the issuer, delegation of strong authentication to the merchant under the responsibility of the issuer, etc.).
3-D Secure payment without strong authentication	Payments made over the internet using the 3-D 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 payments made outside the 3-D Secure infrastructure, including: • payments not subject to European rules on strong authentication (PSD 2),[a] such as payments initiated by the creditor on the basis of a pre-existing agreement between the payer and the creditor (for example: Merchant Initiated Transaction – MIT) and "one-leg" payments (where the issuer or the processor of the payment is located outside the European Union); • payments subject to European rules on strong authentication, but for which the reason for exemption is formalised in the authorisation flow; • payments subject to European rules on strong authentication, but not compliant.

[a] The European rules on strong authentication are set out in a delegated act for 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
Domestic transaction	The issuer and the acceptor are both established in France.[a] However, for remote payments, the fraudster may operate from abroad.
Outgoing European transaction	The issuer is based in France and the acceptor is based abroad in the European Economic Area (EEA).
Outgoing international transaction	The issuer is based in France and the acceptor is based abroad outside the European Economic Area (EEA).
Incoming European transaction	The issuer is based abroad in the European Economic Area (EEA) and the acceptor is based in French territory.
Incoming international transaction	The issuer is based abroad outside the European Economic Area (EEA) and the acceptor is based in French territory.

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

Merchant's sector of activity for remote internet and non-internet payment	Description
Food	Grocery stores, supermarkets, hypermarkets, etc.
Account loading and person-to-person sales	Online sales sites between individuals, etc.
Insurance	Insurance policy subscriptions.
Generalist and semi-generalist trade	Textiles and clothing, generalist department stores, catalogue sales, private sales, etc.
Household goods	Sales of furnishings and DIY products.
Online gaming	Online gaming and betting sites.
Technical and cultural products	Computer hardware and software, photographic equipment, books, CDs, DVDs, etc.
Health, beauty and personal care	Sales of pharmaceutical products, personal care products and cosmetics.
Personal and professional services	Hospitality, rental services, box office, charities, office equipment, courier services, etc.
Telephony and communication	Telecommunication and mobile telephony equipment and services.
Travel and transportation	Rail, air and sea.
Other	Merchants that do not correspond to any of the above categories.

MEASURING CREDIT TRANSFER FRAUD

Payment instruments covered

Credit transfer fraud, as measured in this report, concerns payment orders given by the payer (understood to be 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).

Source of fraud data

Data on credit transfer fraud are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by approved payment service providers[4] as part of the Banque de France's "Census on cashless payment fraud". PSPs report these data in their capacity as the institution servicing the payer in the transaction.

Elements in the analysis of fraud

Credit 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.

[4] 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 (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	Fraud method
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 issuance and transfer 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, "France" includes mainland France, the overseas departments and regions (Guadeloupe, French Guiana, Martinique, Réunion, Saint Pierre and Miquelon, Mayotte, Saint Barthélemy and Saint Martin) and the Principality of Monaco. French Polynesia, Wallis and Futuna and New Caledonia are not included and are not members of the European Union. Transactions between France and these last territories are therefore accounted for as international transactions.

Initiation channels used	Methods of use
Non-electronic means (post, courier, telephone, etc.)	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 orders 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 orders 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, bank counter)	Transfer orders initiated at a bank branch counter or from an automatic teller machine (ATM).
Payment Initiation Service Providers (PISPs)	Transfer orders 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 mandate) 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).

Source of fraud data

Data on direct debit fraud are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by approved payment service providers as part of the Banque de France's "Census on cashless payment fraud". PSPs report these data 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	Fraud method
Deceit	The fraudster, acting as creditor, issues direct debits to account numbers obtained illegally without any authorisation or underlying economic reality ("unauthorised payment transaction" per the European Banking Authority – EBA).
Misappropriation	The fraudster, acting as debtor, uses the identity and international bank account number (IBAN) 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" per the EBA).

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

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

Initiation methods	Description
Direct debits initiated on the basis of a single payment	Electronically initiated direct debits that are independent of other direct debits.
Direct debits initiated from a file or batch	Direct debits 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 the only means of authentication is the payer's signature. As such, banks cannot 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 a 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 those 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.

Source of fraud data

Data on cheque fraud are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by payment service providers as part of the Banque de France's "Census on cashless payment fraud". PSPs report these data in their capacity as the institution receiving cheques for collection from their customers (as remitting institutions).

Elements in the analysis of fraud data

Cheque fraud data are analysed on the basis of the main types of fraud defined by the Observatory. The table below summarises the most commonly observed types of cheque fraud and the methods used.

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).

Since 2021, gross-fraud data for cheques have excluded 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 fraud detected after the cheque has been presented for payment. However, even from 2021 onwards, the breakdown of cheque fraud by type is still based on the former gross-fraud approach.

Types of cheque fraud	Fraud method
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 by the legitimate holder under duress).
Counterfeit	The fraudster entirely fabricates a counterfeit cheque, "issued" by an existing or fake bank.
Forgery	The fraudster intercepts a legitimate cheque and alters it by scratching, erasing or deleting the data.
Misappropriation/replay	Cheque lost or stolen after clearing in a payment system and presented again for collection (replay). 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 beneficiary's name is unchanged and the MICR (Magnetic Ink Character Recognition) line of numbers and characters at the bottom 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, concerns two payment instruments.

- *Lettre de change relevé* (LCR – trade bill): a document issued in 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.

Types and source of fraud data

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

Data on commercial paper fraud are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by payment service providers as part of the Banque de France's "Census on cashless payment fraud". PSPs report these data in their capacity as the institution receiving commercial paper for collection from their customers (as remitting institutions).

MEASURING FRAUD ON 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.

Source of fraud data

Fraud data on money remittances are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by payment service providers as part of the Banque de France's "Census on cashless payment fraud". PSPs report these 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 A PAYMENT INITIATION SERVICE PROVIDER (PISP)

Payment services covered

Payment initiation services correspond to Payment Service 7 as defined in Article L. 314-1 of the French Monetary and Financial Code, in accordance with the provisions of PSD 2, describing 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.

Source of fraud data

Fraud data on payment initiation services are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by payment service providers established or authorised to operate in France as part of the Banque de France's "Census on cashless payment fraud", with a breakdown by initiation channel.

Initiation channel	Description
Remote	Payments initiated over the internet from a computer, mobile phone or similar terminal.
In person	Payments initiated at the point of sale, at an ATM or at a 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").

There are two categories of electronic money instruments:

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

Source of fraud data

Data on e-money payment fraud are provided to the Observatory by the Banque de France and come from the half-yearly regulatory fraud declarations made by electronic money issuers as part of the Banque de France's "Census on cashless payment fraud". Electronic money issuers provide these data with a breakdown by initiation channel (regardless of the medium used, whether a physical medium or an online account held by the institution).

Initiation channel	Description
Remote	Payments initiated over the internet from a computer, mobile phone or similar terminal.
In person	Payments initiated at the point of sale, at an ATM or at a bank counter, including using contactless systems, with the payer physically present.

A5 STATISTICAL DATA ON MEANS OF PAYMENT USE AND FRAUD

You can download the tables in this appendix and additional tables at the following address: ***https://www.banque-france.fr/system/files/2025-11/OSMP_2024_EN_Appendix-5-Statistical-data.xlsx***

OVERVIEW OF MEANS OF PAYMENT

T1 Cashless payment means used in France in 2024

(volume in millions, value in EUR billions, average value in euro, changes and shares in %)

	Number of transactions			Value of transactions			Average value
	2024	Change 2024/2023	Share	2024	Change 2024/2023	Share	
Payment by card[a]	20,982	6.6	62.1	844	4.6	2.4	40
of which contactless	*11,454*	*6.1*	*33.9*	*204*	*16.7*	*0.6*	*18*
of which mobile payment	*2,473*	*53.6*	*7.3*	*56*	*57.6*	*0.2*	*23*
Cheque	784	-12.1	2.3	392	-16.1	1.1	500
Credit transfer	5,973	6.4	17.7	31,108	3.9	89.2	5,209
of which LVT[b]	*11*	*-64.1*	*0.0*	*10,408*	*22.0*	*29.9*	*976,136*
of which instant transfers (SCT Inst)	*598*	*46.5*	*1.8*	*231*	*30.6*	*0.7*	*387*
Direct debit	4,788	3.7	14.2	2,178	1.9	6.2	455
Commercial paper	70	-4.8	0.2	205	-5.6	0.6	2,926
Electronic money	98	11.2	0.3	1	25.9	0.0	13
Money remittance	12	51.6	0.0	1	32.4	0.0	128
Total	**32,707**	**5.6**	**96.8**	**34,730**	**3.4**	**99.6**	**1,062**
Withdrawal by card[a]	1,079	-4.2	3.2	133	-1.6	0.4	124
Total transactions	**33,787**	**5.2**	**100.0**	**34,864**	**3.4**	**100.0**	**1,032**

a) Cards issued in France only.
b) LVT: large-value transfers issued via large-value payment systems (TARGET2, Euro1); professional payments only.

Source: Observatory for the Security of Payment Means.

Note: SCT Inst, SEPA Instant Credit Transfer; SEPA, Single Euro Payments Area.

T2 Historical development of cashless payment

a) In volume terms

(in millions of transactions)

	2017	2018	2019	2020	2021	2022	2023	2024
Card	12,581	13,179	14,485	13,852	16,129	18,258	19,685	20,982
of which contactless	*1,300*	*2,374*	*3,779*	*5,159*	*7,369*	*9,103*	*10,792*	*11,454*
of which by mobile	*5*	*11*	*48*	*129*	*357*	*845*	*1,609*	*2,473*
Cheque	1,927	1,747	1,587	1,175	1,106	1,008	891	784
Credit transfer	3,870	4,038	4,269	4,483	4,843	5,158	5,613	5,973
of which instant transfers (SCT Inst)	*na*	*0*	*14*	*45*	*107*	*198*	*408*	*598*
Direct debit	4,091	4,211	4,370	4,622	5,020	4,914	4,616	4,788
Commercial paper	81	81	78	71	75	75	74	70
Electronic money	55	65	62	36	63	75	88	98
Money remittance	18	16	16	15	2	3	8	12
Total cashless payments	**22,605**	**23,320**	**24,851**	**24,238**	**27,238**	**29,491**	**30,975**	**32,707**
Withdrawal by card	1,481	1,439	1,392	1,064	1,086	1,136	1,127	1,079
Total transactions	**24,086**	**24,759**	**26,243**	**25,302**	**28,324**	**30,627**	**32,102**	**33,787**

b) In value terms

(EUR billions)

	2017	2018	2019	2020	2021	2022	2023	2024
Card	530	568	600	578	660	746	806	844
of which contactless	*13*	*25*	*43*	*80*	*125*	*148*	*175*	*204*
of which by mobile	*0.1*	*0.2*	*1*	*3*	*8*	*18*	*36*	*56*
Cheque	1,002	891	814	614	589	540	467	392
Credit transfer	24,069	24,296	25,164	32,712	38,723	38,895	29,942	31,108
of which instant transfers (SCT Inst)	*na*	*0,086*	*7*	*27*	*50*	*119*	*177*	*231*
Direct debit	1,579	1,645	1,711	1,684	1,895	2,041	2,139	2,178
Commercial paper	260	252	232	197	212	222	218	205
Electronic money	1	1	1	1	1	1	1	1
Money remittance	1.6	2	2	2	1	1	1	1
Total cashless payments	**27,440**	**27,653**	**28,522**	**35,786**	**42,081**	**42,445**	**33,574**	**34,730**
Withdrawal by card	135	137	137	116	124	133	136	133
Total transactions	**27,575**	**27,789**	**28,658**	**35,902**	**42,204**	**42,578**	**33,710**	**34,864**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: SCT Inst, SEPA Instant Credit Transfer; SEPA, Single Euro Payments Area.

T3 Breakdown of payment means fraud in 2024

(value and average value in euro; volume in units; changes and shares in %)

	Volume			Value			Fraud rate	Average
	2024	Change 2024/2023	Share	2024	Change 2024/2023	Share	2024	
Payment by card[a]	7,313,235	10.2	94.0	478,062,959	5.0	40.2	0.0567	65
of which contactless	*746,923*	*1.8*	*9.6*	*22,648,147*	*20.6*	*1.9*	*0.0111*	*30*
of which by mobile	*129,052*	*17.2*	*1.7*	*9,023,196*	*23.7*	*0.8*	*0.0161*	*70*
Cheque (new approach)[b]	173,366	-15.9	2.2	270,317,625	-25.7	22.7	0.0689	1,559
Cheque (former approach)	215,576	-15.7	2.8	457,332,103	-22.2	38.5	0.1166	2,121
Credit transfer	132,298	46.3	1.7	350,992,884	12.3	29.5	0.0011	2,653
of which instant transfers (SCT Inst)	*80,394*	*65.3*	*1.0*	*105,718,759*	*53.2*	*8.9*	*0.0457*	*1,315*
Direct debit	52,718	-32.3	0.7	30,365,272	36.0	2.6	0.0014	576
Commercial paper	350	929.4	0.0	18,037,208	1,291.1	1.5	0.0088	51,535
Electronic money	3,232	3.1	0.0	95,876	-45.6	0.0	0.0077	30
Money remittance	86	-15.7	0.0	17,796	-67.8	0.0	0.0012	207
Total payments	**7,675,285**	**9.4**	**98.6**	**1,147,889,620**	**-0.7**	**96.6**	**0.0033**	**150**
Withdrawal by card[a]	108,013	-2.0	1.4	40,763,581	0.4	3.4	0.0306	377
Total transactions	**7,783,298**	**9.3**	**100.0**	**1,188,653,201**	**-0.6**	**100.0**	**0.0034**	**153**

a) Cards issued in France only.

b) The new approach to cheque fraud excludes fraud that is thwarted after the cheque has been presented to be cashed.

Source: Observatory for the Security of Payment Means.

Notes: SCT Inst, SEPA Instant Credit Transfer; SEPA, Single Euro Payments Area.

Since 2021, total cashless payment fraud has incorporated a new approach to cheque fraud, which excludes fraud that is prevented after the cheque has been presented to be cashed, and includes fraud on electronic money and money remittances.

T4 Historical development of fraud involving payment means

a) In volume terms

(in units)

	2017	2018	2019	2020	2021	2022	2023	2024
Cards	5,364,312	6,068,959	7,071,095	7,421,137	6,764,752	6,692,988	6,635,955	7,313,235
of which contactless	*248,991*	*445,919*	*603,509*	*537,061*	*604,278*	*796,027*	*733,359*	*746,923*
of which by mobile	*22*	*2,070*	*3,494*	*33,761*	*83,266*	*162,869*	*110,133*	*129,052*
Cheque (new approach)	na	na	na	190,001	232,277	218,122	206,197	173,366
Cheque (former approach)	114,906	166,421	183,488	220,685	272,970	266,216	255,857	215,576
Credit transfer	4,642	7,736	15,934	35,893	46,718	76,846	90,453	132,298
of which instant transfers (SCT Inst)	*na*	*5*	*729*	*7,131*	*12,913*	*33,193*	*48,630*	*80,394*
Direct debit	25,801	309,377	43,519	6,485	251,010	49,453	77,876	52,718
Commercial paper	3	5	1	62	1	1	34	350
Electronic money	na	na	na	na	2,001	1,945	3,135	3,232
Money remittance	na	na	na	na	962	154	102	86
Total cashless payment fraud	**5,509,664**	**6,552,498**	**7,314,037**	**7,684,262**	**7,297,721**	**7,039,509**	**7,013,752**	**7,675,285**
Withdrawal by card	177,562	158,908	165,505	113,067	129,083	123,574	110,221	108,013
Total fraudulent transactions	**5,687,226**	**6,711,406**	**7,479,542**	**7,797,329**	**7,426,804**	**7,163,083**	**7,123,973**	**7,783,298**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: SCT Inst, SEPA Instant Credit Transfer; SEPA, Single Euro Payments Area.

b) In value terms

(in euro)

	2017	2018	2019	2020	2021	2022	2023	2024
Cards	344,962,084	401,604,986	428,249,931	439,489,315	421,410,285	420,585,823	455,204,894	478,062,959
of which contactless	*2,748,790*	*5,234,852*	*8,479,354*	*11,292,261*	*16,274,668*	*23,047,180*	*18,786,086*	*22,648,147*
of which by mobile	*1,227*	*73,682*	*216,236*	*2,792,574*	*5,610,270*	*10,942,984*	*7,294,895*	*9,023,196*
Cheque (new approach)	na	na	na	401,611,189	465,021,167	395,416,196	363,929,512	270,317,625
Cheque (former approach)	296,072,847	450,108,464	539,215,175	538,059,139	625,703,442	556,796,815	588,194,101	457,332,103
Credit transfer	78,286,492	97,327,128	161,642,174	266,969,099	287,264,068	313,163,442	312,487,450	350,992,884
of which instant transfers (SCT Inst)	*na*	*29,800*	*2,203,240*	*10,562,419*	*22,406,942*	*52,768,218*	*69,003,730*	*105,718,759*
Direct debit	8,726,403	58,346,253	10,990,025	1,891,051	25,318,677	19,853,012	22,320,813	30,365,272
Commercial paper	153,100	226,217	74,686	538,918	12,079	12,079	1,296,652	18,037,208
Electronic money	na	na	na	na	137,340	77,349	176,276	95,876
Money remittance	na	na	na	na	246,362	77,162	55,333	17,796
Total cashless payment fraud	**728,200,926**	**1,007,613,048**	**1,140,171,991**	**1,246,947,522**	**1,199,409,978**	**1,149,185,062**	**1,155,470,930**	**1,147,889,620**
Withdrawal by card	42,038,924	37,630,659	41,651,788	33,950,879	42,950,169	43,148,054	40,608,913	40,763,581
Total fraudulent transactions	**770,239,850**	**1,045,243,707**	**1,181,823,779**	**1,280,898,401**	**1,242,360,147**	**1,192,333,116**	**1,196,079,843**	**1,188,653,201**

na, not available.

Source: Observatory for the Security of Payment Means

Note: Since 2021, total cashless payment fraud has incorporated a new approach to cheque fraud, which excludes fraud that is prevented after the cheque has been presented to be cashed, and includes fraud on electronic money and money remittances.

CARDS: ISSUANCE

T5 Payments by cards issued in France

(volume in thousands, value in EUR thousands)

	2019		2020		2021	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**12,171,755**	**459,066,750**	**11,193,795**	**424,105,649**	**12,935,438**	**475,079,750**
of which contactless payments (incl. mobile payments)	*3,778,756*	*42,903,452*	*5,159,657*	*79,664,370*	*7,368,699*	*125,082,420*
of which mobile payments	*47,885*	*850,983*	*129,105*	*2,734,667*	*357,355*	*7,596,769*
Remote payments (excl. internet)	**77,150**	**4,838,911**	**134,114**	**7,567,877**	**76,931**	**7,995,010**
Internet payments	**2,236,049**	**135,352,563**	**2,524,317**	**146,563,476**	**3,116,285**	**177,056,237**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*787,664*	*85,221,641*
of which 3-D Secure payments without strong authentication	*na*	*na*	*na*	*na*	*444,723*	*19,267,910*
of which payments excl. 3-D Secure without strong authentication	*na*	*na*	*na*	*na*	*1,883,898*	*72,566,685*
Withdrawals	**1,391,930**	**136,507,651**	**1,064,095**	**115,958,207**	**1,086,289**	**123,867,648**
Total	**15,876,884**	**735,765,875**	**14,916,322**	**694,195,208**	**17,214,942**	**783,998,644**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

T5 Payments by cards issued in France (continued)

(volume in thousands, value in EUR thousands)

	2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**14,868,338**	**537,503,850**	**15,903,747**	**570,896,450**	**16,742,186**	**586,501,562**
of which contactless payments (incl. mobile payments)	*9,102,931*	*148,006,593*	*10,792,452*	*174,706,103*	*11,453,514*	*203,943,905*
of which mobile payments	*845,223*	*17,937,091*	*1,609,423*	*35,539,253*	*2,472,705*	*56,018,195*
Remote payments (excl. internet)	**105,781**	**16,994,865**	**96,368**	**15,880,261**	**95,683**	**14,871,495**
Internet payments	**3,283,604**	**191,418,128**	**3,685,180**	**219,662,525**	**4,144,523**	**242,158,676**
of which 3-D Secure payments with strong authentication	*1,034,950*	*112,713,734*	*1,282,644*	*136,151,668*	*1,153,075*	*139,292,722*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*135,611*	*4,119,307*	*382,740*	*14,661,163*
of which 3-D Secure payments without strong authentication	*781,313*	*27,091,534*	*800,728*	*27,212,160*	*896,289*	*31,855,769*
of which payments excl. 3-D Secure without strong authentication	*1,467,342*	*51,612,860*	*1,466,199*	*52,179,389*	*1,712,419*	*56,349,021*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*877,839*	*30,771,262*	*1,032,022*	*33,940,666*
of which "one-leg" payments	*na*	*na*	*31,151*	*1,997,096*	*43,267*	*2,235,967*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*250,843*	*9,039,674*	*254,557*	*8,025,476*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*30,366*	*10,371,359*	*382,573*	*12,146,912*
Withdrawals	**1,135,675**	**132,879,066**	**1,127,043**	**135,511,148**	**1,079,441**	**133,312,840**
Total	**19,393,398**	**878,795,909**	**20,812,338**	**941,950,384**	**22,061,834**	**976,844,573**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T5 *bis* Number of cards and instruments

T6 Fraudulent transactions using cards issued in France

(volume in units, value in euro, rate in %)

	2019			2020			2021		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,203,233**	**64,992,145**	**0.014**	**972,228**	**47,994,762**	**0.011**	**942,376**	**52,426,587**	**0.011**
of which contactless payments (incl. mobile payments)	*603,509*	*8,479,354*	*0.020*	*537,061*	*11,292,261*	*0.014*	*604,278*	*16,274,668*	*0.013*
of which mobile payments	*3,494*	*216,236*	*0.025*	*33,761*	*2,792,574*	*0.102*	*83,266*	*5,610,270*	*0.074*
Remote payments (excl. internet)	**409,319**	**31,806,788**	**0.657**	**411,344**	**26,899,103**	**0.355**	**124,596**	**22,193,382**	**0.278**
Internet payments	**5,458,543**	**331,450,998**	**0.245**	**6,037,565**	**364,595,450**	**0.249**	**5,697,780**	**346,790,316**	**0.196**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*496,017*	*103,029,680*	*0.121*
of which 3-D Secure payments without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*364,223*	*26,046,078*	*0.135*
of which payments excl. 3-D Secure without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*4,837,540*	*217,714,555*	*0.300*
Withdrawals	**165,505**	**41,651,788**	**0.031**	**113,067**	**33,950,879**	**0.029**	**129,083**	**42,950,169**	**0.035**
Total	**7,236,600**	**469,901,719**	**0.064**	**7,534,204**	**473,440,194**	**0.068**	**6,893,835**	**464,360,454**	**0.059**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T6 Fraudulent transactions using cards issued in France (continued)

(volume in units, value in euro, rate in %)

	2022			2023			2024		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,055,575**	**62,861,464**	**0,012**	**966,134**	**61,618,923**	**0.011**	**943,105**	**62,951,625**	**0.011**
of which contactless payments (incl. mobile payments)	*796,027*	*23,047,180*	*0,016*	*733,359*	*18,786,086*	*0.011*	*746,923*	*22,648,147*	*0.011*
of which mobile payments	*162,869*	*10,942,984*	*0,061*	*110,133*	*7,294,895*	*0,021*	*129,052*	*9,023,196*	*0.016*
Remote payments (excl. internet)	**174,364**	**42,028,102**	**0,247**	**186,499**	**42,177,372**	**0.266**	**183,666**	**40,377,262**	**0.272**
Internet payments	**5,463,049**	**315,696,257**	**0,165**	**5,483,322**	**351,408,599**	**0.160**	**6,186,464**	**374,734,072**	**0.155**
of which 3-D Secure payments with strong authentication	*624,473*	*124,258,815*	*0,110*	*722,396*	*132,754,198*	*0.098*	*676,055*	*128,822,135*	*0.092*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*159,680*	*8,966,661*	*0.218*	*189,142*	*11,192,865*	*0.076*
of which 3-D Secure payments without strong authentication	*625,296*	*25,695,176*	*0,095*	*593,808*	*22,929,848*	*0.084*	*449,128*	*17,294,653*	*0.054*
of which payments excl. 3-D Secure without strong authentication	*4,213,280*	*165,742,266*	*0,321*	*4,007,438*	*186,757,892*	*0.358*	*4,872,139*	*217,424,419*	*0.386*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*na*	*1,995,881*	*87,685,148*	*0.285*	*2,487,438*	*106,598,193*	*0.314*
of which "one-leg" payments	*na*	*na*	*na*	*416,116*	*30,632,806*	*1.534*	*651,446*	*43,751,776*	*1.957*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*553,018*	*16,515,229*	*0.183*	*516,679*	*13,485,307*	*0.168*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*1,042,423*	*51,924,709*	*0.501*	*1,216,576*	*53,589,143*	*0.441*
Withdrawals	**123,574**	**43,148,054**	**0,032**	**110,221**	**40,608,913**	**0.030**	**108,013**	**40,763,581**	**0.031**
Total	**6,816,562**	**463,733,877**	**0,053**	**6,746,176**	**495,813,807**	**0.053**	**7,421,248**	**518,826,540**	**0.053**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T7 Types of fraud involving payments by cards issued in France in 2024

(volume in units, value in euro, share in %)

	Lost or stolen cards				Intercepted cards				Altered or counterfeit cards			
	Volume		Value		Volume		Value		Volume		Value	
	Number	Share	Amount	Share	Number	Share	Amount	Share	Number	Share	Amount	Share
Face-to-face payments and UPT	**641,803**	**68.1**	**37,605,552**	**59.7**	**9,883**	**1.0**	**1,434,341**	**2.3**	**112,006**	**11.9**	**8,507,879**	**13.5**
of which contactless payments (incl. mobile payments)	*532,917*	*71.3*	*13,271,574*	*58.6*	*3,916*	*0.5*	*83,663*	*0.4*	*86,689*	*11.6*	*4,810,958*	*21.2*
of which mobile payments	*53,737*	*41.6*	*3,769,237*	*41.8*	*287*	*0.2*	*16,688*	*0.2*	*40,215*	*31.2*	*3,308,416*	*36.7*
Remote payments (excl. internet)	**17,076**	**9.3**	**3,683,722**	**9.1**	**76**	**0.0**	**8,922**	**0.0**	**618**	**0.3**	**174,492**	**0.4**
Internet payments	**348,324**	**5.6**	**26,141,227**	**7.0**	**4,636**	**0.1**	**294,559**	**0.1**	**128,069**	**2.1**	**7,198,422**	**1.9**
of which 3-D Secure payments with strong authentication	*38,007*	*5.6*	*8,308,430*	*6.4*	*649*	*0.1*	*137,504*	*0.1*	*1,039*	*0.2*	*225,670*	*0.2*
of which payments excl. 3-D Secure with strong authentication	*4,861*	*2.6*	*305,371*	*2.7*	*348*	*0.2*	*17,116*	*0.2*	*97*	*0.1*	*7,978*	*0.1*
of which 3-D Secure payments without strong authentication	*51,585*	*11.5*	*2,322,316*	*13.4*	*207*	*0.0*	*5,777*	*0.0*	*1,184*	*0.3*	*76,021*	*0.4*
of which payments excl. 3-D Secure without strong authentication	*253,871*	*5.2*	*15,205,110*	*7.0*	*3,432*	*0.1*	*134,162*	*0.1*	*125,749*	*2.6*	*6,888,753*	*3.2*
of which Merchant Initiated Transactions (MIT)	*192,607*	*7.7*	*10,054,028*	*9.4*	*1,987*	*0.1*	*73,622*	*0.1*	*73,907*	*3.0*	*3,377,006*	*3.2*
of which "one-leg" payments	*11,543*	*1.8*	*1,610,838*	*3.7*	*546*	*0.1*	*27,479*	*0.1*	*13,061*	*2.0*	*1,526,388*	*3.5*
of which PSD 2 compliant non-3-D Secure payments	*18,374*	*3.6*	*862,303*	*6.4*	*385*	*0.1*	*8,938*	*0.1*	*1,516*	*0.3*	*48,375*	*0.4*
of which non-PSD 2 compliant non-3-D Secure payments	*31,347*	*2.6*	*2,677,941*	*5.0*	*514*	*0.0*	*24,123*	*0.0*	*37,265*	*3.1*	*1,936,984*	*3.6*
Withdrawals	**79,034**	**73.2**	**31,584,937**	**77.5**	**3,654**	**3.4**	**1,120,781**	**2.7**	**7,808**	**7.2**	**2,053,621**	**5.0**
Total	**1,086,237**	**14.6**	**99,015,438**	**19.1**	**18,249**	**0.2**	**2,858,603**	**0.6**	**248,501**	**3.3**	**17,934,414**	**3.5**

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T7 Types of fraud involving payments by cards issued in France in 2024 (continued)

(volume in units, value in euro, share in %)

	Misappropriated card numbers				Other				All sources	
	Volume		Value		Volume		Value		Volume	Value
	Number	Share	Amount	Share	Number	Share	Amount	Share		
Face-to-face payments and UPT	**33,140**	**3.5**	**4,556,656**	**7.2**	**146,273**	**15.5**	**10,847,197**	**17.2**	**943,105**	**62,951,625**
of which contactless payments (incl. mobile payments)	*20,018*	*2.7*	*1,447,959*	*6.4*	*103,383*	*13.8*	*3,033,993*	*13.4*	*746,923*	*22,648,147*
of which mobile payments	*8,962*	*6.9*	*534,246*	*5.9*	*25,851*	*20.0*	*1,394,609*	*15.5*	*129,052*	*9,023,196*
Remote payments (excl. internet)	**165,163**	**89.9**	**36,458,568**	**90.3**	**733**	**0.4**	**51,558**	**0.1**	**183,666**	**40,377,262**
Internet payments	**5,665,079**	**91.6**	**337,167,693**	**90.0**	**40,356**	**0.7**	**3,932,171**	**1.0**	**6,186,464**	**374,734,072**
of which 3-D Secure payments with strong authentication	*633,888*	*93.8*	*118,930,572*	*92.3*	*2,472*	*0.4*	*1,219,959*	*0.9*	*676,055*	*128,822,135*
of which payments excl. 3-D Secure with strong authentication	*181,129*	*95.8*	*10,653,401*	*95.2*	*2,707*	*1.4*	*208,999*	*1.9*	*189,142*	*11,192,865*
of which 3-D Secure payments without strong authentication	*392,920*	*87.5*	*14,671,798*	*84.8*	*3,232*	*0.7*	*218,741*	*1.3*	*449,128*	*17,294,653*
of which payments excl. 3-D Secure without strong authentication	*4,457,142*	*91.5*	*192,911,922*	*88.7*	*31,945*	*0.7*	*2,284,472*	*1.1*	*4,872,139*	*217,424,419*
of which Merchant Initiated Transactions (MIT)	*2,208,720*	*88.8*	*92,770,543*	*87.0*	*10,217*	*0.4*	*322,994*	*0.3*	*2,487,438*	*106,598,193*
of which "one-leg" payments	*613,780*	*94.2*	*39,489,357*	*90.3*	*12,516*	*1.9*	*1,097,714*	*2.5*	*651,446*	*43,751,776*
of which PSD 2 compliant non-3-D Secure payments	*492,159*	*95.3*	*12,374,463*	*91.8*	*4,245*	*0.8*	*191,228*	*1.4*	*516,679*	*13,485,307*
of which non-PSD 2 compliant non-3-D Secure payments	*1,142,483*	*93.9*	*48,277,559*	*90.1*	*4,967*	*0.4*	*672,536*	*1.3*	*1,216,576*	*53,589,143*
Withdrawals	**902**	**0.8**	**159,379**	**0.4**	**16,615**	**15.4**	**5,844,863**	**14.3**	**108,013**	**40,763,581**
Total	**5,864,284**	**79.0**	**378,342,296**	**72.9**	**203,977**	**2.7**	**20,675,789**	**4.0**	**7,421,248**	**518,826,540**

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T8 Geographical breakdown of fraud involving cards issued in France in 2024

(volume in units, value in euro, share in %)

	Domestic transactions				European transactions			
	Volume		Value		Volume		Value	
	Number	Share	Amount	Share	Number	Share	Amount	Share
Face-to-face payments and UPT	**844,956**	**89.6**	**48,773,873**	**77.5**	**40,880**	**4.3**	**3,726,751**	**5.9**
of which contactless payments (incl. mobile payments)	*677,978*	*90.8*	*16,717,451*	*73.8*	*31,516*	*4.2*	*2,163,143*	*9.6*
of which mobile payments	*106,442*	*82.5*	*6,777,574*	*75.1*	*3,823*	*3.0*	*483,730*	*5.4*
Remote payments (excl. internet)	**108,914**	**59.3**	**21,901,906**	**54.2**	**30,640**	**16.7**	**8,292,438**	**20.5**
Internet payments	**1,698,767**	**27.5**	**140,961,462**	**37.6**	**2,843,968**	**46.0**	**140,451,519**	**37.5**
of which 3-D Secure payments with strong authentication	*243,803*	*36.1*	*64,612,099*	*50.2*	*333,371*	*49.3*	*51,411,372*	*39.9*
of which payments excl. 3-D Secure with strong authentication	*29,664*	*15.7*	*2,723,581*	*24.3*	*133,819*	*70.8*	*6,709,739*	*59.9*
of which 3-D Secure payments without strong authentication	*269,807*	*60.1*	*11,345,394*	*65.6*	*134,624*	*30.0*	*4,434,507*	*25.6*
of which payments excl. 3-D Secure without strong authentication	*1,155,493*	*23.7*	*62,280,388*	*28.6*	*2,242,154*	*46.0*	*77,895,901*	*35.8*
of which Merchant Initiated Transactions (MIT)	*911,249*	*36.6*	*46,970,926*	*44.1*	*1,028,521*	*41.3*	*39,736,426*	*37.3*
of which "one-leg" payments	*0*	*0.0*	*0*	*0.0*	*0*	*0.0*	*0*	*0.0*
of which PSD 2 compliant non-3-D Secure payments	*82,250*	*15.9*	*3,895,661*	*28.9*	*431,126*	*83.4*	*9,281,176*	*68.8*
of which non-PSD 2 compliant non-3-D Secure payments	*161,994*	*13.3*	*11,413,801*	*21.3*	*782,507*	*64.3*	*28,878,299*	*53.9*
Withdrawals	**97,042**	**89.8**	**38,795,063**	**95.2**	**2,824**	**2.6**	**808,281**	**2.0**
Total	**2,749,679**	**37.1**	**250,432,304**	**48.3**	**2,918,312**	**39.3**	**153,278,989**	**29.5**

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T8 Geographical breakdown of fraud involving cards issued in France in 2024 (continued)

(volume in units, value in euro, share in %)

	International transactions				Total	
	Volume		Value		Volume	Value
	Number	Share	Amount	Share		
Face-to-face payments and UPT	**57,269**	**6.1**	**10,451,001**	**16.6**	**943,105**	**62,951,625**
of which contactless payments (incl. mobile payments)	*37,429*	*5.0*	*3,767,553*	*16.6*	*746,923*	*22,648,147*
of which mobile payments	*18,787*	*14.6*	*1,761,892*	*19.5*	*129,052*	*9,023,196*
Paiements à distance (hors internet)	**44,112**	**24.0**	**10,182,918**	**25.2**	**183,666**	**40,377,262**
Internet payments	**1,643,729**	**26.6**	**93,321,091**	**24.9**	**6,186,464**	**374,734,072**
of which 3-D Secure payments with strong authentication	*98,881*	*14.6*	*12,798,664*	*9.9*	*676,055*	*128,822,135*
of which payments excl. 3-D Secure with strong authentication	*25,659*	*13.6*	*1,759,545*	*15.7*	*189,142*	*11,192,865*
of which 3-D Secure payments without strong authentication	*44,697*	*10.0*	*1,514,752*	*8.8*	*449,128*	*17,294,653*
of which payments excl. 3-D Secure without strong authentication	*1,474,492*	*30.3*	*77,248,130*	*35.5*	*4,872,139*	*217,424,419*
of which Merchant Initiated Transactions (MIT)	*547,668*	*22.0*	*19,890,841*	*18.7*	*2,487,438*	*106,598,193*
of which "one-leg" payments	*651,446*	*100.0*	*43,751,776*	*100.0*	*651,446*	*43,751,776*
of which PSD 2 compliant non-3-D Secure payments	*3,303*	*0.6*	*308,470*	*2.3*	*516,679*	*13,485,307*
of which non-PSD 2 compliant non-3-D Secure payments	*272,075*	*22.4*	*13,297,043*	*24.8*	*1,216,576*	*53,589,143*
Withdrawals	**8,147**	**7.5**	**1,160,237**	**2.8**	**108,013**	**40,763,581**
Total	**1,753,257**	**23.6**	**115,115,247**	**22.2**	**7,421,248**	**518,826,540**

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the acquirer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

(volume in thousands, value in EUR thousands)

	2019		2020		2021	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**11,774,183**	**437,193,670**	**10,978,602**	**413,760,411**	**12,611,966**	**460,274,895**
of which contactless payments (incl. mobile payments)	*3,690,364*	*41,558,002*	*5,081,519*	*78,386,853*	*7,202,992*	*121,694,861*
of which mobile payments	*45,249*	*794,288*	*126,945*	*2,687,300*	*348,251*	*7,390,633*
Remote payments (excl. internet)	**34,859**	**2,773,069**	**60,243**	**5,428,918**	**56,236**	**5,540,339**
Internet payments	**1,768,890**	**109,593,147**	**2,011,431**	**122,128,921**	**2,399,865**	**142,184,895**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*661,960*	*72,184,112*
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*389,530*	*15,797,723*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*1 348,375*	*54,203,060*
Withdrawals	**1,339,625**	**130,198,441**	**1,038,647**	**112,337,533**	**1,056,936**	**119,485,544**
Total	**14,917,558**	**679,758,326**	**14,088,924**	**653,655,783**	**16,125,003**	**727,485,673**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

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

(volume in thousands, value in EUR thousands)

	2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**14,340,211**	**514,159,801**	**15,252,122**	**543,567,354**	**16,006,233**	**556,741,575**
of which contactless payments (incl. mobile payments)	*8,781,813*	*141,160,469*	*10,357,439*	*164,920,568*	*10,909,977*	*190 761 361*
of which mobile payments	*808,622*	*17,132,553*	*1,533,084*	*33,773,794*	*2,350,573*	*53,025,223*
Remote payments (excl. internet)	**87,602**	**13,259,829**	**82,700**	**12,227,259**	**81,806**	**11,294,926**
Internet payments	**2,393,161**	**146,642,890**	**2,580,907**	**164,682,672**	**2,817,916**	**179,442,255**
of which 3-D Secure payments with strong authentication	*809,038*	*88,956,221*	*977,983*	*105,884,327*	*914,093*	*109,906,448*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*57,239*	*1,938,429*	*164,512*	*6,793,036*
of which 3-D Secure payments without strong authentication	*717,916*	*24,981,800*	*661,070*	*22,814,974*	*772,768*	*27,751,133*
of which payments excl. 3-D Secure without strong authentication	*866,207*	*32,704,868*	*884,617*	*34,044,942*	*966,543*	*34,991,639*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*704,832*	*25,137,618*	*759,880*	*26,194,801*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*92,513*	*4,489,918*	*99,379*	*3,924,928*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*87,272*	*4,417,407*	*107,284*	*4,871,909*
Withdrawals	**1,101,989**	**128,161,781**	**1,085,417**	**129,282,806**	**1,038,313**	**126,861,199**
Total	**17,922,963**	**802,224,301**	**19,001,146**	**849,760,091**	**19 944 269**	**874 339 955**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T9 *bis* Payments by cards issued and accepted in the European Economic Area – European transactions

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

T10 Fraudulent transactions using cards issued and accepted in France – Domestic transactions

(volume in units, value in euro, rate in %)

	2019			2020			2021		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,069,418**	**44,175,058**	**0.010**	**793,350**	**36,280,495**	**0.009**	**825,325**	**43,515,617**	**0.009**
of which contactless payments (incl. mobile payments)	*582,050*	*7,912,021*	*0.019*	*522,873*	*10,502,092*	*0.013*	*576,537*	*14,002,613*	*0.012*
of which mobile payments	*3,215*	*197,048*	*0.025*	*29,807*	*2,447,707*	*0.091*	*75,039*	*4,801,997*	*0.065*
Remote payments (excl. internet)	**64,113**	**7,498,207**	**0.270**	**74,832**	**8,964,315**	**0.165**	**77,941**	**10,604,251**	**0.191**
Internet payments	**2,630,697**	**183,067,879**	**0.167**	**2,847,769**	**212,962,645**	**0.174**	**2,577,337**	**191,873,234**	**0.135**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*267,556*	*69,544,332*	*0.096*
of which 3-D Secure payments without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*159,344*	*11,208,886*	*0.071*
of which payments excl. 3-D Secure without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*2,150,437*	*111,120,015*	*0.205*
Withdrawals	**122,260**	**35,935,625**	**0.028**	**102,962**	**32,477,429**	**0.029**	**121,642**	**41,437,842**	**0.035**
Total	**3,886,488**	**270,676,769**	**0.040**	**3,818,913**	**290,684,884**	**0.044**	**3,602,245**	**287,430,944**	**0.040**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

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

(volume in units, value in euro, rate in %)

	2022			2023			2024		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**989,454**	**53,593,598**	**0.010**	**885,533**	**50,277,021**	**0.009**	**844,956**	**48,773,873**	**0.009**
of which contactless payments (incl. mobile payments)	*754,985*	*20,231,615*	*0.014*	*684,776*	*15,698,156*	*0.010*	*677,978*	*16,717,451*	*0.009*
of which mobile payments	*152,726*	*9,566,583*	*0.056*	*98,610*	*6,066,551*	*0.018*	*106,442*	*6,777,574*	*0.013*
Remote payments (excl. internet)	**120,708**	**24,857,056**	**0.187**	**118,903**	**22,602,626**	**0.185**	**108,914**	**21,901,906**	**0.194**
Internet payments	**1,874,565**	**145,299,292**	**0.099**	**1,913,224**	**152,815,486**	**0.093**	**1,698,767**	**140,961,462**	**0.079**
of which 3-D Secure payments with strong authentication	*314,967*	*72,922,674*	*0.082*	*314,857*	*72,017,359*	*0.068*	*243,803*	*64,612,099*	*0.059*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*36,576*	*2,353,042*	*0.121*	*29,664*	*2,723,581*	*0.040*
of which 3-D Secure payments without strong authentication	*342,714*	*17,460,124*	*0.070*	*258,701*	*12,634,204*	*0.055*	*269,807*	*11,345,394*	*0.041*
of which payments excl. 3-D Secure without strong authentication	*1,216,884*	*54,916,494*	*0.168*	*1,303,090*	*65,810,881*	*0.193*	*1,155,493*	*62,280,388*	*0.178*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*na*	*1,044,582*	*49,260,633*	*0.196*	*911,249*	*46,970,926*	*0.179*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*70,590*	*4,496,448*	*0.100*	*82,250*	*3,895,661*	*0.099*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*187,918*	*12,053,800*	*0.273*	*161,994*	*11,413,801*	*0.234*
Withdrawals	**115,643**	**41,344,934**	**0.032**	**102,357**	**38,832,083**	**0.030**	**97,042**	**38,795,063**	**0.031**
Total	**3,100,370**	**265,094,880**	**0.033**	**3,020,017**	**264,527,216**	**0.031**	**2,749,679**	**250,432,304**	**0.029**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

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

T11 Breakdown of remote fraud by sector of activity involving domestic transactions in 2024

(volume in units, value in euro, volume fraud rate per thousand, value fraud rate in %)

	Transactions		Fraud		Fraud rate	
	Volume	Value	Volume	Value	Volume (%)	Value (%)
Generalist and semi-generalist trade	839,775,334	47,851,435,622	331,775	25,646,539	0.395	0.054
Technical and cultural products	167,243,767	7,480,671,089	301,261	14,058,213	1.801	0.188
Travel and transportation	326,985,440	30,154,845,761	163,659	21,327,646	0.501	0.071
Telephony and communication	409,511,562	15,409,913,699	262,287	19,961,503	0.640	0.130
Food	34,103,581	2,614,453,637	10,090	1,060,996	0.296	0.041
Household goods, furnishings and DIY	117,021,604	13,443,874,493	40,974	12,257,418	0.350	0.091
Insurers	14,109,505	2,838,800,127	5,752	818,359	0.408	0.029
Health, beauty and personal care	53,374,504	3,373,912,500	24,330	2,323,234	0.456	0.069
Personal and professional services	491,092,639	39,221,545,908	499,264	41,107,865	1.017	0.105
Account loading and person-to-person sales	122,727,707	12,116,829,244	74,282	15,918,915	0.605	0.131
Online gaming	159,189,679	4,864,731,237	66,173	4,375,325	0.416	0.090
Miscellaneous	164,587,463	11,366,167,820	27,834	4,007,355	0.169	0.035
Total	**2,899,722,785**	**190,737,181,137**	**1,807,681**	**162,863,368**	**0.623**	**0.085**

Source: Observatory for the Security of Payment Means.

T12 Payments by cards accepted in France

(volume in thousands, value in EUR thousands)

	2019		2020		2021	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**12,277,149**	**468,895,511**	**11,284,433**	**428,180,387**	**13,031,098**	**480,804,099**
of which contactless payments (incl. mobile payments)	*3,802,953*	*42,931,374*	*5,187,488*	*79,877,184*	*7,437,197*	*125,344,168*
of which mobile payments	*56,169*	*1,014,657*	*145,527*	*2,979,437*	*388,175*	*8,403,747*
Remote payments (excl. internet)	**48,998**	**5,586,755**	**69,950**	**7,087,913**	**64,620**	**7,272,724**
Internet payments	**1,906,065**	**121,920,272**	**2,158,226**	**132,554,575**	**2,565,276**	**155,816,405**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*708,194*	*78,650,830*
of which 3-D Secure payments without strong authentication	*na*	*na*	*na*	*na*	*409,008*	*18,152,505*
of which payments excl. 3-D Secure without strong authentication	*na*	*na*	*na*	*na*	*1,448,074*	*59,013,071*
Withdrawals	**1,375,145**	**136,636,741**	**1,062,376**	**116,986,747**	**1,083,643**	**125,105,264**
Total	**15,607,358**	**733,039,279**	**14,574,985**	**684,809,622**	**16,744,636**	**768,998,491**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

T12 Payments by cards accepted in France (continued)

(volume in thousands, value in EUR thousands)

	2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**15,093,611**	**551,753,133**	**16,159,605**	**588,228,633**	**17,012,813**	**604,699,649**
of which contactless payments (incl. mobile payments)	*9,248,429*	*149,971,446*	*10,982,717*	*178,132,864*	*11,665,395*	*208,538,219*
of which mobile payments	*897,307*	*19,846,999*	*1,716,563*	*39,282,385*	*2,640,235*	*61,840,034*
Remote payments (excl. internet)	**107,228**	**18,523,094**	**105,756**	**18,799,343**	**106,081**	**18,394,978**
Internet payments	**2,589,260**	**166,197,062**	**2,821,038**	**190,607,365**	**3,093,897**	**209,248,154**
of which 3-D Secure payments with strong authentication	*871,961*	*99,937,461*	*1,049,797*	*120,158,448*	*983,884*	*125,202,674*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*86,343*	*3,228,632*	*207,164*	*8,955,485*
of which 3-D Secure payments without strong authentication	*748,083*	*27,403,752*	*707,064*	*26,605,058*	*824,916*	*32,032,178*
of which payments excl. 3-D Secure without strong authentication	*969,216*	*38,855,848*	*977,834*	*40,615,228*	*1,077,933*	*43,057,816*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*730,327*	*26,600,426*	*799,769*	*28,458,565*
of which "one-leg" payments	*na*	*na*	*13,616*	*1,740,365*	*18,288*	*2,203,462*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*101,735*	*5,110,587*	*108,621*	*4,746,678*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*132,156*	*7,163,850*	*151,255*	*7,649,111*
Withdrawals	**1,134,543**	**134,637,455**	**1,117,986**	**135,559,666**	**1,069,029**	**133,303,352**
Total	**18,924,643**	**871,110,743**	**20,204,386**	**933,195,008**	**21,281,820**	**965,646,133**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the card issuer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T12 *bis* Payments by cards issued in the European Economic Area and accepted in France – European transactions

T12 *ter* Payments by cards issued abroad outside the European Economic Area and accepted in France – International transactions

T13 Fraudulent transactions using cards accepted in France

(volume in units, value in euro, rate in %)

	2019			2020			2021		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,170,399**	**64,448,538**	**0.0137**	**841,280**	**42,883,367**	**0.0100**	**874,166**	**49,441,754**	**0.0103**
of which contactless payments (incl. mobile payments)	*602,309*	*8,534,090*	*0.0199*	*538,313*	*12,238,895*	*0.0153*	*601,803*	*15,600,613*	*0.0124*
of which mobile payments	*3,890*	*307,230*	*0.0303*	*35,968*	*3,640,684*	*0.1222*	*84,421*	*5,793,427*	*0.0689*
Remote payments (excl. internet)	**108,259**	**23,167,505**	**0.4147**	**105,972**	**17,644,315**	**0.2489**	**96,257**	**15,211,163**	**0.2092**
Internet payments	**2,989,333**	**232,763,441**	**0.1909**	**3,176,400**	**248,966,265**	**0.1878**	**2,885,920**	**227,162,875**	**0.1458**
of which 3-D Secure payments with strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*306,265*	*76,891,633*	*0.0978*
of which 3-D Secure payments without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*213,403*	*20,406,481*	*0.1124*
of which payments excl. 3-D Secure without strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*2,366,252*	*129,864,761*	*0.2201*
Withdrawals	**127,005**	**37,354,814**	**0.0273**	**104,960**	**33,084,175**	**0.0283**	**124,077**	**42,256,276**	**0.0338**
Total	**4,394,996**	**357,734,298**	**0.0488**	**4,228,612**	**342,578,122**	**0.0500**	**3,980,420**	**334,072,068**	**0.0434**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

T13 Fraudulent transactions using cards accepted in France (continued)

(volume in units, value in euro, rate in %)

	2022			2023			2024		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,084,701**	**67,409,965**	**0.0122**	**999,344**	**67,688,751**	**0.0115**	**936,033**	**60,704,064**	**0.0100**
of which contactless payments (incl. mobile payments)	*819,535*	*24,406,015*	*0.0163*	*769,979*	*21,899,061*	*0.0123*	*750,184*	*21,346,502*	*0.0102*
of which mobile payments	*170,752*	*12,007,511*	*0.0605*	*127,622*	*10,042,616*	*0.0256*	*132,824*	*9,630,052*	*0.0156*
Remote payments (excl. internet)	**144,965**	**35,446,137**	**0.1914**	**142,763**	**32,984,939**	**0.1755**	**142,032**	**33,542,430**	**0.1823**
Internet payments	**2,252,283**	**190,461,573**	**0.1146**	**2,337,170**	**201,724,304**	**0.1058**	**2,244,306**	**203,744,409**	**0.0974**
of which 3-D Secure payments with strong authentication	346,366	80,959,973	0.0810	354,651	83,805,192	0.0697	267,924	73,737,188	0.0589
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*71,563*	*5,522,986*	*0.1711*	*44,498*	*4,443,794*	*0.0496*
of which 3-D Secure payments without strong authentication	*405,445*	*26,105,266*	*0.0953*	*342,878*	*20,687,862*	*0.0778*	*402,394*	*20,996,741*	*0.0655*
of which payments excl. 3-D Secure without strong authentication	*1,500,472*	*83,396,334*	*0.2146*	*1,568,078*	*91,708,264*	*0.2258*	*1,529,490*	*104,566,686*	*0.2429*
of which Merchant Initiated Transactions (MIT)	*na*	*na*	*na*	*1,098,829*	*52,343,346*	*0.1968*	*1,013,164*	*53,073,094*	*0.1865*
of which "one-leg" payments	*na*	*na*	*na*	*92,524*	*12,994,451*	*0.7467*	*134,338*	*20,595,974*	*0.9347*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*80,195*	*5,068,095*	*0.0992*	*92,684*	*4,512,752*	*0.0951*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*296,530*	*21,302,372*	*0.2974*	*289,304*	*26,384,866*	*0.3449*
Withdrawals	**120,217**	**42,811,637**	**0.0318**	**106,749**	**40,292,502**	**0.0297**	**100,323**	**40,070,346**	**0.0301**
Total	**3,602,166**	**336,129,312**	**0.0386**	**3,586,026**	**342,690,496**	**0.0367**	**3,422,694**	**338,061,249**	**0.0350**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, a payment where the card issuer is located outside the European Union; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

T13 *quater* Breakdown of fraud involving payments by cards accepted in France in 2024

T13 *quinquies* Geographical breakdown of fraud involving cards accepted in France in 2024

CHEQUES

T14 Cheques exchanged

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

	2019	2020	2021	2022	2023	2024
Volume	1,586.5	1,175.5	1,105.8	1,008.0	891.5	783.8
Value	814.5	614.2	588.6	539.8	467.3	392.2
Average value	**513.4**	**522.5**	**532.3**	**535.5**	**524.1**	**500.4**

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 euro, volume fraud rate per thousand, value fraud rate in %)

a) Former approach

	2019	2020	2021	2022	2023	2024
Volume	**183,488**	**220,685**	**272,970**	**266,216**	**255,857**	**215,576**
Fraud rate (per thousand)	0.116	0.188	0.247	0.264	0.287	0.275
Value	**539,215,175**	**538,059,139**	**625,703,442**	**556,796,815**	**588,194,101**	**457,332,103**
Fraud rate (%)	0.066	0.088	0.106	0.103	0.126	0.117
Average value	**2,939**	**2,438**	**2,292**	**2,092**	**2,299**	**2,121**

b) New approach

	2019	2020	2021	2022	2023	2024
Volume	**na**	**190,001**	**232,277**	**218,122**	**206,197**	**173,366**
Fraud rate (per thousand)		0.162	0.210	0.216	0.231	0.221
Value	**na**	**401,611,189**	**465,021,167**	**395,416,196**	**363,929,512**	**270,317,625**
Fraud rate (%)		0.065	0.079	0.073	0.078	0.069
Average value	**na**	**2,114**	**2,002**	**1,813**	**1,765**	**1,559**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: The former approach takes into account any cheque transaction settled and rejected for fraud. The new approach to measuring cheque fraud excludes fraud that is thwarted after the cheque has been presented to be cashed.

T16 Types of cheque fraud

(volume in units, value in euro, share in %)

	2019		2020		2021		2022		2023		2024	
	Number/ Value	Share	Number/ Value	Share	Number/ Value	Share	Number/ Value	Share	Number/ Value	Share	Number/ Value	Share
Volume												
Theft, loss	154,211	84.0	196,754	89.2	244,750	89.7	237,854	89.3	225,859	88.3	192,307	89.2
Forgery	16,459	9.0	13,894	6.3	18,074	6.6	18,885	7.1	20,583	8.0	14,260	6.6
Counterfeiting	9,574	5.2	7,207	3.3	5,119	1.9	5,969	2.2	5,720	2.2	6,249	2.9
Misappropriation, replay	3,244	1.8	2,830	1.3	5,026	1.8	3,508	1.3	3,695	1.4	2,760	1.3
Value												
Theft, loss	296,367,562	55.0	365,813,764	68.0	398,739,224	63.7	375,576,575	67.5	385,379,003	65.5	285,010,973	62.3
Forgery	145,881,745	27.1	102,801,337	19.1	100,395,756	16.0	93,152,894	16.7	103,932,879	17.7	89,327,982	19.5
Counterfeiting	76,511,582	14.2	32,340,420	6.0	33,725,041	5.4	32,648,566	5.9	29,927,137	5.1	44,088,111	9.6
Misappropriation, replay	20,454,286	3.8	37,103,618	6.9	92,823,421	14.8	55,418,781	10.0	68,955,081	11.7	38,905,037	8.5

Source: Observatory for the Security of Payment Means.

Note: Cheque fraud is broken down by type based on the former approach, which takes into account any cheque transaction settled and rejected for fraud.

CREDIT TRANSFERS

T17 Credit transfers issued by type

(volume in millions, value in EUR millions)

	2019		2020		2021		2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Total	**4,251**	**25,879,217**	**4,483**	**32,713,128**	**4,843**	**38,722,734**	**5,158**	**38,894,879**	**5,613**	**29,942,161**	**5,973**	**31,108,348**
of which SEPA Credit Transfers	*4,174*	*9,602,866*	*4,384*	*10,029,108*	*4,668*	*12,980,883*	*4,689*	*9,655,892*	*4,867*	*9,823,091*	*5,023*	*10,480,787*
of which SEPA Instant Transfers – SCT Inst	*14*	*7,074*	*45*	*26,243*	*107*	*50,053*	*198*	*118,972*	*408*	*177,099*	*598*	*231,252*
of which LVT[a]	*9*	*12,266,316*	*9*	*19,042,030*	*9*	*19,661,685*	*19*	*15,907,892*	*30*	*8,533,346*	*11*	*10,407,612*
of which other transfers	*54*	*4,002,960*	*45*	*3,615,748*	*59*	*6,030,114*	*252*	*13,212,124*	*309*	*11,408,625*	*341*	*9,988,697*
Total – excl. LVT	**4,242**	**13,612,900**	**4,474**	**13,671,098**	**4,834**	**19,061,050**	**5,138**	**22,986,988**	**5,583**	**21,408,815**	**5,962**	**20,700,736**

a) Large-value transfers issued via TARGET2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA, Single Euro Payment Area; SCT Inst, SEPA Instant Credit Transfer; LVT, large-value transfers.

T17 *bis* Credit transfers issued by initiation channel

T17 *ter* Credit transfers issued by geographical destination

T18 Fraudulent transactions by type of credit transfer

(volume in units, value in euro, rate in %)

	2019			2020			2021		
	Volume	Value		Volume	Value		Volume	Value	
		Amount	Fraud rate		Amount	Fraud rate		Amount	Fraud rate
Total	**15,934**	**161,642,174**	**0.0006**	**35,893**	**266,969,099**	**0,0008**	**46,718**	**287,264,068**	**0.0007**
of which SEPA Credit Transfers	*13,302*	*127,572,549*	*0.0013*	*25,254*	*191,474,396*	*0.0019*	*33,199*	*246,527,533*	*0.0019*
of which SEPA Instant Transfers – SCT Inst	*729*	*2,203,240*	*0.0311*	*7,131*	*10,562,419*	*0.0402*	*12,913*	*22,406,942*	*0.0448*
of which LVT[a]	*15*	*15,476,053*	*0.0001*	*51*	*2,439,224*	*0.0000*	*5*	*1,539,120*	*0.0000*
of which other transfers	*1,888*	*16,390,332*	*0.0004*	*3,457*	*62,493,060*	*0.0017*	*601*	*16,790,473*	*0.0003*
Total – excl. LVT	**15,919**	**146,166,121**	**0.0011**	**35,842**	**264,529,875**	**0.0019**	**46,713**	**285,724,948**	**0.0015**

a) Large-value transfers issued via TARGET2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA, Single Euro Payment Area; SCT Inst, SEPA Instant Credit Transfer; LVT, large-value transfers.

T18 Fraudulent transactions by type of credit transfer (continued)

(volume in units, value in euro, rate in %)

	2022			2023			2024		
	Volume	Value		Volume	Value		Volume	Value	
		Amount	Fraud rate		Amount	Fraud rate		Amount	Fraud rate
Total	**76,846**	**313,163,442**	**0.0008**	**90,453**	**312,487,450**	**0,0010**	**132,298**	**350,992,884**	**0.0011**
of which SEPA Credit Transfers	*40,874*	*205,737,587*	*0.0021*	*38,591*	*202,417,172*	*0.0021*	*41,693*	*199,872,166*	*0.0019*
of which SEPA Instant Transfers – SCT Inst	*33,193*	*52,768,218*	*0.0444*	*48,630*	*69,003,730*	*0.0390*	*80,394*	*105,718,759*	*0.0457*
of which LVT[a)]	*49*	*1,934,774*	*0.0000*	*32*	*9,828,077*	*0.0001*	*20*	*3,496,816*	*0.0000*
of which other transfers	*2,730*	*52,722,863*	*0.0004*	*3,200*	*31,238,471*	*0.0003*	*10,191*	*41,905,143*	*0.0004*
Total – excl. LVT	**76,797**	**311,228,668**	**0.0014**	**90,421**	**302,659,373**	**0.0014**	**132,278**	**347,496,068**	**0.0017**

a) Large-value transfers issued via TARGET2 or Euro1.

Source: Observatory for the Security of Payment Means.

Note: SEPA, Single Euro Payment Area; SCT Inst, SEPA Instant Credit Transfer; LVT, large-value transfers.

T18 *bis* Fraudulent transactions by transfer initiation channel

T18 *ter* Fraudulent transactions by geographical destination of credit transfers

T19 Total fraud on credit transfers

(volume in units, value and average value in euro, volume fraud rate per thousand, value fraud rate in %)

	2019	2020	2021	2022	2023	2024
Volume	**15,934**	**35,893**	**46,718**	**76,846**	**90,453**	**132,298**
Rate (per thousand)	0.0037	0.0080	0.0096	0.0149	0.0161	0.0222
Value	**161,642,174**	**266,969,099**	**287,264,068**	**313,163,442**	**312,487,450**	**350,992,884**
Rate (%)	0.0006	0.0008	0.0007	0.0008	0.0010	0.0011
Average value	**10,144**	**7,438**	**6,149**	**4,075**	**3 455**	**2 653**

Source: Observatory for the Security of Payment Means.

T20 Fraud on credit transfers by type

(volume in units, value in euro, share in %)

	2019		2020		2021		2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Deceit	**13,769**	**98,525,485**	**28,211**	**87,061,255**	**35,865**	**87,370,131**	**57,443**	**120,006,990**	**63,471**	**134,097,939**	**75,038**	**135,980,519**
Share	86.4	61.0	78.6	32.6	76.8	30.4	74.8	38.3	70.2	42.9	56.7	38.7
Forgery	**125**	**3,438,923**	**203**	**3,377,807**	**875**	**5,387,862**	**179**	**2,838,371**	**269**	**2,293,923**	**406**	**3,498,532**
Share	1.6	2.1	0.6	1.3	1.9	1.9	0.2	0.9	0.3	0.7	0.3	1.0
Misappropriation	**1,534**	**56,514,755**	**5,731**	**157,318,883**	**8,523**	**168,094,274**	**16,991**	**148,732,203**	**25,071**	**152,081,946**	**54,693**	**183,251,281**
Share	19.8	35.0	16.0	58.9	18.2	58.5	22.1	47.5	27.7	48.7	41.3	52.2
Other	**506**	**3,163,011**	**1,748**	**19,211,154**	**1,455**	**26,411,801**	**2,233**	**41,585,878**	**1,642**	**24,013,643**	**2,161**	**28,262,553**
Share	3.2	2.0	4.9	7.2	3.1	9.2	2.9	13.3	1.8	7.7	1.6	8.1

Source: Observatory for the Security of Payment Means.

DIRECT DEBITS

T21 Direct debits issued by type of mandate

(volume in millions, value in EUR millions)

	2019		2020		2021		2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Total	**4,370**	**1,710,931**	**4,622**	**1,684,258**	**5,020**	**1,895,098**	**4,914**	**2,040,963**	**4,616**	**2,138,539**	**4,788**	**2,178,198**
Breakdown of direct debits by type of mandate												
Direct debit by electronic mandate	na	na	na	na	1,106	430,781	1,357	1,045,754	1,254	1,021,429	1,228	1,026,955
Direct debit by paper-based mandate	na	na	na	na	3,914	1,464,317	3,558	995,210	3,362	1,117,110	3,560	1,151,243
Direct debits by initiation method												
Direct debit initiated in a file/batch	4,312	1,672,338	4,560	1,647,504	4,936	1,819,420	4,645	1,929,438	4,242	2,009,917	4,479	2,064,694
Direct debit initiated on the basis of a single payment	58	38,593	61	36,754	84	75,678	269	111,525	374	128,622	310	113,504

na, not available.

Source: Observatory for the Security of Payment Means.

T21 *bis* Direct debits issued by geographical origin of the payer

T22 Direct debit fraud

(volume in units, value and average value in euro, volume fraud rate per thousand, value fraud rate in %)

	2019	2020	2021	2022	2023	2024
Volume	**43,519**	**6,485**	**251,010**	**49,453**	**77,876**	**52,718**
Fraud rate (per thousand)	0.0100	0.0014	0.0500	0.0101	0.0169	0.0110
Value	**10,990,025**	**1,891,051**	**25,318,677**	**19,853,012**	**22,320,813**	**30,365,272**
Fraud rate (%)	0.0006	0.0001	0.0013	0.0010	0.0010	0.0014
Average value	**253**	**292**	**101**	**401**	**287**	**576**

Source: Observatory for the Security of Payment Means.

T22 *bis* Fraudulent direct debits by geographical origin of the payer

T22 *ter* Fraudulent direct debits by type of mandate

T23 Types of direct debit fraud

(volume in units, value in euro, share in %)

	2019		2020		2021		2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Deceit	**14,601**	**3,961,260**	**6,011**	**1,388,326**	**250,493**	**25,201,709**	**43,788**	**14,206,533**	**70,212**	**22,003,546**	**27,476**	**29,202,487**
Share	33.6	36.0	92.7	73.4	99.8	99.5	88.5	71.6	90.2	98.6	52.1	96.2
Misappropriation	**26,223**	**6,677,467**	**62**	**10,720**	**517**	**116,968**	**5,665**	**5,646,479**	**7,664**	**317,267**	**25,242**	**1,162,784**
Share	60.3	60.8	1.0	0.6	0.2	0.5	11.5	28.4	9.8	1.4	47.9	3.8

Source: Observatory for the Security of Payment Means.

Note: Until 2020, direct debit fraud included two other types "Falsifications" and "Other", which explains why the breakdown does not always total 100% of fraud.

OTHER

Electronic money

Commercial papers: trade bills and promissory notes

Money remittances

Payment initiation services

Published by
Banque de France

Managing Editor
Érick Lacourrège
Director General Cash and Retail Payments
Banque de France

Editor-in-Chief
Julien Lasalle
Deputy Director Cash and Retail Payments Policy and Oversight
Banque de France

Editorial Secretariat
Aurélie Barberet, Pierre Bienvenu, Clément Bourgeois,
Véronique Bugaj, Julien Cisamolo, Caroline Corcy,
Anne-Marie Fourel, Trân Huynh, Fatih Kurt,
Isabelle Maranghi, Adrien Mocek, Ségolène Mure,
Didier Névonnic, Cyril Ronfort,
Marine Soubielle, Valérie Tallarita

Translator
Scott Oldale

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
September 2025
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).

BANQUE DE FRANCE

EUROSYSTÈME

www.banque-france.fr