OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2025

BANQUE DE FRANCE
EUROSYSTÈME



www.observatoire-paiements.fr

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

© Observatory for the security of payment means – 2026

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2025

addressed to
The Minister of the Economy, Finance and Industrial,
Energy 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 2026

CONTENTS

SUMMARY 4

2025 IN NUMBERS 6

CHAPTER 1
FRAUD IN 2025 9

1.1 Overview 10

1.2 Current state of payment card fraud 13

1.3 Current state of cheque fraud 20

1.4 Current state of credit transfer fraud 21

1.5 Current state of direct debit fraud 22

1.6 Current state of commercial paper fraud 23

1.7 Current state of social engineering fraud 24

CHAPTER 2
WORK CARRIED OUT BY THE OBSERVATORY ON FRAUD PREVENTION 29

2.1 Action plan to combat social engineering fraud 29

2.2 Prevention of fraud on remote card payments 40

2.3 Monitoring of the Observatory's other actions and recommendations
This section 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-2025*

CHAPTER 3
SECURITY OF PAYMENTS USING CRYPTO-ASSETS 45

3.1 Introduction 45

3.2 A typology of payments using crypto-assets 46

3.3 The underlying technical functionality 49

3.4 The security challenges 51

3.5 Compliance challenges 54

APPENDICES 59

A1 Security recommendations for the use of payment means

A2 Responsibilities and organisation of the Observatory 60

A3 Members of the Observatory

A4 Methodology for measuring fraud involving cashless means of payment 62

A5 Statistical data on means of payment use and fraud

BOX 25

Indicators from the French Ministry of the Interior on means of payment fraud in 2025 25

SUMMARY

Growth in the use of cashless means of payment continued at a steady pace in 2025 *(up 5.5% in terms of annual transactions and 4.2% in total transaction value) and was driven by the use of the most innovative solutions. For example, payments by mobile now account for one in five point-of-sale card payments, and the annual value of instant credit transfers doubled between 2024 and 2025 to account for 17% of total transfers issued.*

Chapter 1 *of this Annual Report shows that annual fraud in value terms has risen but at a slower rate year-on-year (up 3.8%, to EUR 1.2 billion) with the number of fraudulent transactions falling significantly (down 8%, or 7.2 million transactions).*

- ***The slower rise in fraud can be attributed to the historically low fraud rates for card payments*** *(EUR 47 of fraud per EUR 100,000 of payments)* ***and for cheques*** *(EUR 69 per EUR 100,000). These two payment methods have benefited from the action plans that the Observatory has implemented in recent years to enhance their security.*

- *With growth in fraud moderating,* ***the methods used by fraudsters are evolving. Social engineering fraud****, such as fake bank adviser scams, CEO fraud and bank account switch scams,* ***is on the rise****. It is projected to have reached EUR 516 million in 2025, and therefore to account for just over 40% of total annual payment fraud by value. Its share has doubled in four years.*

Chapter 2 provides an overview of the actions undertaken and supported by the Observatory in terms of fraud prevention*, which mainly include:*

- ***Actions carried out in cooperation with the telecommunications and digital sectors to prevent social engineering fraud upstream.*** *These initiatives are designed to ensure stronger tools and better cross-sector coordination in the fight against identity theft across the different communication channels, including digital messaging and social media.*

- ***The development of mechanisms for sharing information between payment service providers, particularly the beneficiary verification service introduced in October 2025 and, since May 2026, the*** **Fichier national des comptes signalés pour risque de fraude** ***(the French national register of accounts flagged for fraud risk).*** *These mechanisms act as additional infrastructure for the sharing of information useful in detecting high-risk transfers, particularly in cases of social engineering fraud.*

- ***The deployment of an action plan to secure remote card payments made without the use of the 3-D Secure technical protocol.*** *The action plan combines collective measures focused on the most vulnerable channels and individual measures targeting the merchants that are most exposed to fraud. It has already helped to improve the fraud rate for card payments over the internet in 2024 and 2025 and will continue to do so in 2026.*

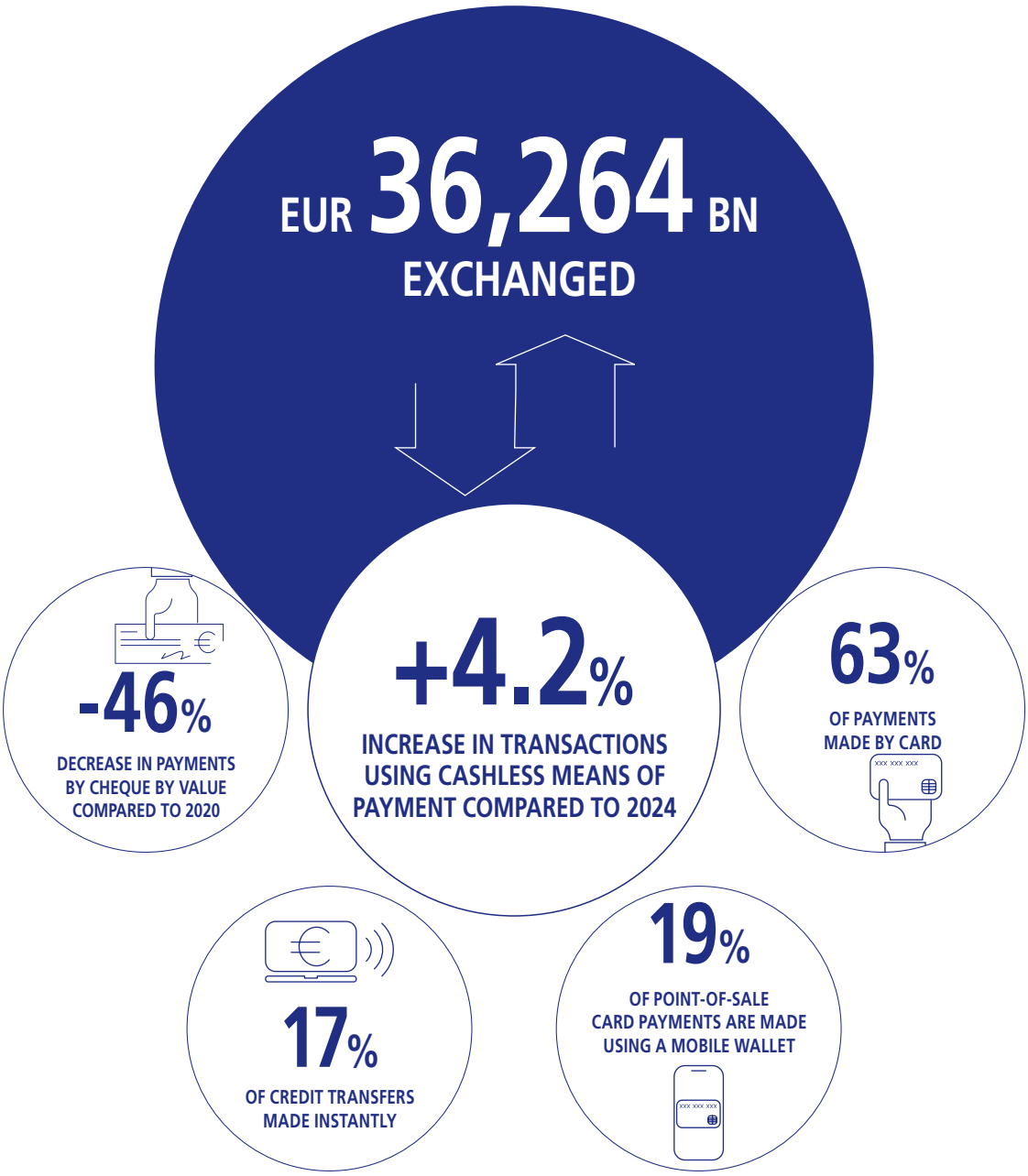
- ***Monitoring of the Observatory's recommendations to improve cheque security****, particularly with regard to the delivery of chequebooks by post and granting wider access to the* Fichier national des chèques irréguliers *(the French national register of irregular cheques) to help banks protect their depositors.*

Chapter 3 reports on the Observatory's monitoring of the security of payments using crypto-assets *and issues recommendations for payment industry professionals, merchants and users. These recommendations focus on the conditions required to ensure that they can be used with a level of security that matches traditional retail payment methods, such as cards or bank transfers, as closely as possible.*

Against a backdrop of rapidly evolving payment methods – and fraud techniques – the Observatory remains committed to ensuring the security of all payment means. ***The aim is to offer genuine freedom of choice to all users, both individuals and businesses, in their day-to-day***

transactions. *As part of its work programme for 2026-27, the Observatory will direct its technology monitoring efforts towards the security of new authentication techniques and their integration into new payment journeys. This monitoring will address the security issues related to retail involving artificial intelligence agents. The Observatory will also build on the monitoring study published in its* 2023 Annual Report *to further its analysis of future risks linked to quantum computing in order to more clearly define the associated roadmap for the French market. Lastly, it will continue the fraud prevention initiatives undertaken in partnership with telecommunications and digital sector players, as well as its public awareness campaigns.*

THE USE OF MEANS OF PAYMENT IN 2025



FRAUD TRENDS IN 2025

0.047%
SHARP DECLINE IN CARD PAYMENT FRAUD RATE BELOW ITS HISTORIC LOW



-50%
DECREASE IN THE FRAUD RATE FOR CARD PAYMENTS OVER THE INTERNET SINCE 2020





0.069%
RATE OF CHEQUE FRAUD STABILISED

EUR 1.241 BN
IN LOSSES



+3.8%
INCREASE IN FRAUD BY VALUE



0.041%
INSTANT CREDIT TRANSFER FRAUD RATE



EUR 516 M
OF SOCIAL ENGINEERING FRAUD

2025 IN NUMBERS

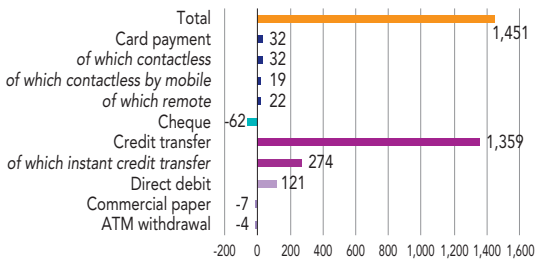
1

FRAUD IN 2025

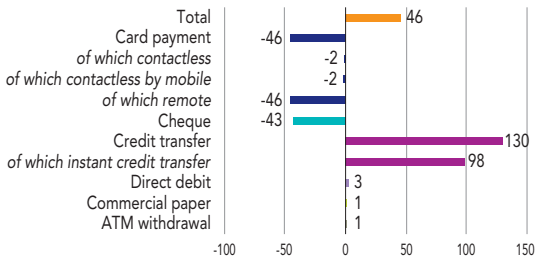
Key data

C1 Changes in means of payment between 2024 and 2025

a) Payment flows (EUR billions)

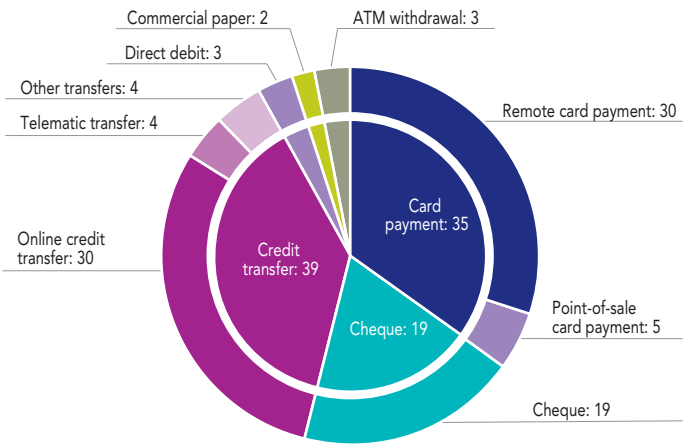


b) Fraud (EUR millions)



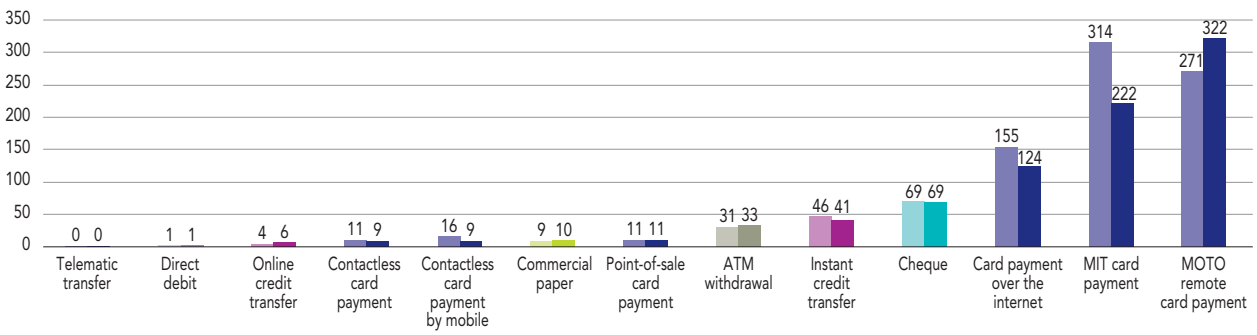
Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

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 2024 and 2025 (in EUR defrauded per EUR 100,000 of payments)

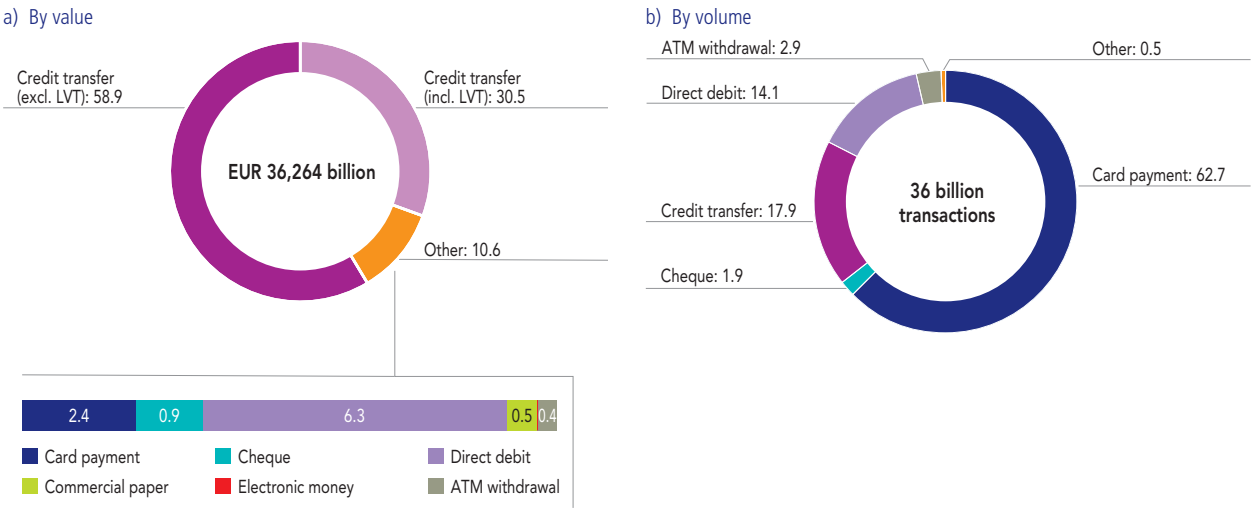


Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine; MIT, merchant-initiated transaction.

1.1 Overview

1.1.1 An overview of means of payment

C4 Use of cashless means of payment in 2025 (%)



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

Individuals, businesses and public authorities carried out 35.6 billion cashless payment transactions in 2025 (up 5.5% from 2024), with a total value of EUR 36,264 billion (up 4.2% from 2024).

As has been the case in recent years, the use of innovative payment methods saw sustained growth rates, while cheque use continued to fall: the value of cheque transactions decreased by 16%, and now accounts for just 1.9% of transaction volumes.

Credit transfers continued to make up the lion's share of total transaction flows by value, retaining a steady share at 89%. Large-value transfers (LVTs) accounted for 34% of transferred values, but only 0.2% of transfer volumes. The use of instant credit transfers expanded (up 78% in volume terms and 118% by value) and now accounts for 17% of all transfers by volume, compared with 10% in 2024.

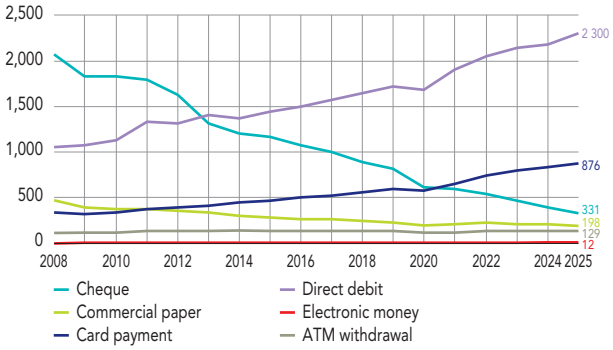
Bankcards are still France's preferred cashless payment method, and their use continues to increase. Their share of transaction volumes (excluding withdrawals) rose from 62.1% in 2024 to 62.7% in 2025. The growth in transaction volumes was also echoed in contactless payments, which accounted for 72% of point-of-sale card payments, compared with 68% in 2024. This growth was partly driven by payments by mobile phone, which continue to expand and accounted for more than 19% of point-of-sale card payments, compared with 15% in 2024.

Cash withdrawals by cards fell for the second consecutive year (down 5% in volume terms and 3% by value).

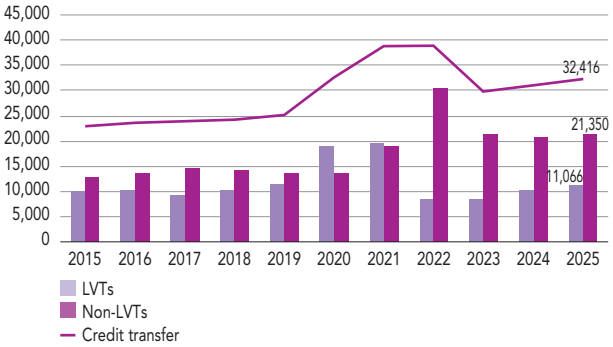
Direct debits followed the broad trend observed across all means of payment and rose by 5% in volume terms and 6% by value compared with 2024.

C5 Payment flows in value terms (EUR billions)

a) By instrument (excluding credit transfers)

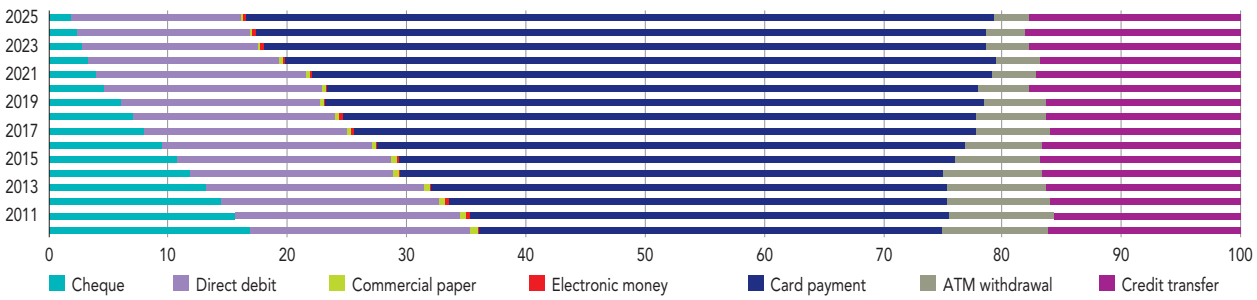


b) By credit transfer



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

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

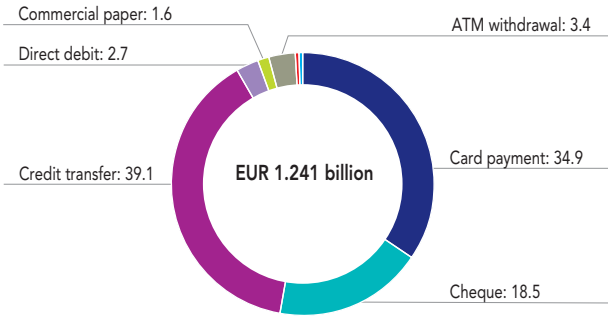


Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

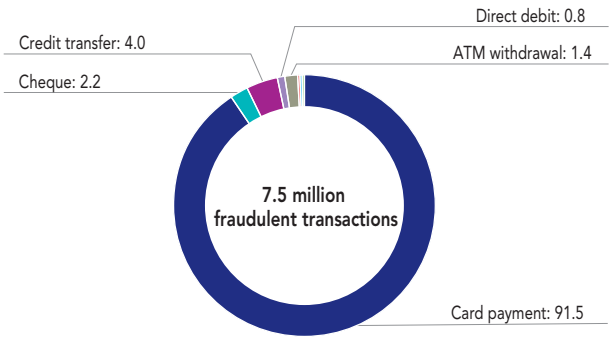
1.1.2 Overview of means of payment fraud

C7 Breakdown of fraud (%)

a) By value

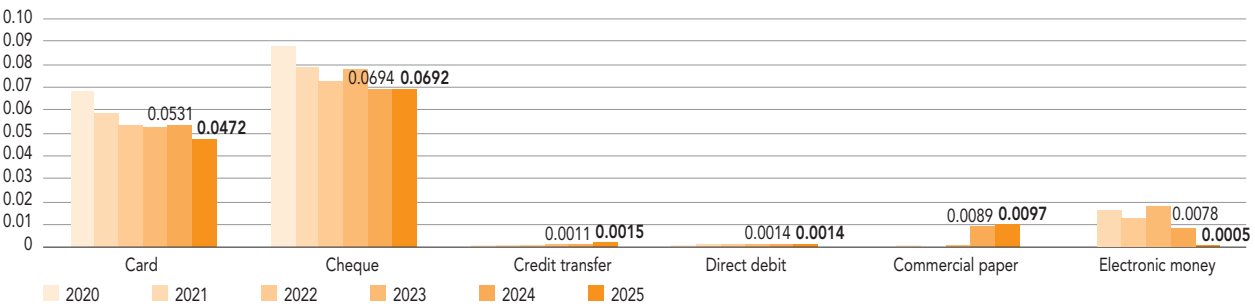


b) By volume



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.

The increase in cashless transactions has gone hand-in-hand with an increase in fraud, which rose – albeit at a slower rate than in 2024 (up 3.8% compared with 4.2% in terms of value) – to EUR 1.241 billion. However, the number of fraudulent transactions declined by 7.6% to 7.2 million cases.

These trends are the result of an increase in credit transfer fraud (up EUR 130 million, including EUR 98 million on instant credit transfers) and, to a lesser extent, (i) direct debit fraud (up EUR 3 million), (ii) fraud on card withdrawals (up EUR 1.3 million), and (iii) commercial paper fraud (up EUR 1.1 million). This was partly offset by a decline in remote card payment fraud (down EUR 46 million), which accounts for the bulk of the change in overall card payment fraud, and a decrease in cheque fraud (down EUR 43 million).

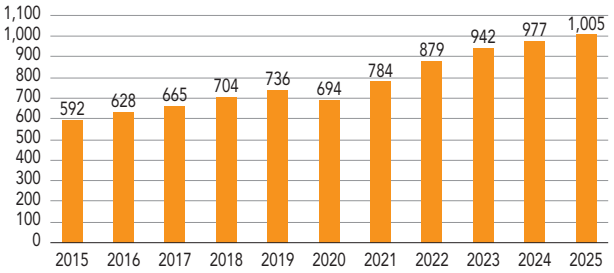
Credit transfers therefore became the main source of fraud by value in 2025, accounting for 39% of fraud, compared with 30% in 2024.

1.2 Current state of payment card fraud

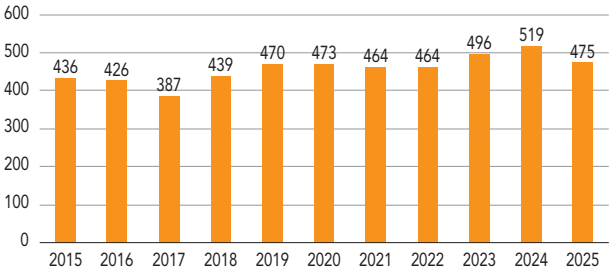
1.2.1 Overview – Cards issued in France

C9 Cards issued in France in 2025

a) Total value of transactions (EUR billions)



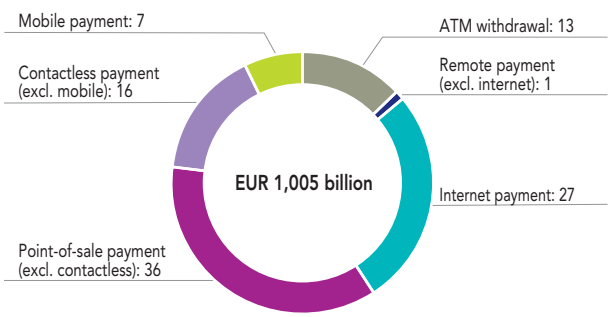
b) Total value of fraud (EUR millions)



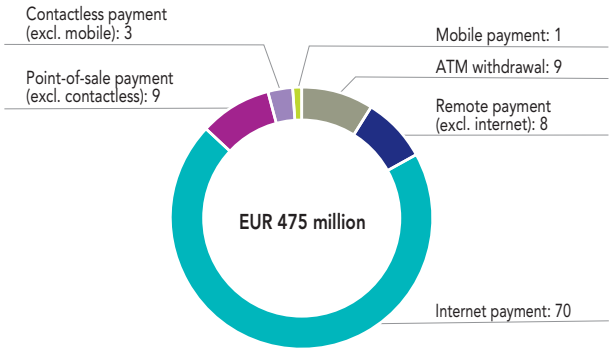
Source: Observatory for the Security of Payment Means.

C10 Use of cards issued in France by payment initiation channel in 2025 (%)

a) Breakdown of transaction amount

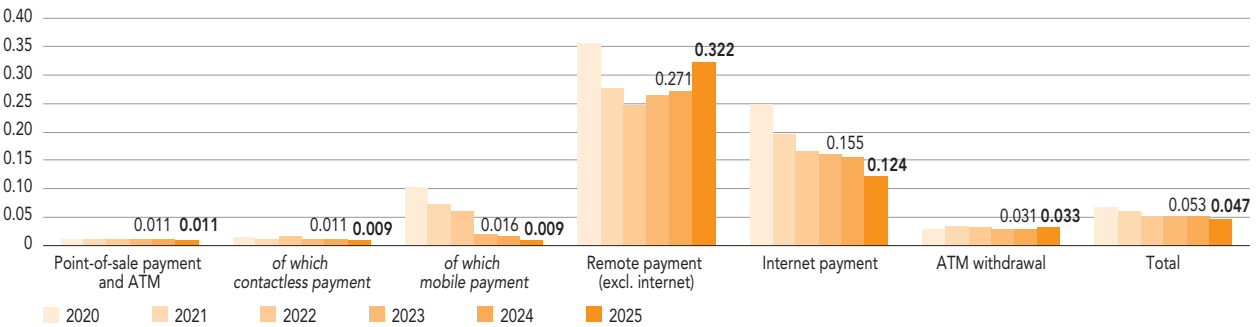


b) Breakdown of fraud amount



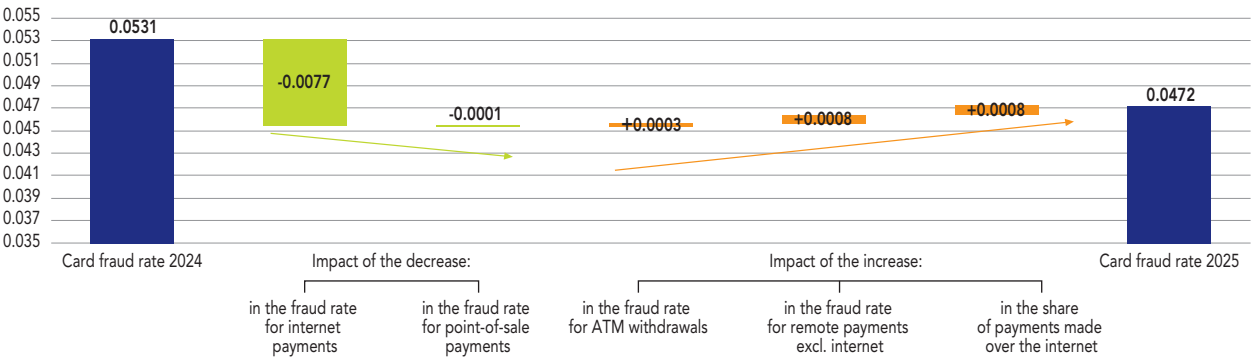
Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

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.

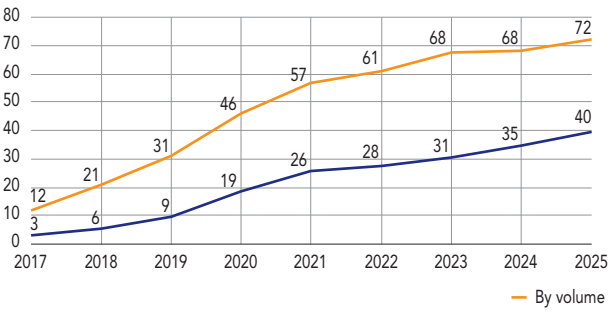
C11 *bis* Impact of changes in fraud rates by channel on the overall fraud rate (%)



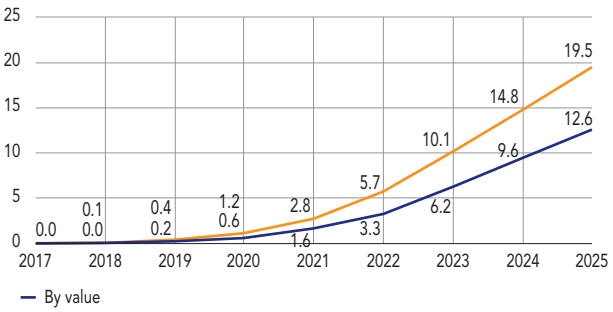
Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

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.

Payment cards continued to be the main means of payment for everyday use, with transaction flows continuing to increase in 2025 in terms of both volume and value (6.5% and 4% respectively). Growth in payments made by mobile continued, increasing by 38% and accounting for 19% of point-of-sale payments.

While transaction volumes increased, fraud fell to EUR 475 million by value, down 8.6% compared with 2024. Internet card payments remain the most exposed channel, despite fraud declining sharply: they account for 70% of fraud in terms of value, but only 27% of total transaction amounts.

After three years of stabilisation, the fraud rate on payments by cards issued in France began to decline again, to 0.047%, a new record low. While fraud rates on payments at points of sale and unattended payment terminals remained stable and very low at 0.011%, the fraud rate for internet payments fell again, and significantly, to 0.124% in 2025 from 0.155% in 2024. This result reflects the impact of the action plan drawn up by the *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) to address this issue and the effort deployed by the payments ecosystem as a whole. The fraud rate for remote payments not made over the internet, which include payments for which customers communicate their payment card information to businesses via mail orders and telephone orders (MOTO), increased significantly to 0.322% in 2025, compared with 0.271% in 2024. As a result of the measures implemented to prevent fraud on remote card payments[1] – including restrictions on uses and the introduction of a velocity limit – transaction volumes have fallen more rapidly (down 21%) than cases of fraud (down 7%).

The decline in the fraud rate for mobile payments accelerated in 2025 (down 43% compared with 2024). This long-term trend is directly linked to improved checks on user enrolment in mobile payment solutions through the systematic use of strong cardholder authentication, following a reminder of the relevant regulatory requirements by the European Banking Authority and the Observatory. These improvements are all the more remarkable given that payment by mobile has soared in popularity over recent years.

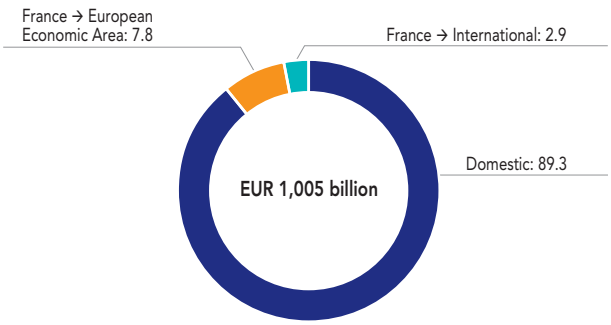
Lastly, the fraud rate for card withdrawals rose to 0.033% in 2025 (from 0.031% in 2024), due to an increase in courier fraud.

1 See Chapter 2, Section 2, "Prevention of fraud on remote card payments".

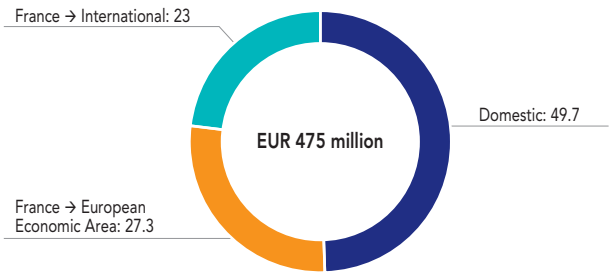
1.2.2 Breakdown of fraud by geographical area – Cards issued in France

C13 Cards issued in France by geographical area (%)

a) Breakdown of transaction amount

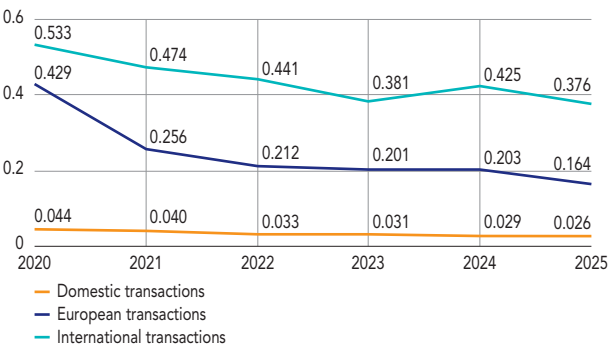


b) Breakdown of fraud amount



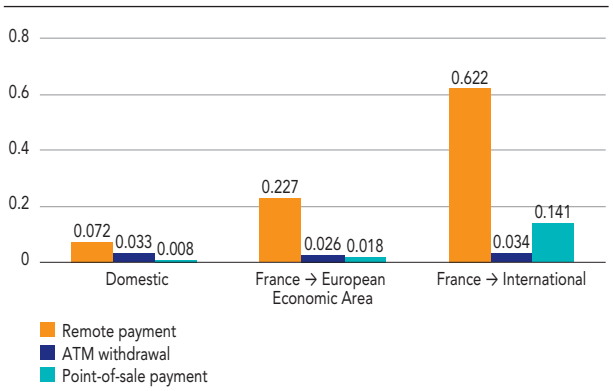
Source: Observatory for the Security of Payment Means.

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.

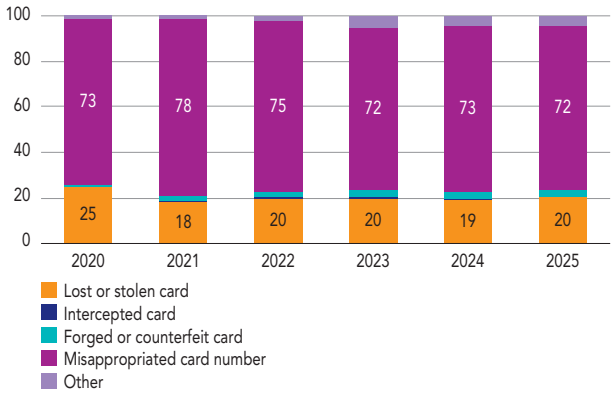
In 2025, international transactions (including those to the European Economic Area) continued to account for half of the total value of card payment fraud (50% in 2025, compared with 52% in 2024), despite accounting for only 11% of transactions.

Although international card transactions are, by their very nature, more exposed to fraud, their fraud rate has continued to improve following a slight rise in 2024 (0.376% in 2025, compared with 0.425% in 2024, for international transactions outside the European Economic Area, and 0.164% compared with 0.203%, for European transactions).

International transactions outside the European Economic Area are largely made up of remote payments (85%), which are historically more prone to fraud than their domestic equivalents. International payments at point of sale also remain more exposed to fraud than those made in France or within the European Economic Area, 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.

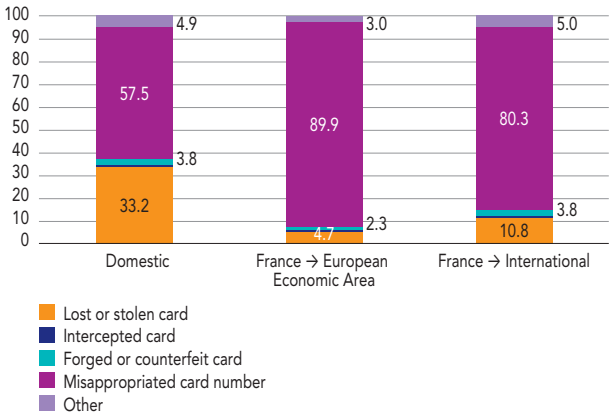
1.2.3 Breakdown of fraud by geographical area – Cards issued in France

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



Source: Observatory for the Security of Payment Means.

C17 Types of fraud by geographical area in value terms in 2025 (%)



Source: Observatory for the Security of Payment Means.

Card number theft, mainly using phishing techniques by email or SMS, continues to be by far the most common type of fraud, but its share in terms of value stabilised (72% in 2025 and 73% in 2024).

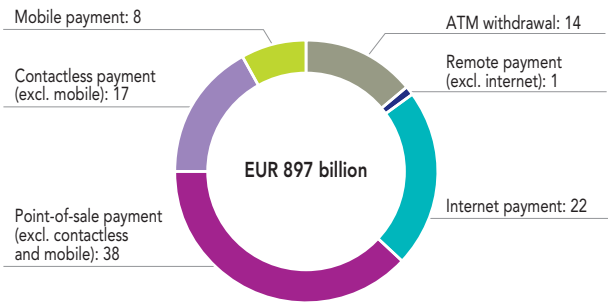
The proportion of fraud linked to lost or stolen cards was also stable and remained low (20% in 2025, compared with 19% in 2024). Logically, lost or stolen French cards are used first and foremost on French territory (33% of fraud), while fraud involving card number theft takes place primarily over the internet with no regard to geographical location, although it is even more prevalent in European and international transactions.

Other types of payment card fraud, such as those involving intercepted or counterfeit cards, remain marginal.

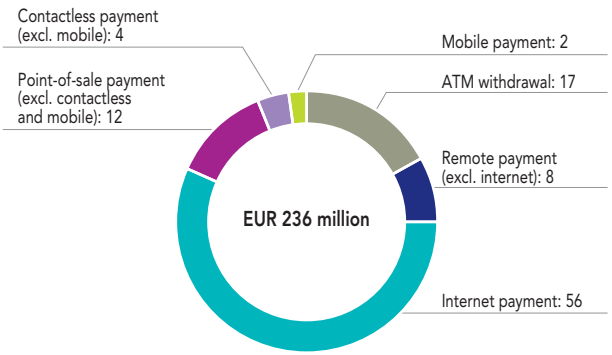
1.2.4 Breakdown of fraud in domestic transactions

C18 Domestic card transactions in value terms (%)

a) Breakdown of transactions

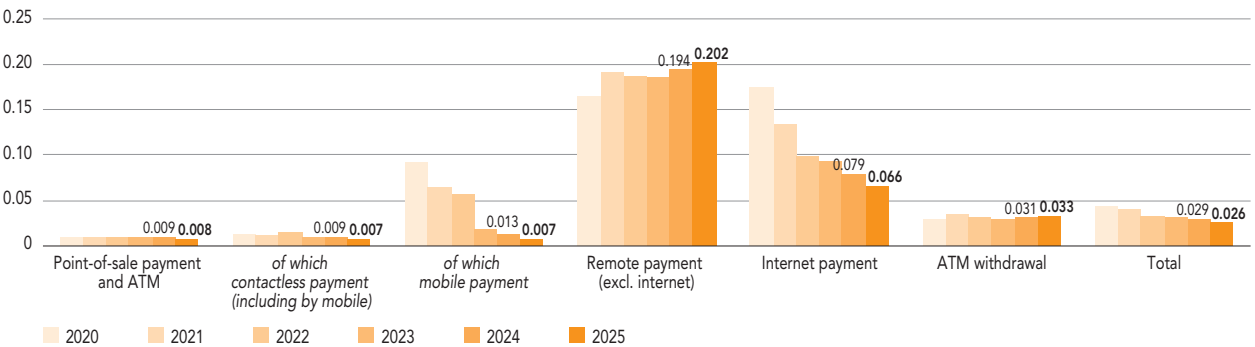


b) Breakdown of fraud



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

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



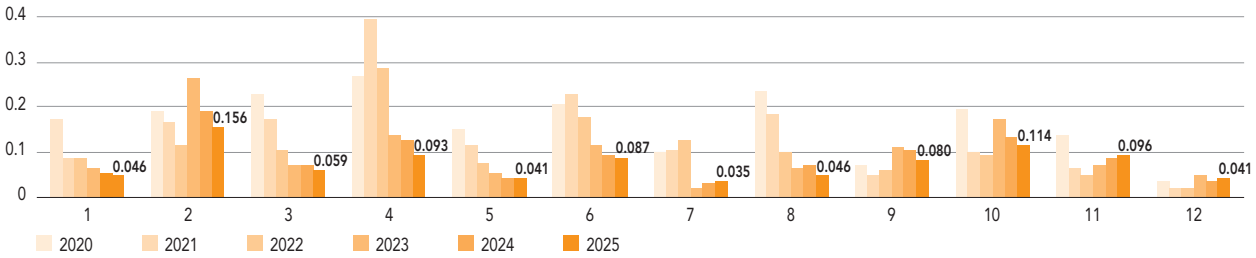
Source: Observatory for the Security of Payment Means.
Note: ATM, automated teller machine.

Domestic transactions are increasingly secure, with the fraud rate once again hitting a historic low, at 0.026% in 2025 (down from 0.029% in 2024).

Remote (internet and non-internet) payment transaction scams accounted for 64% of total French domestic fraud, with EUR 152 million in losses, despite making up only 23% of the amounts exchanged. The cumulative fraud rate for these payments fell by a further 8% year-on-year to 0.072%, versus 0.079% in 2024. The rate has more than halved since 2020.

1.2.5 Focus on domestic card payment fraud on the internet

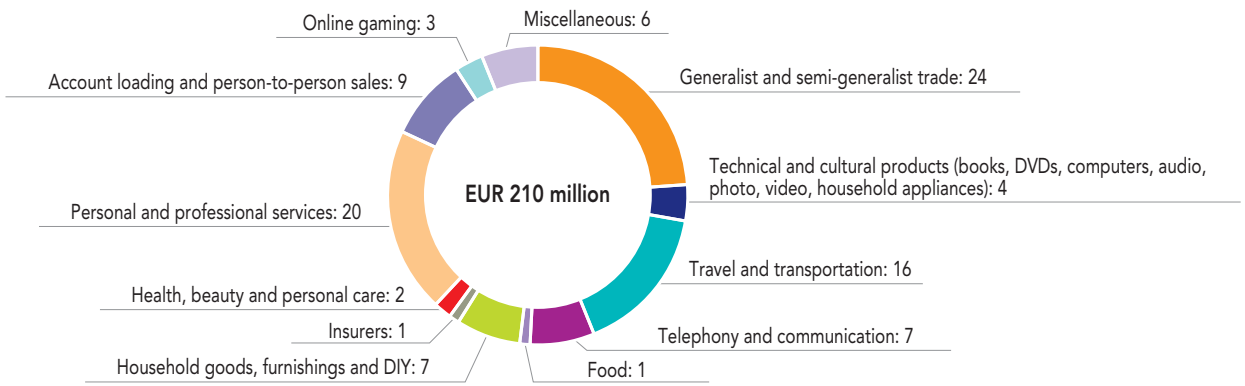
C20 Changes in fraud rates on domestic card payments over the internet, by sector (%)



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

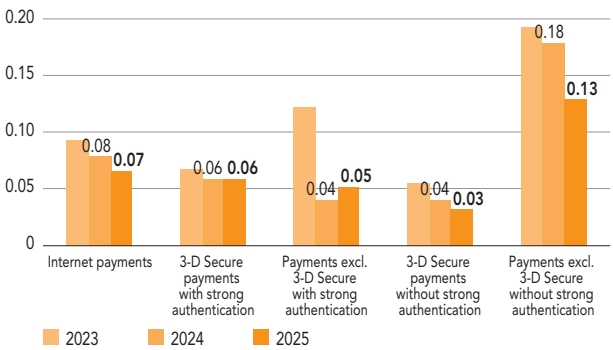
Source: Observatory for the Security of Payment Means.

C21 Breakdown of fraud on domestic card payments over the internet, by sector and in value terms in 2025 (%)



Source: Observatory for the Security of Payment Means.

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



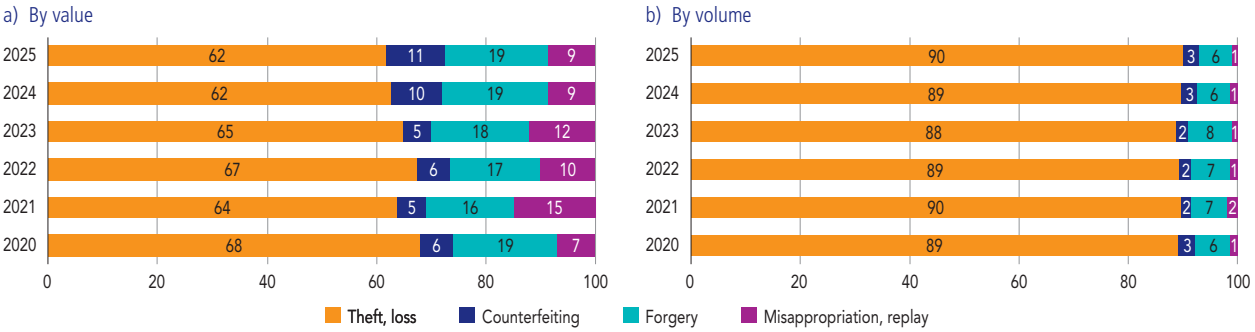
Source: Observatory for the Security of Payment Means.

Domestic card payments over the internet that (i) do not use the 3-D Secure protocol (or an equivalent proprietary protocol) and (ii) do not apply strong authentication are proportionally two times more exposed to fraud than other channels (three times more exposed in 2024). The structurally higher fraud rate warrants the measures introduced in June 2024 by the Observatory for these types of payment, which will continue to be rolled out over the coming years *(see Chapter 2, Section 2,"Prevention of fraud on remote card payments")*. Thanks to these measures, the associated fraud rate has nonetheless already fallen sharply (0.13% in 2025, compared with 0.18% in 2024). 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 remote card transaction flows (58%) and fraud (65%).

Furthermore, strong authentication exempt solutions are always effective when they rely on 3-D Secure. The fraud rate remained half that for transactions involving strong authentication (0.03%, compared with 0.06%), which shows that the exemptions in place continue to effectively identify the least risky transactions.

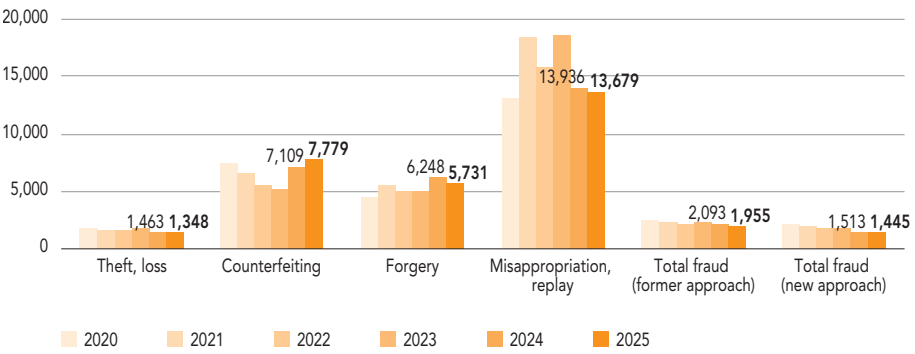
1.3 Current state of cheque fraud

C23 Breakdown of cheque fraud by type (%)



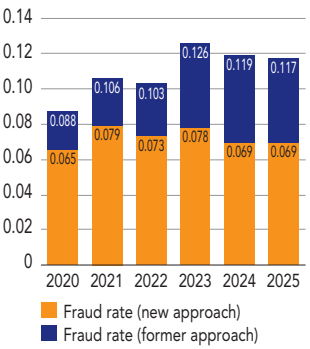
Source: Observatory for the Security of Payment Means.

C24 Average value of cheque fraud by type of fraud (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.

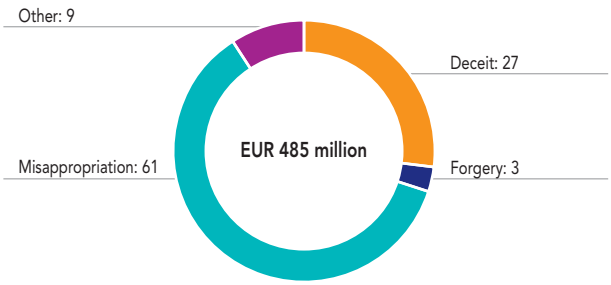
Cheque fraud continued to decline in 2025, falling 16% year-on-year to EUR 229 million. The rate after deduction of thwarted cheque fraud remained stable at 0.069%. These positive results demonstrate the lasting impact of the implementation of the Observatory's recommendations against cheque fraud published in 2021, including measures to block or delay cheque payments. As a result, 41% of fraudulent payments were neutralised (EUR 158 million in thwarted fraud).

By far the main type of cheque fraud continues to be 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. Consequently, the shipment and delivery of chequebooks remain a key area of vulnerability in the cheque lifecycle.

Lastly, 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 efforts to build on the progress made, particularly with regard to implementing recommendations on the protection of chequebooks during shipment and delivery and the simplification of procedures for reporting loss or theft *(see Chapter 2, Section 3.1, "The Observatory's recommendations on cheque fraud")*.

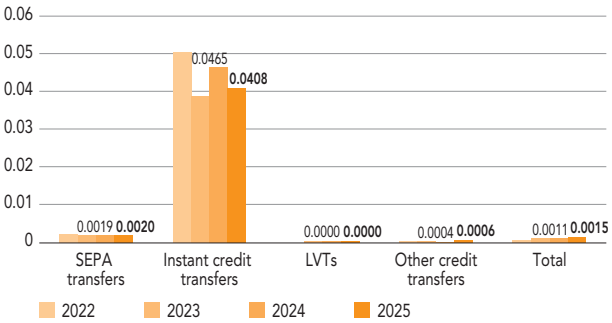
1.4 Current state of credit transfer fraud

C26 Breakdown of transfer fraud by type of fraud in value terms in 2025 (%)



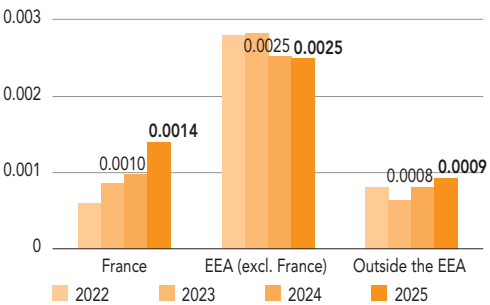
Source: Observatory for the Security of Payment Means.

C27 Transfer fraud rate by type of transfer (%)



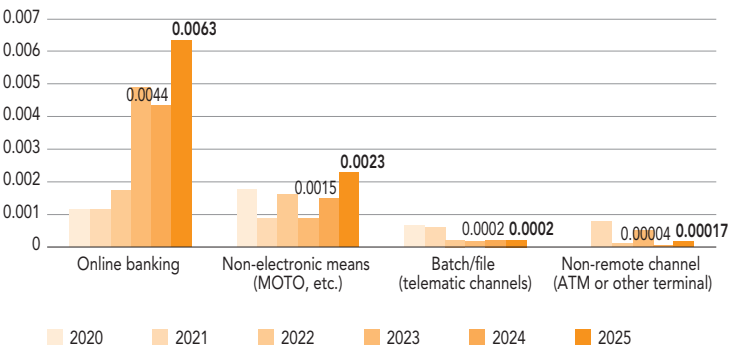
Source: Observatory for the Security of Payment Means.
Note: SEPA, Single Euro Payments Area; LVT, large-value transfer.

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: ATM, automated teller machine.

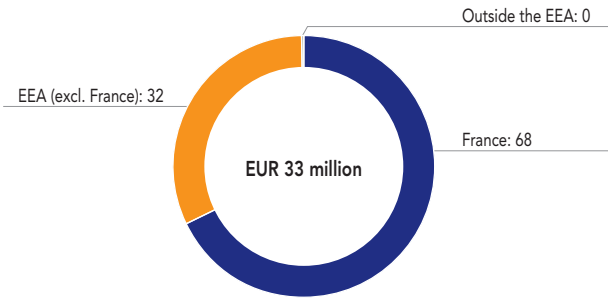
Credit transfer fraud rose by 37% to EUR 485 million in 2025 as a result of a structural change in the fraud: the telematic channels used by businesses continued to have very low exposure to fraud (a fraud rate of just 0.0002%), while fraudster tended to concentrate their attacks on online banking solutions (a fraud rate of 0.0063%). 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 (45% increase in the domestic fraud rate), although European transfers remain almost twice as exposed to fraud compared with French domestic transfers, despite a slight decline in the fraud rate (down 1%).

The instant credit transfer fraud rate edged down from 0.046% in 2024 to 0.041% in 2025 and remained below the card fraud rate (0.049%), even though these two payment methods, both widely used by consumers, rely on similar security mechanisms, including the same strong authentication solutions for online payments.

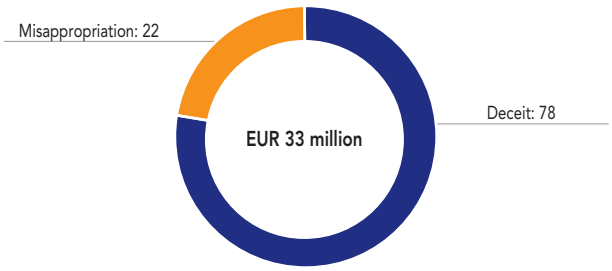
1.5 Current state of direct debit fraud

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

a) By geographical area



b) By type of fraud

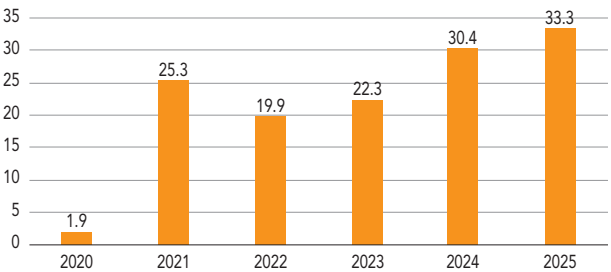


Source: Observatory for the Security of Payment Means.

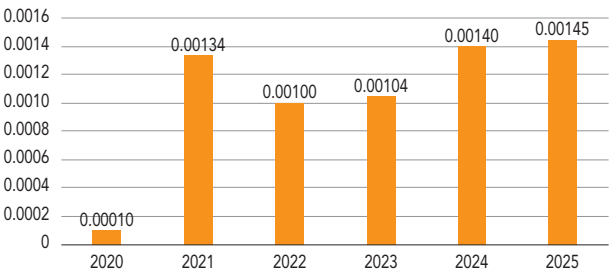
Note: EEA, European Economic Area.

C31 Direct debit fraud

a) By value (EUR millions)



b) Rate (%)



Source: Observatory for the Security of Payment Means.

Direct debit fraud rose by 9% in value terms to EUR 33 million, while the fraud rate remained relatively stable at 0.0014%.

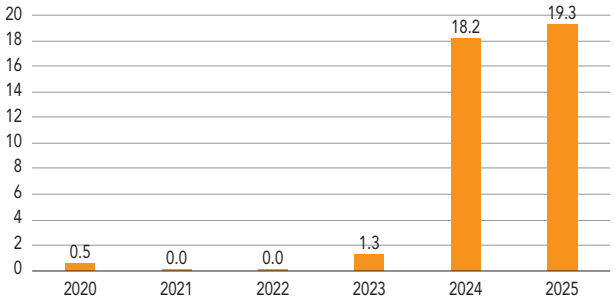
This type of fraud is mainly perpetrated – at 78%, compared with 96% in 2024 – by fraudsters that have no direct debit mandate nor any economic relationship with the victim that issue fake orders. Fraud by misappropriation – whereby the fraudster usurps the identity and international bank account number (IBAN) of a third party to sign a direct debit mandate, increased year-on-year to 22% in 2025, compared with just 4% in 2024.

French account holders remain the most affected, although people within the European Economic Area are twice as likely to fall victim to direct debit fraud as in 2024 (their share rose from 16% in 2024 to 32% in 2025).

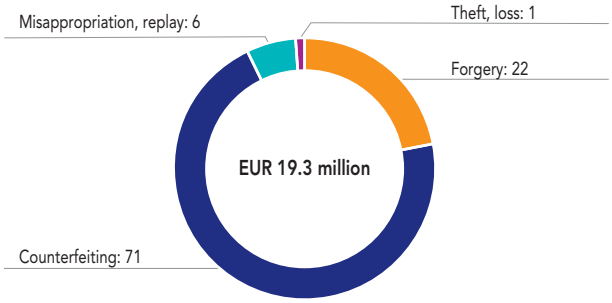
1.6 Current state of commercial paper fraud

C32 Commercial paper fraud

a) By value (EUR millions)



b) By type of fraud (%)



Source: Observatory for the Security of Payment Means.

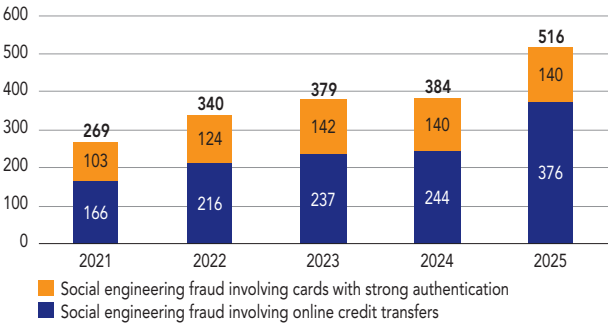
Following a significant increase in 2024, commercial paper fraud tended towards stabilisation in value terms in 2025 (up 6% to EUR 19.3 million), and continued to account for a marginal amount of the total value of means of payment fraud (less than 2%). As the value of transactions declined in 2025 compared with 2024 (down 3.5%), the fraud rate rose mechanically. The average value of each fraudulent transaction increased from EUR 51,888 in 2024 to EUR 60,912 in 2025.

The fraud typology remained similar to 2024, with counterfeit commercial papers – fake commercial papers created entirely by fraudsters – predominating. Forgery, whereby fraudsters intercept and amend genuine commercial papers, accounted for 22% of the fraud in value terms.

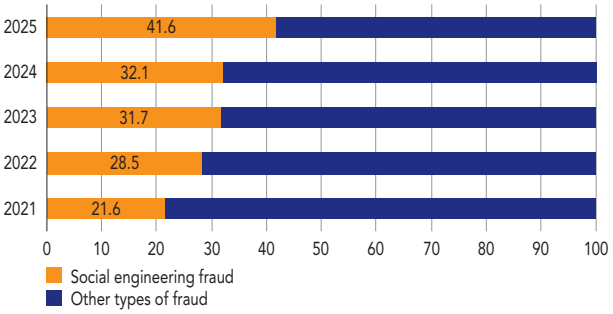
1.7 Current state of social engineering fraud

C33 Change in social engineering fraud in value terms

a) By value (EUR millions)

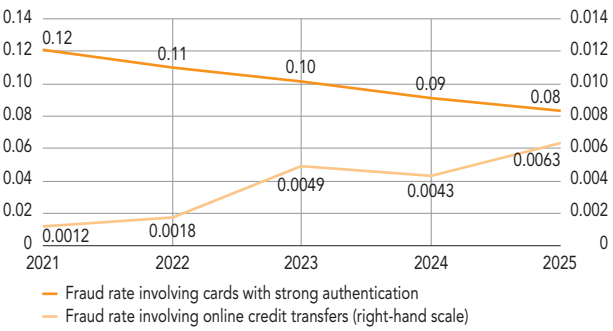


b) Share (%)



Source: Observatory for the Security of Payment Means.

C34 Changes in social engineering fraud rates (%)



Source: Observatory for the Security of Payment Means.

Social engineering fraud includes cases where the customer is manipulated during a phone call. Often, the fraudster poses as a payment service provider, such as a fake bank adviser or an anti-fraud service employee. The Observatory measures the extent of this fraud by proxy, through the sum of fraudulent transactions by payment card with strong authentication and by online bank transfer.

Although social engineering fraud has been trending upwards since 2021 (rising by 43% between 2021 and 2024), the rate of increase accelerated in 2025, growing by 34% over the year to EUR 516 million. While fraud on strongly authenticated card transactions remained stable at EUR 140 million, online banking fraud increased significantly from EUR 244 million in 2024 to EUR 376 million in 2025. The online banking transfer fraud rate picked up sharply in 2025, following a one-off decline in 2024 (0.0063% in 2025, compared with 0.0044% in 2024). This significant increase is due to rapid growth in the value of fraud against a more moderate rise in transaction volumes (54% compared with 18%). The fraud rate for strongly authenticated card transactions continued to fall (0.08% in 2025, compared with 0.09% in 2024).

Lastly, in value terms and for all fraud techniques combined, the share of fraud attributable to social engineering scams continued to grow, reaching 41.6% in 2025, up from 32.1% in 2024. Given this trend, the Observatory invites the various players in the ecosystem to: (i) step up their awareness-raising efforts; (ii) implement concrete measures to combat this type of fraud (adapting authentication procedures for online banking and banking apps, enhancing scoring tools and exploiting new data-sharing mechanisms, etc.); and (iii) strengthen their cooperation with the telecommunications and digital sectors *(see Chapter 2, Section 1, "Action plan to combat social engineering fraud")*.

BOX

❶

Indicators from the French Ministry of the Interior on means of payment fraud in 2025

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 2025, as they do every year, these two bodies reported their main observations on payment means 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 9 July 2026, the *Service statistique ministériel de la sécurité intérieure* (SSMSI – French ministerial statistical service for internal security) published its 2025 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 make it impossible to directly reconcile the data published by the SSMSI and the figures published by the Observatory.

1.2 The findings of the SSMSI and the Observatory show the same trends

Despite the different methods and sources, there are a number of similarities between the SSMSI's report and trends in means of payment fraud noted by the Observatory.

The number of victims of scams and means of payment fraud recorded by the *Police Nationale* and the *Gendarmerie Nationale* continued to increase, rising from 417,300 cases in 2024 to 448,300 in 2025 (up 7% between 2024 and 2025, compared with a 1.4% increase between 2023 and 2024).

Means of payment fraud is increasingly based on manipulating victims (e.g. fake bank adviser scams, CEO fraud, bank account details fraud, etc.) and continues to target individuals more than organisations. According to the SSMSI study, organisations accounted for 8% of victims of fraud in 2025, down from 16% in 2016.

The study reports that in 2025, **more than half of all scams and means of payment fraud cases were linked to digital technology (53%, compared with 50% in 2024)**. This share has soared since 2016, when it accounted for 31%, reflecting the growing role of digital technology in scams and means of payment fraud.

Young adults are the most common victims of scams and means of payment fraud. The number of victims known to law enforcement rises significantly from age 18 onwards, peaking at between 20 and 24 years of age, with a rate of 9.6 victims per 1,000 people in that age bracket (up from 9 victims in 2024).

1 See Ministry of the Interior, *Insécurité et délinquance en 2025: bilan statistique*, 2026 edition.

2 According to the SSMSI's *Vécu et ressenti en matière de sécurité* (VRS) 2023 survey into people's experiences and feelings with regards to their security, a little over 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.

More than 70% of victims fall into the 18-to-44 age bracket, despite it accounting for only 33% of the population.

Scams involving fake bank transfer orders and targeting organisations (companies, government agencies, local authorities) are watched particularly closely by law enforcement. Law enforcement agencies define fake bank transfer order scams as 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 insists on the need to act urgently and in strict confidentiality.

In 2025, 640 fake bank transfer order scams against organisations were reported to the DNPJ, with losses totalling EUR 43 million, compared with 680 cases[4] and losses of EUR 36 million[5] in 2024. The number of cases declined slightly by 6%, despite remaining high, while the total value increased by 19%. The development of artificial intelligence tools, which can be used to produce perfectly forged emails or voices and images impersonating company directors, could further fuel the momentum of fake bank transfer order scams.

Bank transfer fraud by misappropriation **reported to the Observatory by payment industry players** rose sharply in both value and volume terms, by 62% and 276%, respectively.

2. Focus on the Perceval and Thésée platforms

Since 2018, the *Gendarmerie*'s **Perceval platform** has been used to collect reports of the fraudulent use of payment cards on the internet from users. Its data can be more easily reconciled with the trends observed by the Observatory. There were 206,902 cases filed in 2025, down 9% from 227,711 in 2024. It is important to note that one case reported on Perceval may actually cover several different fraudulent transactions initiated using the same stolen card details.

The number of frauds reported on Perceval remained largely stable. Only 39% of card fraud involving internet payments as quantified by the Observatory was reported on Perceval in 2024, compared with 37% in 2025 and 44% in 2023. Victims tend to report only the largest frauds: in 2025, the average value of a fraudulent transaction, according to the Observatory's statistics, was EUR 60, compared with EUR 178 according to Perceval (EUR 622 per complaint filed, which contained an average of 3.49 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 certain types of internet scams to lodge a complaint online.[6] In 2025, 55,300 complaints were made on the Thésée platform. This represents 12% of the total number of victims of means of payment fraud and scams recorded by the SSMSI, which was relatively unchanged year-on-year (11% in 2024).

The Observatory urges scam and fraud victims to report their cases on the Perceval and Thésée platforms, or, if ineligible, file a complaint at a police station or with the *gendarmerie*. These reports provide law enforcement agencies with the information they need to dismantle fraud networks.

4 The 2024 statistics reported here may be slightly higher than those contained in the OSMP's *2024 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. The DNPJ can be informed about complaints several months after the incidents occurred, which means that the totals for the years in question have to be 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 for cases of fake retail websites, fake online rentals, classified ad frauds, romance scams, online blackmail, email account hacking and ransomware. For all other types of scams (such as CEO fraud, bank account details fraud, fake bank adviser scams, fake IT support scams or investment scams), a complaint must be lodged in person at a police station or gendarmerie unit. Thésée data are included in the number of victims of means of payment fraud published on 9 July 2026 by the SSMSI in its statistical study on insecurity and crime in 2025.

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 card data stolen by the crime networks are then re-encoded on counterfeit magnetic stripe cards, which are then 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 have a strong cardholder authentication solution.

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 have so far remained limited.

Figures from the *Groupement des Cartes Bancaires CB* (France's national interbank network) highlight an overall decline 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.

A shimmer is 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

WORK CARRIED OUT BY THE OBSERVATORY ON FRAUD PREVENTION

2.1 Action plan to combat social engineering fraud

2.1.1 Background to our work

European Directive No. 2015/2366 of 25 November 2015 on payment services (PSD 2) introduced stricter regulatory requirements regarding the security of remote payments. The Observatory assisted in its implementation, notably within the framework of a migration plan for the roll-out of strong customer authentication, both for internet card payments and for credit transfers made on online banking platforms.

Technical measures to make payments safer and more secure have therefore been strengthened. Consequently, fraud scenarios have evolved in response. Fraudsters now focus on scamming their victims through manipulation.

For example, in the case of the "fake bank adviser" scam, the fraudster usually poses as a bank adviser or an anti-fraud service employee. They try to persuade the victim to authorise fraudulent transactions, using strong authentication, under the pretence of cancelling or blocking them. To contact their victims and impersonate payment service providers (PSPs), fraudsters use communication channels that are well known to the general public (telephone calls, messaging apps, social media networks, etc.).

Preventing this type of fraud requires a comprehensive approach that takes into account the tactics and tools of the fraudsters:

- Raising user awareness is key given that the attacks target users directly. The challenge is both to prevent the sensitive data that is subsequently reused in social engineering scams from initially being disclosed – particularly during phishing campaigns – and to enable users to detect these types of scams and know how to react.
- At the PSP level, improving their communication and engagement with their customers is essential to countering social engineering manipulation. It is therefore important to provide different opportunities throughout each payment journey to make customers aware of the possibilities that the transaction may be fraudulent. For PSPs, the aim is also for them to adapt their risk management tools to better identify fraud attempts and to delay or even block transactions where necessary.
- Lastly, it is important to improve the security of the communication channels through which users are exposed to these different types of identity theft: fake emails, SMS or instant messaging; mirror sites; and fake online advertising. To fulfil an ambition of this kind, the Observatory has to develop its cooperation with stakeholders who do not strictly fall within the payments sector, such as telecommunication or social media operators.

2.1.2 Measures taken by payment service providers

Social engineering techniques are becoming increasingly sophisticated and tend to impair users' ability to properly understand the messages directed at them. To remedy this, payment service providers are faced with the imperative of having to protect their customers from themselves, which involves enhancing the fraud prevention mechanisms already in place to ensure their effectiveness keeps pace with evolving threats, while leveraging technological and regulatory developments.

2.1.2.1 Enhancing the effectiveness of existing prevention measures against the risk of social engineering fraud

A number of recommendations on fraud prevention previously issued by the Observatory remain to this day appropriate levers for action against social engineering fraud. This is particularly the case for:

- Recommendations relating to the use of artificial intelligence (AI) for fraud prevention purposes *(see Section 2.4 of this chapter, Table 8)*, which invite institutions to continuously enhance their AI-based detection systems, particularly with regard to the data scope. In this regard, using metadata from the user's telephone that makes it possible to determine whether the user is communicating with a third party (via a telephone call or a videoconferencing service) at the moment an atypical transaction is authorised is an avenue worth exploring.
- Recommendations relating to the security of real-time payments *(see Section 2.4 of this chapter, Table 12)*, particularly Recommendations No. 3 and No. 4. Recommendation No. 3 invites payment service providers to implement measures to configure the conditions for use of real-time payments (particularly with regard to transaction ceilings). Recommendation No. 4 calls for the detection of series of high-risk transactions, for example, the closure of savings accounts, the creation of a new beneficiary and an increase in the transaction ceiling prior to a request to issue a credit transfer for an unusual amount).
- The introduction of the *Fichier national des comptes signalés pour risque de fraude* (the French national register of accounts flagged for fraud risk) – *see Section 2.3.2 of this chapter, "Recommendations on SEPA payment fraud"*.[1] This register serves as an additional tool in the fight to prevent social engineering fraud as it enables payment service providers to share information on accounts used by fraudsters.

The Observatory will monitor the implementation of these recommendations, as part of an ongoing process of continuously improving fraud detection mechanisms and strengthening the capacity to delay, or even block, transactions with a manifestly high risk of social engineering fraud.

2.1.2.2 Improvements arising from the recommendations on procedures for reimbursing fraudulent payment transactions

The Observatory's recommendations on procedures for reimbursing fraudulent payment transactions were published on 16 May 2023 and in its 2022 Annual Report. These formed a set of 13 recommendations issued amid a significant rise in fraud cases involving social engineering techniques. Its aim was to clarify the procedures used in applying the legislative framework for the reimbursement of disputed transactions and to strengthen fraud prevention mechanisms.

Eighteen months after its implementation, the assessment of the results of the recommendations set out in the 2024 Annual Report highlighted, in particular: (i) improved security of payment journeys, particularly online and in banking applications; (ii) improved handling of fraud-related disputes; and (iii) the systematic and immediate reimbursement of fraudulent card payments not covered by strong authentication. However, it highlighted the need for further efforts regarding the reimbursement of fraudulent payments by credit transfer without strong authentication.

In conjunction with the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French Prudential Supervision and Resolution Authority), the Banque de France will continue to monitor practices at individual institutions, especially those that could further improve the application of the recommendations. To this end, the Banque de France will notably draw on statistical classification indicators on disputes and reimbursements generated on the basis of data collected on behalf of the Observatory from the main institutions operating in France.

1 SEPA – Single Euro Payments Area.

T1 The Observatory's recommendations regarding reimbursement in cases of fraud *(recommendations originally set out in the 2022 Annual Report)*

Recommendations	Target audience
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 No. 8), and to limit the duration of the investigation to 30 days, other than in exceptional circumstances.	Payment service providers
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.	Payment service providers
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.	Payment service providers
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, 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) 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 merchant-initiated transaction – 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, reimbursement depends on the conditions set out in their framework contract and the specific circumstances of the transaction.	Payment service providers
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.	Payment service providers

T1 The Observatory's recommendations regarding reimbursement in cases of fraud (continued)

Recommendations	Target audience
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 No. 11), any alerts linked to the transaction and sent to the user via different communication channels, elements reported by the user (see Recommendation No. 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 No. 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 No. 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 No. 1 to No. 3 in order to determine the user's right to reimbursement.	Payment service providers
7 – Good practices for the security of payment means Consumers should endeavour to remain vigilant with regard to 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 service 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 of uncertain origin; • never entrusting a payment instrument to a third party (relative, courier, etc.); • remaining attentive to communications from payment service providers 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.).	Consumers

T1 The Observatory's recommendations regarding reimbursement in cases of fraud (continued)

Recommendations	Target audience
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.	Consumers
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.	Payment service providers
10 – Procedures for registering credit transfer beneficiary IBANs[a)] Payment service providers are asked to clearly indicate, each time a beneficiary is added to a transfer, whether a concordance check between the IBAN and beneficiary name has been carried out. 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.	Payment service providers
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 procedure explicitly offers an option to cancel the transaction.	Payment service providers
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.	Payment service providers
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, spoofing and SIM-swapping.	Service providers and information technologies

a) Since 9 October 2025, the beneficiary verification service has been made mandatory under European legislation (Regulation (EU) No. 260/2012 of 14 March 2012, as amended by Regulation (EU) 2024/886 of 13 March 2024) and thus helps to minimise fraud and errors when entering International Bank Account Numbers (IBANs). Payment service providers must, however, ensure that they explicitly inform their customers when the beneficiary verification service is not available (e.g. international transfers, transfers in foreign currencies, etc.). They are also invited to remind their customers of best practice (regularly reviewing their lists of beneficiaries, making a follow-up call in case of doubt, not responding to unsolicited requests regarding the registration of their beneficiaries, etc.).

Source: Observatory for the Security of Payment Means.

Note: SEPA, Single Euro Payment Area; IBAN, international bank account number; spoofing, usurping a caller ID; SIM-swapping, duplicating a SIM card.

2.1.3 Cooperation with the telecommunications and digital sectors

In 2023, the composition of the Observatory's membership was consequently expanded to players in the telecommunications sector: the sector's main professional organisations (the *Fédération française des télécoms* (FFTélécoms – the French Telecoms Federation) and the *Association française pour le développement des services et usages multimédias multi-opérateurs* (AF2M – the French association for the development of multi-operator multimedia services and uses) and the *Autorité de régulation des communications électroniques, des postes et de la distribution de la presse* (Arcep – the French Regulatory Authority for Electronic Communication, Postal Services and Print Media Distribution). The Observatory is working with these bodies to monitor the implementation of the MAN (number authentication mechanism) programme,[2] which is designed to prevent fraudsters from usurping telephone numbers (spoofing) to make calls to their victims. Furthermore, the Observatory is working alongside the telecommunications sector and PSPs to help in their implementation of the recommendations set out in its 2024 Annual Report. These recommendations are primarily aimed at preventing the illegitimate use of traditional telephone channels and at improving cooperation between PSPs and the telecommunications sector *(see* "Recommendations intended to strengthen the security of telecommunications channels" *below).*

However, the heightened security of telephone channels is prompting fraudsters to exploit the features now offered by instant messaging apps and social media platforms. As a result, the Observatory published a roadmap for developing cooperation with the major digital sector players, such as Apple, Google, Meta and TikTok, in its 2024 Annual Report *(see* the roadmap for digital sector players *below).*

As part of efforts to prevent social engineering fraud, enhanced cooperation with the telecommunications and digital sectors complements other prevention and awareness-raising initiatives that are monitored and promoted by the Observatory (for example, improvements to strong authentication procedures, beneficiary verification, or the French national register of accounts flagged for fraud risk). This enhanced cooperation must, in particular, result in concrete actions on the part of digital sector players (such as platforms and social media networks) to limit the risks of fraud and secure the digital environment.

2.1.3.1 Overview of the progress observed

Cooperation with telecommunications sector players has led to significant progress in preventing social engineering fraud, although certain measures have not yet been fully implemented. In addition to the MAN number authentication mechanism, which has been largely operational since January 2025, several initiatives should further reinforce communication security:

- Displaying "No caller ID" when an international call (roaming) using a French mobile number cannot be authenticated, as required by Arcep in its national numbering plan, amended in December 2025.
- Launching a trial, starting in June 2026, of the Do Not Originate (DNO) mechanism for numbers identified by PSPs as being reserved exclusively for inbound calls: this mechanism complements the MAN programme by strengthening protection against spoofing of the most sensitive telephone numbers, such as those dedicated to blocking lost or stolen bankcards.
- Introducing, upon completion of a preliminary feasibility study, a single helpline number enabling payment service users to contact their PSP in the event of suspected fraud. This solution draws some inspiration from the Stop Scams UK initiative in the United Kingdom (contacted by dialling 159).

Furthermore, the Observatory has entered into early discussions with digital sector players – primarily Google, Meta and TikTok –, which have proven to be receptive and supportive of this approach. The work involved will be a long-term initiative. This cooperation should encourage players to reinforce the mechanisms they use to monitor and control their releases prior to diffusion. It also aims to enhance the exchange of information on fraudulent uses and content by simultaneously exploiting data held by (i) PSPs (particularly within the framework of the fraud cases they are investigating and their anti-fraud tools), and (ii) digital sector players (through cases flagged by their users but also through the results of their proactive analysis using artificial intelligence).

2.1.3.2 Improved security of communications between payment service providers and their customers, and strengthened cooperation with telecommunications operators

Operators using French telephone numbers are now legally required[3] to authenticate the numbers used to make calls, which is a first in the European Union. Operators have therefore put in place the interoperable MAN number authentication mechanism, which is the technical system that allows them to comply with their new legal obligation. Using it, an outgoing call is signed by the caller's operator. The operators who then route this call to its intended recipient use digital certificates to verify that the signature

associated with the call is valid. Failing this, the call routing must be terminated. The MAN programme is therefore a major tool in preventing caller ID usurpation (spoofing).

However, the persistence of a few cases of fake bank adviser scams using spoofing has prompted the Observatory to propose a trial of the Do Not Originate (DNO) mechanism to be led by the main telecommunications operators and begin in June 2026. Under the DNO mechanism, the PSP that owns the line identifies numbers reserved exclusively for inbound calls. This is the case, for example, with certain numbers set aside to receive requests to block lost or stolen cards. Any call made from this type of number is therefore presumed to be fraudulent, and will be automatically cut off thanks to DNO before the fraudster can even begin a conversation with the intended victim. In addition to the MAN programme, whose effectiveness relies on telecommunications operators rigorously applying their verification process, the DNO thereby strengthens the fight against spoofing for the most sensitive and high-risk numbers.

The Observatory works to prevent fraudulent SMSs and mitigate the risks of phishing by promoting the use of Originator Address Codes (OAdCs) when PSPs contact customers by SMS. An OAdC – also known as a Sender ID, sender field or sender identifier – is the alphanumeric label that identifies the sender of an SMS instead of a 5-digit short number ("ABC Bank" rather than "38123", for example). PSPs now contribute codes to the lists of protected OAdCs drawn up by the AF2M. At the same time, PSPs are gradually exploiting the flow of reports to the 33700 telephone number, which corresponds to the platform that receives SMSs flagged as potentially fraudulent by their recipients. AF2M forwards to the relevant PSPs any SMSs reported to 33700 that mention their name. If the SMS is fraudulent, the PSP can have the website usurping its identity and whose link is contained in the SMS blocked.

These measures help to strengthen the security of the SMS communication channel, which is still used by many PSPs. Ultimately, replacing SMSs with the Rich Communication Services (RCS)[4] protocol, which is set to become the default messaging service on mobile phones, will provide greater security for users as it incorporates an upstream sender verification mechanism for messages sent by businesses or public authorities.

Several PSPs have also implemented measures to prevent SIM swapping. This type of fraud involves diverting a user's mobile phone line so that the fraudster receives one-time confirmation codes instead of the user. PSPs try to prevent this type of fraud by using the SIM Verify application programming interface (API) proposed by AF2M. This tool makes it possible to determine whether a new SIM card has recently been issued (which may correspond to legitimate use, but also to a case of SIM swapping). The PSP combines this information with other factors (such as whether the transaction is unusual given the payment service user's normal behaviour) to assess the level of risk of the transaction and refuse it if the risk appears too great.

Certain banking applications take a similar approach to detect whether the user, at payment initiation or confirmation, is communicating by telephone with a third party (a scenario which may notably suggest social engineering fraud). This detection relies on the exploitation of a telephone's metadata, and more specifically the call-in-progress indicator.[5] PSPs are now working with AF2M to identify areas for improvement of the SIM Verify API and to explore the possibility of making greater use of telephone and telephone line metadata.

Lastly, under the aegis of the *Fédération bancaire française* (FBF – French Banking Federation), the major banking groups along with the professional organisations in the telecommunications sector have been studying the feasibility of an "anti-fraud" short number, drawing inspiration from the 159 telephone number available in the United Kingdom, which is shared by the main British banking institutions. In the event of a suspicious call or a risk of fraud, any member of the public would be able to call a short number (to be determined) to be quickly put through to their bank's anti-fraud service.

2 The MAN programme enables the authentication of a number used to make a call, in accordance with Article L. 44 of the *Code des postes et des communications électroniques* (the French postal and electronic communications code) and its version in force since July 2023, and thereby helps to prevent fraudsters from usurping telephone numbers belonging to third parties (PSPs, public authorities, etc.).

3 Article L. 44 of the *Code des postes et des communications électroniques* (the French postal and electronic communications code).

4 RCS is a messaging protocol that offers enhanced functionality compared to SMS and MMS. An RCS messaging app will be pre-installed on the two main platforms (iOS and Android). Unlike proprietary messaging services such as WhatsApp or iMessage, RCS is standardised and interoperable.

5 The use of metadata for the purposes of combating fraud prompted a statement from the *Commission nationale de l'informatique et des libertés* (CNIL – French Data Protection Agency), published on 15 July 2025, setting out the rules to be followed to protect individuals' rights: *https://www.cnil.fr/fr/controle-appel-en-cours-utilisation-dune-application-bancaire-reglementation*

2.1.3.3 Developing cooperation with digital platforms

Although fraudsters continue to use the telephone, the new channels offered by digital platforms, such as instant messaging and social media, are now a preferred point of entry for both social engineering fraud and financial scams in general. These platforms offer a low-cost, global attack surface that facilitate information gathering on victims (identity, habits, location, relationships, etc.) and thereby enable scammers to personalise their messages to appear credible and legitimate and make their manipulation particularly effective. It was against this backdrop that in 2025 the Observatory undertook to launch, organise and facilitate cooperation between the major digital sector players and the payments ecosystem to combat banking scams, and in particular social engineering fraud. The Observatory first drew up a roadmap structured around four key areas *(see* the roadmap for digital sector player *below)*, then identified three priority digital sector players: Google, Meta and TikTok. The first working meetings with these various players were organised by the Observatory and took place during the first half of 2026.

The meetings confirmed that it was essential to step up cooperation with the French payments and telecommunications ecosystem. This cooperation begins with a better understanding of the security strategies deployed by digital sector players to combat illegal and fraudulent content given the needs expressed by fraud experts within the payments ecosystem. Three pillars are taking shape from their anti-fraud efforts and initiatives.

First, the digital sector players that met with the Observatory commit to (i) further improving the security of their products and services, and (ii) continuing to reinforce guidance and raise awareness amongst their users on the fraud techniques that could be used to target them (Pillar No. 1). This could involve introducing authentication procedures, warning messages or advertiser verification schemes. In terms of advertising, digital sector players must pay greater attention to the legitimacy of advertisers and step up their efforts to prevent fraudulent content and online scams. For example, in the specific case of advertisements for financial products and services, they must seek to verify their advertisers' authorisation directly against the official registers maintained by regulators.[6] Nonetheless, the effectiveness of the measures already employed by digital sector players must be checked and can certainly be improved further.

Second, the digital sector players also commit to reinforcing their existing mechanisms designed to detect and close fraudulent accounts and content in real time (Pillar No. 2). To do so, they rely heavily on artificial intelligence (AI) models, which analyse abnormal behaviour (mass creation of accounts, identical messages, etc.), identify social engineering scenarios (fake investments, identity theft of company directors or public officials) or detect malicious links or misleading content on a large scale and in real time. Thanks to these advanced AI tools, platforms were able to block or remove around ten billion malicious advertisements in 2025 and to suspend tens of millions of accounts worldwide. In addition to this upstream screening, the digital sector players claim to process, at a later stage, cases flagged to them by users and, as a priority, by public authorities. However, the question of whether they comply with the European regulatory framework remains open and must be monitored closely.

Several participants in the Observatory's work have stated that the prior verification of advertisers is particularly worthwhile to prevent the dissemination of fraudulent advertising. Upstream checks could be likened to a Know-Your-Business (KYB) process for clients placing advertisements on internet platforms. This verification ensures that the advertisers actually exist and, in the case of promotional material for financial services (such as investment proposals), that they are authorised to operate in the country in which the advertisement is placed. The digital sector players stress, however, that the effectiveness of these types of verification could be enhanced if official registers (company registers maintained at national and European level, registers of entities authorised to operate in the financial sector, etc.) were to evolve in terms of their format and content.

Third, the digital sector players are convinced that combating cybercrime requires cooperation between all public and private stakeholders, and information exchange between them (Pillar No. 3). They are therefore particularly open to supporting the integration of French PSPs into their existing information-sharing programmes: the Priority Flagger Program[7] for Google, the Fraud Intelligence Reciprocal Exchange (FIRE) programme for Meta, or the Global Signal Exchange,[8] launched and supported by an alliance of major digital sector players, including Google and Meta. These programmes, which certain French banks already participate in, aim to share with digital sector players any information gathered and risk alerts generated in relation to fraud. However, the programmes in their current state suffer from certain limitations as they are more reactive than proactive.

Involving financial institutions and telecommunications sector players in information-sharing programmes would

help to further enhance the fraud prevention and detection tools available to digital sector players. Equally, these programmes must enable PSPs to more quickly access information on the dissemination of fraudulent content on the internet, messaging apps or social media. To this end, on 16 March 2026, numerous digital sector players signed the "Industry accord against online scams and fraud", a voluntary global anti-fraud agreement at the UN Global Fraud Summit held in Vienna, Austria. The accord aims to organise a collective, transversal and structured response to online fraud worldwide, and should help to speed up the sharing of fraud signals and improve the tracking of multi-channel criminal networks.

The Observatory recognises the commitments made by digital sector players, such as Google, Meta and TikTok, as well as their willingness to step up their operational cooperation with the French payments ecosystem to detect and prevent fraud. At the same time, the Observatory invites French payment industry players to explore existing cooperation programmes. This cooperative approach, initiated at national level, is set to continue and deepen in the coming months and years. It may subsequently be extended to the European level, particularly in view of the entry into force of the European Payment Services Regulation (PSR), which should facilitate such cooperation.

6 Furthermore, this verification is expected to be required under the forthcoming European Payment Services Regulation (PSR), which is scheduled for publication in the Official Journal of the European Union by the end of 2026.

7 A priority reporting programme that gives selected specialist organisations a dedicated channel to report policy-violating content for certain products and services or potentially fraudulent content to Google.

8 A global, multi-stakeholder and cross-sector exchange platform for the sharing of abuse signals, launched in October 2024 by the Global Anti-Scam Alliance (GASA). Its aim is to gain a better understanding of how scams operate and to identify those responsible.

9 Signatories include Google, Meta, Microsoft, Amazon, LinkedIn, OpenAI, Pinterest and Match Group.

RECOMMENDATIONS INTENDED TO STRENGTHEN THE SECURITY OF TELECOMMUNICATIONS CHANNELS *(RECOMMENDATIONS ORIGINALLY SET OUT IN THE 2024 ANNUAL REPORT)*

Recommendation No. 1:

In order to combat social engineering fraud, payment service providers (PSPs) are encouraged to explore the different ways of making their communications with customers more secure, drawing on best practice in the market, for example:

- Identifying and regulating channels of communication with customers so as to reduce, or even eliminate, exchanges via SMS or email, by favouring as much as possible the mobile application, which is thought to be more secure, including for telephone conversations.
- Sending a notification on the mobile application when a legitimate call from the organisation is in progress to endorse the call. Without this notification, the customer should automatically suspect that the caller is perpetrating a fraud.
- Using mobile phone metadata to detect if a call is taking place at the same time as sensitive transactions are being carried out on the mobile application in order to flag potential social engineering fraud. On 15 July 2025, the *Commission nationale de l'informatique et des libertés* (CNIL – French Data Protection Agency) published articles on its website setting out the conditions under which banks can check for a call in progress while a banking application is in use.
- Strengthening the security of certain authentication procedures, particularly when registering a new telephone number (for example, by using the Global System for Mobile Communications' Number Verify standard) or when installing an application on a new device (for example, by supplementing strong authentication with a short video capture).

Recommendation No. 2:

PSPs are invited to provide telephone operators with numbers intended solely for inbound calls so that a protection mechanism for these numbers can be put into operation by 2026 as they are particularly exposed to spoofing.

Recommendation No. 3:

The Observatory urges PSPs and telecommunications sector players to explore the feasibility of introducing a single helpline number for contacting a bank's anti-fraud services. In the event of a suspicious call, consumers would be advised to hang up and ring this helpline number to verify the legitimacy of the call.

Recommendation No. 4:

Payment industry professionals, as well as large companies and public authorities, which are regularly targeted in phishing campaigns, are invited to work with the AF2M to (i) protect the fields used in their SMSs (sensitive OAdCs), (ii) contribute to the blacklist (strictly prohibited OAdCs), and (iii) subscribe to the information feed provided by the 33700 platform in order to identify new risks of identity theft in flagged messages and take the necessary action to eliminate them, such as cutting off the URLs contained in the messages that have been reported.

Recommendation No. 5:

PSPs that use SMS-OTP (one time password) as an authentication factor are encouraged to consider integrating the multi-operator SIM Verify application programming interface (API) into their real-time fraud prevention processes, as well as any other tool that would enable the detection of a recent request to port a number to a new operator.

ROADMAP INTENDED TO STRENGTHEN THE ACTIONS OF DIGITAL SECTOR PLAYERS AND THEIR COOPERATION WITH THE FRENCH PAYMENTS ECOSYSTEM *(GUIDELINES ORIGINALLY SET OUT IN THE 2024 ANNUAL REPORT)*

Priority No. 1:

Information sharing between digital sector players and payment service providers

Much like the Fraud Intelligence Reciprocal Exchange (FIRE) programme in the United Kingdom between the banking sector and Meta, the aim is to organise an effective channel for sharing information on fraudsters' activities. This could notably enable French PSPs to flag (including through the mechanism set out in Article 16 of European Regulation (EU) 2022/2065 on digital services, known as the DSA, or Digital Services Act) to digital sector players any scams that have taken root on one of their platforms (Facebook, Instagram, WhatsApp, TikTok, etc.), so that they can close the accounts used by fraudsters or remove any fraudulent content brought to their attention, which they can judge to be unlawful "without detailed legal analysis", under penalty of being held liable.

Furthermore, for very large online platforms as designated by the European Commission, all the information likely to be reported to them, particularly by PSPs, could help them to better identify systemic risks associated with the dissemination of fraudulent content online, monitor suspicious activities more effectively, and adapt the mitigation measures needed in response, accordingly.

Priority No. 2:

Information sharing on the reporting of suspicious numbers

There are numerous proprietary reporting mechanisms put in place by digital sector players, whether they be messaging tools, operating systems or mobile phone manufacturers. These coexist alongside the 33700 platform set up by AF2M, but not all of these players share information with one another.

Priority No. 3:

Combating identity theft in digital uses

Fraudsters often encourage their victims to switch their communications to proprietary messaging apps such as WhatsApp, Signal or Telegram that are considered to be more secure. However, in the absence of identity verification and know-your-customer procedures as thorough as those in the financial sector, fraudsters can easily pose as PSPs on these digital applications, by using a bank's logo as a profile picture for example, or as merchants, by using online advertising linked to mirror sites. Furthermore, authentication procedures for digital sector players are often still based solely on a username and password combination. As an example, this allows fraudsters to easily gain access to messaging tools, intercept sensitive data or carry out transfer fraud by informing genuine contacts of a change in bank details.

Priority No. 4:

Combating fraudulent advertising

In particular, the possibility for digital sector players to strengthen know-your-customer procedures for advertisers conducting sales from their platforms will be explored so that they can verify that links lead to legitimate websites without the identity of a third-party retailer having been usurped. In this regard, platforms may be asked to remove any links or references to websites identified on the blacklists of the *Autorité de contrôle prudentiel et de résolution* (ACPR – Prudential Supervision and Resolution Authority) and the *Autorité des marchés financiers* (AMF – the French Financial Markets Authority), their European equivalents, or other blacklists drawn up by public authorities.

2.2 Prevention of fraud on remote card payments

2.2.1 Background to our recommendations

The different types of remote card payments are not equally vulnerable to fraud, which led the Observatory to adopt a set of recommendations in June 2024 for the most exposed remote payment processes: payments that do not use the 3-D Secure authentication protocol. The Observatory's plan to improve security covers (i) non-3-D Secure payments over the internet and (ii) MOTO (mail order, telephone order) remote payments, whereby payment card details are provided by telephone or in writing.

The plan notably involves the implementation of a velocity limit, calculated as the cumulative amount of purchases made with the same card from the same merchant over a rolling 24-hour period.[10] Beyond this limit, transactions that do not comply with the Observatory's recommendations must be declined by the issuers.

The implementation of this plan to improve the security of remote card payments is overseen by an ad hoc Observatory steering committee made up of payment service providers, technical acceptance service providers and retailer representatives, under the aegis of the Banque de France. The plan is regularly updated based on the decisions taken by the steering committee following discussions with its members, and published in French and English on the Observatory's website. Table 2 provides an overview of the recommendations, along with an indication of their progress.

This plan relies on the coordinated implementation of measures by all issuing PSPs established in France, and on merchants' involvement in their deployment. The main French issuing PSPs apply the plan correctly. However, the Observatory once again urges independent issuers and subsidiaries of large groups to ensure that the recommendations set out in this security plan are properly implemented.

2.2.2 Action plan

Since 2025, the steering committee's work on the implementation of the security plan has been structured around two focus areas.

Focus 1: MOTO payments

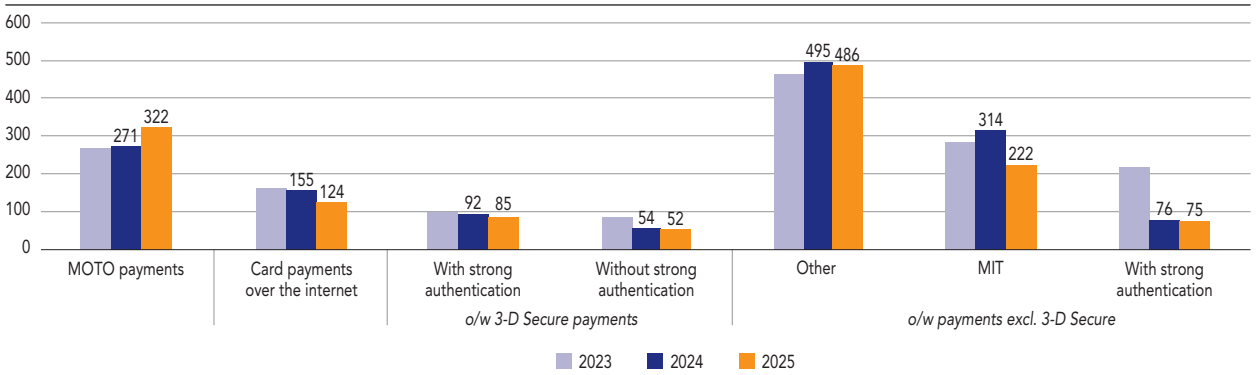
With the exception of certain duly identified business sectors, the velocity limit has been set at EUR 500 since June 2024. The Observatory has asked the steering committee to gradually phase out these sectoral exemptions so as to achieve a uniform velocity limit of EUR 500 across all sectors by the end of 2026. At the same time, the Observatory recommends the use of secure procedures for the transmission of card numbers over the telephone (direct entry on the keypad or an interactive voice response system). Furthermore, it supports the development of a telephone-order (TO) payment authentication solution. The card payment networks defined the specifications at the start of 2026 and this new authentication solution will begin to be rolled out as from the second half of 2026. In practical terms, strong payment authentication – generally on a mobile banking application – may be required for any payment where the card number is communicated by telephone.

Focus 2: Non-3-D Secure card payments over the internet

The velocity limit for payments where the acquiring PSP is located within the European Economic Area (EEA) has been set at EUR 0.01 since January 2026. The Observatory now recommends applying velocity limits to international card payments. The timeframe for implementation varies depending on the part of the world concerned to take account of each region's level of 3-D-Secure maturity.

A third focus area for the steering committee's action plan is also taking shape, involving the Observatory monitoring, in the coming months and years, the strengthening of the security of MIT (merchant-initiated transaction) card payments. This action aligns with Recommendation No. 2 *bis* of the security plan. The aim is to increase the transparency of information relating to direct debit mandates in 3-D Secure authentication windows, when the consumer authorises a card-based direct debit mandate. This focus area also aims to offer consumers the tools to view and manage the various mandates they have signed on their online banking solutions. Card industry stakeholders have already launched initiatives to consider the matter, and they will be monitored by the steering committee.

Fraud on payment cards issued by French PSPs (in EUR defrauded per EUR 100,000 of payments)



Source: Observatory for the Security of Payment Means.
Note: MIT, merchant-initiated transaction; MOTO, mail order, telephone order.

2.2.3 Effects of the Observatory's plan

The fraud statistics for 2025 confirm that remote card payments remain far more vulnerable to fraud than point-of-sale payments: while remote payments account for only 28% of the total value of card transactions, they account for 78% of the total value of fraud. The most exposed channels are still (i) MOTO payments, (ii) payments over the internet that do not use the 3-D Secure strong authentication, and (iii) MITs. The fraud rate for these three categories of payment is three to five times higher than for other remote card payments. The Observatory's involvement in improving the security of remote card payments therefore continues to be essential.

That said, the positive results of the Observatory's security plan can already be seen in 2025's fraud statistics.

"MOTO" payments

First, MOTO (mail order, telephone order) transactions – card payments by post or telephone – are declining in both volume and value (down 12% in volume year-on-year compared with 1% between 2023 and 2024, and down 21% in value compared with 6% between 2023 and 2024). This decline is likely the result of greater use of alternative payment solutions, such as card payments over the internet or bank transfers, or even point-of-sale payments, in line with the Observatory's recommendations.

Second, the value of fraud involving MOTO transactions fell by 7% to EUR 37.7 million in 2025 (compared with EUR 40.4 million in 2024) but as this decrease is less pronounced than the decline in transaction values, it mechanically resulted in an increase in the fraud rate. Nevertheless, pursuing the implementation of the security plan should ultimately lead to a reduction in the fraud rate.

A closer examination of the data shows that fraud is falling more rapidly for domestic MOTO transactions (down 13% in value between 2024 and 2025) than for European and international MOTO payments. Consequently, the steering committee may consider rounding out the action plan in the future with measures to improve the security of international MOTO transactions.

Non-3-D Secure payments over the internet

The fraud rate for card payments over the internet, as well as across all associated initiation channels, fell by 20% between 2024 and 2025 from 0.155% to 0.124%. This decrease is the result of a decline in (i) the fraud rate for MIT payments (down 21%), (ii) the fraud rate for 3-D Secure payments with strong authentication (down 9%) and (iii) the proportion of non-3-D Secure payments (i.e. unauthenticated payments excluding MIT payments), which was down by 22%.

Meanwhile, MIT-type payments were on the rise (up 12% in volume and 14% in value terms), while at the same time the associated fraud fell sharply (down 17% in volume and 21% in value terms). The fraud rate therefore dropped mechanically by 21%. Measures to ensure MIT payment security are not yet widespread. However, work carried out under the aegis of the Observatory with a number of merchants identified as priority cases due to high fraud rates on their MIT transactions has started to show results. Nevertheless, the proportion of fraud on these payments remains high and could be due to commercial disputes. For example, consumers may dispute having taken out a subscription and report the transactions as fraudulent to their PSP. However, as a general rule, the PSP reimburses

10 Velocity = cumulative amount of purchases/card/merchant/24 hours.

the customer after submitting a chargeback request to the merchant concerned. Under the current framework, chargeback mechanisms do not allow for the satisfactory identification of unfair disputes.

2.2.4 Current state of the implementation of recommendations and outlook for 2027

MOTO payments

First, discussions are ongoing with the ten or so priority merchants (Recommendation No. 3 *bis*) that operate in exempt sectors but whose exposure to fraud is regularly higher than the financial centre average. Each priority merchant has been asked to provide an action plan aimed at (i) reducing their MOTO transactions as much as possible in favour of more secure channels, and (ii) improving the security of the MOTO transactions that remain. Once approved, each action plan is monitored by the Observatory through to completion.

Second, with the exception of a restricted list of business sectors, the velocity limit was lowered to EUR 500 from June 2024. This EUR 500 limit will apply to all sectors by the end of 2026.[11] Only the catalogue sales sector (MCC[12] 5965) for purchases made by post (ERT[13] code 22 under the *Groupement des Cartes Bancaires* classification) will remain exempt. The lack of an authentication solution for card payments initiated on paper makes the exemption unavoidable. Payments initiated by telephone (telephone order, TO) but that have been authenticated using the 3-D Secure protocol will also be exempt from this velocity limit.

Consequently, the Observatory strongly urges all stakeholders (card issuers, acquirers, payment acceptance service providers and, of course, merchants) to participate in the deployment of the telephone payment authentication solution in order to ensure that it is rolled out and functions smoothly from the second half of 2026 onwards *(see Recommendation No. 5)*. The specifications have already been defined by the *Groupement des Cartes Bancaires* CB network and are compatible with the Visa and Mastercard networks. Merchants accepting payments by telephone, particularly those for whom transactions may exceed EUR 500, should consult their banking and payment service providers to find out the timelines involved for implementing this solution. They will then be able to plan in advance for the developments needed.

The successful deployment of the telephone payment authentication solution is a strategic priority for the Observatory in 2026 and 2027. The solution could make France a pioneer in ensuring the security of these transactions, which as yet have not benefited from the positive effects of strong authentication. In the future, once this solution has been adequately deployed and has proven its effectiveness in preventing fraud and also accessibility for users, the steering committee will work towards gradually lowering the velocity limit to below EUR 500 for non-3-D Secure MOTO transactions.

Non-3-D Secure payments over the internet

First, as with MOTO payments, the steering committee has continued to monitor merchants identified as priority cases for MIT payments (Recommendation No. 3 *ter*). Monitoring of their action plan will continue in 2026 and 2027.

At the same time, the velocity limit for non-3-D Secure card payments has been gradually reduced in successive steps to EUR 0.01 since January 2026 (Recommendation No. 3). The Observatory's plan did not initially cover international payments to merchants and acquiring PSPs located outside the European Economic Area (EEA), but the velocity limit has now been extended to merchants and acquirers located in:

- non-EEA European countries (such as the United Kingdom or Switzerland), and countries in the Pacific franc monetary zone, where the 3-D Secure protocol is well established in payments ecosystems, with a limit of EUR 1.01 from March 2026;
- a zone covering Africa and the Middle East, where a velocity limit of EUR 100 has been in place since July 2026;
- a zone covering Asia, North and South America, Oceania and the Pacific, where a velocity limit of EUR 500 has been in place since September 2026.

Each country has been assigned to a geographical zone and associated with a deployment timetable set out in the Observatory's plan published on its website *(see Recommendation No. 3* quater *and Appendix 5*).

Lastly, issuing PSPs have noted a substantial improvement in the level of compliance amongst MITs, which are increasingly providing valid chaining references. Nevertheless, some merchants still report problems with general performance or with the coverage of complex use cases.

Furthermore, by the end of 2026, all major French banking groups will enable merchants to display enhanced information on a recurring payment in the 3-D Secure window (frequency, end date, amount per instalment, subscription cost in the event of a trial period, etc.). The greater transparency with regard to the characteristics of MIT mandates will help inform consumer validation. Banks have also launched a review to explore ways to provide

tools within their online banking interfaces for viewing and managing subscriptions paid for by card.

Therefore, in 2027, the Observatory will focus on: (i) enhancing the transparency of MIT mandates within 3-D-Secure authentication windows with better information for the customer on the terms and consequences of the mandate; (ii) monitoring the deployment of tools for managing these mandates from online banking interfaces; and lastly (iii) working alongside the French market in the implementation of these new tools. When combined with the terminal identification tools used by consumers, these features should enable issuing PSPs to better distinguish fraud from commercial disputes, both when processing claims and in regulatory reporting. They should thus help to reduce the fraud rates reported on MIT transactions.

2.3 Monitoring of the Observatory's other actions and recommendations

This section is available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/fr/publications-etstatistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyensde-paiement-2025

11 The procedure allowing individual exemptions remains in force. Certain merchants may therefore accept MOTO payments without a velocity limit, provided they have satisfactorily demonstrated that their payment flows are secure (see Appendix 3 of the security plan).

12 MCC – Merchant Category Code.

13 ERT – *environnement règlementaire et technique* (regulatory and technical environment).

T2 Summary of the implementation of the Observatory's recommendation on remote card payments excluding 3-D Secure

Recommendations	Level of implementation
Recommendation No. 1: Restricting MOTO and MIT payments to cases where no other payment method is possible	MOTO payments issued by French PSPs were down in 2025 by 12% and 21% in volume and value terms, respectively. MIT payments were up by 14% and 12% in volume and value terms, respectively, which is consistent with changes in digital uses.
Recommendation No. 2: Valid chaining for MITs	A substantial improvement in the level of compliance from MITs providing valid chaining references.
Recommendation No. 2 *bis*: Security of MITs	Discussions under way on the tools to be implemented to address the recommendation.
Recommendation No. 3: Velocity limits and implementation of a soft decline mechanism	Velocity limit set at EUR 500 for MOTO payments (with sectoral exemptions to be gradually phased out by the end of 2026) and at EUR 0.01 for non-3-D-Secure payments over the internet.
Recommendation No. 3 *bis*: Specific measures applicable to merchants identified as priority cases for reducing fraud in MOTO payments	Monitoring the action plans submitted by merchants through to their completion.
Recommendation No. 3 *ter*: Specific measures applicable to merchants identified as priority cases for reducing fraud in MIT payments	Monitoring the action plans submitted by merchants through to their completion.
Recommendation No. 3 *quater* on one-leg transactions: Velocity limit for non-3-D Secure internet payments with an acquiring PSP established outside the European economic area (EEA)	The reduction in limits is underway and will continue until the end of 2026.
Recommendation No. 4: Securing payment data for MOTO payments	Regular reminders to all the players in the ecosystem. The implementation of this recommendation is also monitored when individual applications for exemptions from velocity limits are being assessed.
Recommendation No. 5: Trialling MOTO payment authentication	Widespread implementation is planned from the second half of 2026.

Source: Observatory for the Security of Payment Means.
Note: MOTO, mail order, telephone order; MIT, merchant-initiated transactions; PSP, payment service provider.

3

SECURITY OF PAYMENTS USING CRYPTO-ASSETS

3.1 Introduction

The emergence of new technologies, such as distributed ledger technology[1] (DLT), has led to the development of new types of financial assets. These include "crypto-assets", which can be exchanged between economic players and serve as a means of settling[2] retail and financial transactions without, in principle, resorting to cash or cashless means of payment or traditional market infrastructures. These crypto-assets form the cornerstone of decentralised finance (DeFi), which aims to dispense with traditional centralised finance and payment channels. This decentralisation means that transaction monitoring, decisions and validations are carried out by a network of participants, according to mechanisms defined by the underlying network, without a single central authority.

A crypto-asset is defined as a digital representation of value or rights that is able to be transferred and stored electronically using DLTs, such as blockchain, or similar technology. Their issuance and distribution are governed in the European Union by the MiCA Regulation.[3] For the purposes of this study, we consider two types of assets:

- "first-generation" crypto-assets, such as Bitcoin and Ether, which are not pegged to a reserve of assets and whose value is highly volatile – linked to supply meeting demand – compared with legal tender currencies;
- "second-generation" crypto-assets, or "stablecoins", which were created in an attempt to overcome this volatility and are often pegged to a traditional financial asset such as a currency, commodity or security, or basket of assets (a stock market index, for example). When designed for use as a settlement asset, they are generally pegged at a 1:1 ratio to a legal tender currency. In accordance with the MiCA Regulation and the clarifications provided by the European Banking Authority (EBA), they therefore qualify as "electronic money tokens" (EMT)[4] and are classified as electronic money units for regulatory purposes (in particular, the second European Payment Services Directive – PSD2 – and the second Electronic Money Directive – EMD2).[6]

3.1.1 From an infrastructure perspective

From an operating perspective, crypto-asset transactions are recorded in a blockchain[7] and distributed via a decentralised and generally public network, whose purpose is to group, secure and timestamp those transactions cryptographically to guarantee their traceability and integrity. Taken individually, certain aspects of these technologies resemble those used to secure traditional payments. However, when combined with blockchain technology, they can operate in a fully decentralised manner without a trusted third party to maintain a reference account. In fact, every participant, or "node", in the blockchain has an identical copy of the ledger of transactions, making attempts at falsification more complex.

3.1.2 From a players' perspective

In practice, direct access to the blockchain requires information technology (IT) skills and resources that are generally beyond the reach of traditional retail payment users (merchants or consumers). As a result, the implementation of retail payment solutions using crypto-assets requires specialised intermediaries, which then delegate the execution of crypto-asset unit exchanges through the blockchain.

1 A "distributed ledger" is an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism (Article 3 of the European Markets in Crypto-Asset Regulation – MiCAR).

2 The use of crypto-assets for settlement purposes in the purchase of other crypto-assets (including unique and non-fungible crypto-assets or real-world assets represented in the form of tokens) is excluded from the scope of the study.

3 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

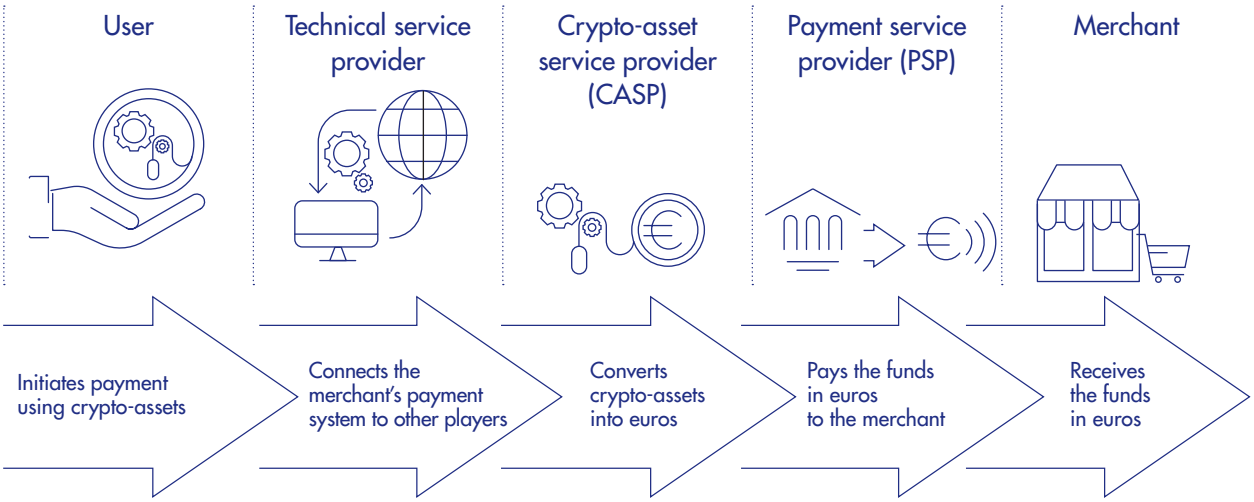
4 EMT: "e-money token" issued by an electronic money institution (EMI) or credit institution (CI).

5 Article L. 315-1 of the French Monetary and Financial Code (CMF I. and II): "Electronic money is a monetary value stored in electronic form, including magnetic form [...] and electronic money units are said to be units of value."

6 European Directive (EU) 2015/2366 on payment services (PSD2) and Directive 2009/110/EC on electronic money (EMD2).

7 For further information, see: *"La blockchain"*, Banque de France, ABC de l'Économie, *L'Éco en Bref*.

D1 OVERVIEW OF THE PLAYERS INVOLVED IN PAYMENTS USING CRYPTO-ASSETS



Source: Observatory for the Security of Payment Means.

Throughout the crypto-asset payment journey, various players intervene to facilitate the payment, from the end user to the merchant that accepts them as a method of payment. Thus, in order to bring together the various payment using crypto-assets stakeholders, players such as crypto-asset issuers, exchange platforms[8] and banking institutions, which are notably in charge of transferring the transaction amount in euro to the merchant, can be involved.

3.1.3 Bridges with the "traditional" payment sector exist

In almost all cases, merchants prefer to receive payment in legal tender currency, i.e. euro, which requires the crypto-assets used by the payer to be converted before the proceeds of the conversion are passed on to the merchant. Various conversion options are available, depending on the type of payment using crypto-assets – QR codes,[9] payment cards or crypto-asset wallets – and each involves a mix of crypto-asset services and traditional payment services.

3.1.4 The objectives of this study

This study falls within the remit of the *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) as it focuses on an analysis of the security of retail payments using crypto-assets in France.

This study is intended to provide an overview of payment using crypto-assets solutions in France following the entry into force of the European MiCA Regulation (MiCAR), to identify the security issues specific to payment using crypto-assets, and given this context, to present the recommendations the OSMP considers appropriate.

Other risks[10] associated with crypto-asset holdings or use (market, credit, liquidity or money-laundering risks) are therefore not discussed as part of this study. However, any players intending to hold or trade crypto-assets, or more broadly, offer crypto-asset-related services, should take them into consideration. Similarly, neither the strictly legal aspects of payment using crypto-assets,[11] nor the tax implications involved, will be addressed in this study.

3.2 A typology of payments using crypto-assets

Technically, first-generation crypto-assets such as Bitcoin can be used to make payments but in practice, their value volatility and the fees and delays associated with each transaction mean that they are unsuitable for everyday payments. Consequently, the following analysis primarily concentrates on stablecoin payments and their use cases, while also marginally touching on certain use cases for first-generation payments using crypto-assets. Since merchants prefer in practice to be paid in euro, using stablecoins notably means that the exchange risk and volatility associated with other crypto-assets when converting to a legal tender currency are more limited.

It is important to note from the outset that **crypto-assets are currently very rarely used in retail payments in France**. In fact, less than 3% of French people[12] surveyed in 2023 claimed to have already used crypto-assets for payment purposes. Moreover, the number of referenced retail businesses directly accepting payments using crypto-assets in France in 2025 was very low. For example, approximately 300 out of a total of 300,000 points of sale – 0.1% – accept Bitcoin.

Furthermore, crypto-assets, including stablecoins, are used to buy and sell other crypto-assets, but in practice are only marginally used to purchase traditional goods and services. Nevertheless, leaving aside retail payments made in France, the use of stablecoins, particularly those regulated under MiCAR, is growing, mainly for transactions on financial markets, for cross-border payments between professionals and for cash management, including at group level.

3.2.1 Point-of-sale payments

From a practical perspective, instruments similar to those available for traditional payments are used for point-of-sale payments using crypto-assets. **Payment initiation** is made either via a merchant's electronic payment terminal, which generates a QR code containing the transaction information, or via a customer's payment card, be it the card itself or integrated into their mobile phone. Whatever the case, the crypto-asset **payment acceptance** solution can be integrated into the cash register system or provided on a device such as a tablet or phone, used as a mobile payment solution (SoftPos – Software point of sale).

In the case of a point-of-sale payment with a QR code, customers first scan the QR code generated by the merchant's payment terminal. Depending on the options offered by the merchant, customers then choose (i) their exchange platform, (ii) their crypto-asset wallet (if they have several), and (iii) the crypto-asset they wish to use for payment. In the next step, the payer validates the transaction with the exchange platform or EMT issuer, which then transmits it to the blockchain network. Lastly, the transaction is confirmed and the sale is finalised. This is followed by a conversion phase, which has no impact on the customer's payment journey, during which the payment passes through a payment gateway, in charge of establishing the link between crypto-assets and traditional banking channels (such as SEPA). The exchange platform, or EMT issuer, converts the crypto-assets into a legal tender currency (euro), and the amount is then paid in euro to the merchant through a payment service provider.

In the case of a point-of-sale payment with a payment card, the payment is made by placing a physical or virtual card in contact with a payment terminal. Most cards are preloaded with crypto-assets or are connected to a crypto-asset wallet. Several options for the crypto-asset to be used for payment are available. In principle, the user sets a default choice for future transactions but that choice may automatically switch to another crypto-asset when the balance of the default asset does not cover the entire payment. The conversion into a legal tender currency then takes place via payment gateways on an exchange platform or another crypto-asset service provider (CASP), in the same way as payments with a QR code. Lastly, the transaction is carried out through traditional card payment networks until the merchant receives the funds through the intermediary of their payment service provider (PSP).

For both types of crypto-asset point-of-sale payment solutions, an internet connection is most often required to validate the transaction. However, it is sometimes possible to pay offline – without a direct internet connection – depending on the chosen payment method[13] through the use of NFC[14] technologies or QR codes.

3.2.2 Remote payment transactions

Remote payment transactions using crypto-assets can be made as an e commerce payment through a traditional payment method (such as a card, bank transfer, or from an electronic money account), either directly from the merchant's website or from a payment link generated by the merchant. The option to pay using crypto-assets becomes available alongside other possible options when prompted to choose the payment method. The payment

8 These exchange platforms convert the crypto-assets held in a user's crypto-asset wallet.

9 Quick Response (QR) code payment is a digital payment solution whereby payers scan a two-dimensional code with their smartphones to initiate a transaction.

10 "*Crypto-actifs: l'AMF appuie l'appel à la prudence lancée par l'ESMA à destination des investisseurs individuels*", AMF (18 December 2024). It is important to bear in mind that crypto-assets are very risky because they generally offer little protection and are generally less regulated than most other types of assets, with some players sometimes unregulated.

11 *Rapport sur l'évolution de la notion juridique de monnaie*, Haut Comité Juridique de Place (HCJP), June 2025.

12 "*Quel avenir pour le monde des crypto-actifs?*", Banque de France, 17 October 2024.

13 Self-custody wallet, hard wallet or specific payment cards.

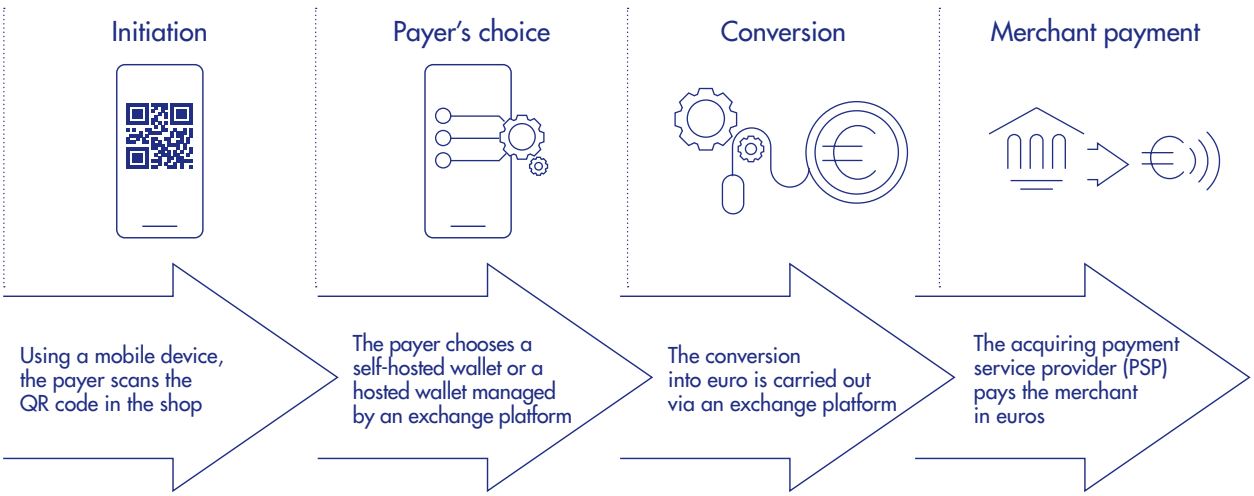
14 Near Field Communication technology enables very short-range data payload sharing between compatible devices.

then proceeds as described above, with the choice of asset in the electronic wallet, the completion of the transaction, and then the conversion to pay the merchant in a legal tender currency.

3.2.3 Wallet-to-wallet payments

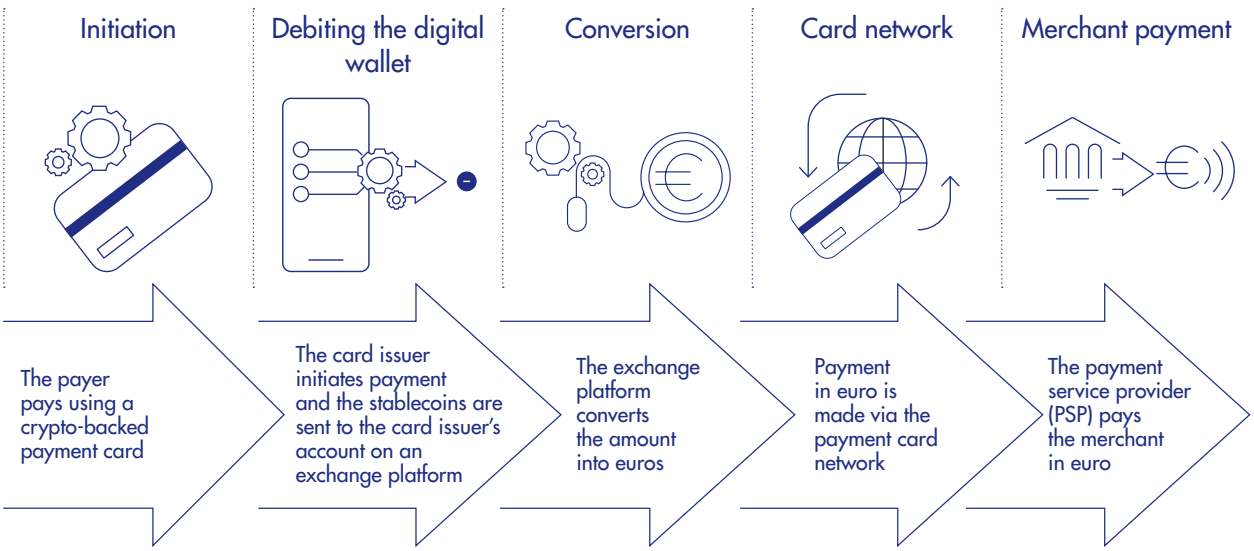
There is an alternative – albeit very rarely used – payment method in which both the user and the merchant have a crypto-asset wallet. In this scenario, payment is made directly from one wallet to another, using crypto-assets without conversion into legal tender currency. It can be applied in both remote and point-of-sale payments but is virtually non-existent in France. The risks to the user in the case of a payment made directly from wallet to wallet are heightened when the wallets are self-hosted (non-custodial wallets),[15] or a payment is made using non-EMT crypto-assets.

D2 POINT-OF-SALE PAYMENT FLOWS USING A QR CODE



Source: Observatory for the Security of Payment Means.

D3 POINT-OF-SALE PAYMENT FLOWS USING A PAYMENT CARD



Source: Observatory for the Security of Payment Means.

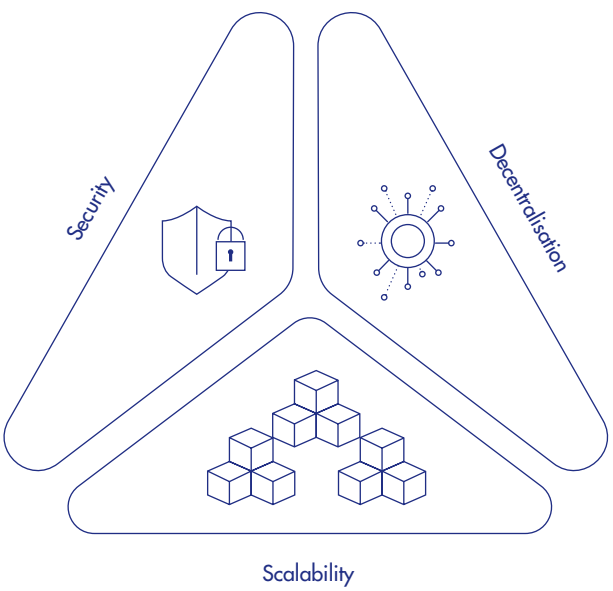
3.3 The underlying technical functionality

The principle of blockchain is structured around an IT infrastructure implementing technical protocols that enable the entire system to function.

The two main categories of blockchains – permissioned and permissionless – are determined by their mode of participation (often private, and often public, respectively). Technically, both function identically but what distinguishes them is their access. In private blockchains, transactions are only visible to participants who have permission to access them. Access is therefore limited and, as a result, there is only partial transparency. On the other hand, when the blockchain is public, the transactions are visible to all and are regarded as immutable, and network fees can sometimes be high.

At the design stage of a blockchain, the main objectives pursued are (i) network security, (ii) decentralisation (control by multiple participants), and (iii) scalability (the system's capacity to handle more transactions more quickly and at lower cost). These three objectives are difficult to reconcile, and make up a kind of "trilemma". The functioning of blockchains has therefore evolved in recent years to strike an optimal balance depending on market uses and expectations.

D4 THE BLOCKCHAIN TRILEMMA



Source: Observatory for the Security of Payment Means.

3.3.1 Native blockchains

Originally, the blockchain was based on a first layer – "Layer 1" – which allows transactions to be recorded directly "on-chain". It employs consensus mechanisms[16] to guarantee process security and decentralisation. These mechanisms consist of a network of nodes[17] that use various protocols[18] to agree on the validity of transactions without the intervention of a central authority. This so-called blockchain "infrastructure" is designed with security, governance, consensus and execution features.

The structure of the underlying technology can be broken down into three main components:

- the **network**, which consists of several computers or servers – nodes – that execute an algorithm to secure the system by receiving transactions, validating them according to the rules of the protocol used, and storing the blocks;
- the **blocks**, which comprise a set of transactions and which can vary in number depending on the chain used; and
- a **chain**, which links the blocks end-to-end through a cryptographic[19] hash, which consists of an unalterable digital fingerprint that secures the transaction (in practice, the data contained in the previous block are encrypted and thus immutable).

Execution time can be long and costly depending on several factors:

- the number of computers validating the transaction – transaction processing speeds vary depending on the network and the number of active validators;
- fees – the "nodes" prioritise transactions with higher network fees (as this is how the node validators are remunerated), more commonly known as "gas fees";
- network congestion – as the number of active nodes[20] is fixed, transactions that accumulate may be put on hold until a new block to contain them becomes available.

15 In this case, private keys are stored locally on the device.

16 A pre-defined process, through which the transaction is completed.

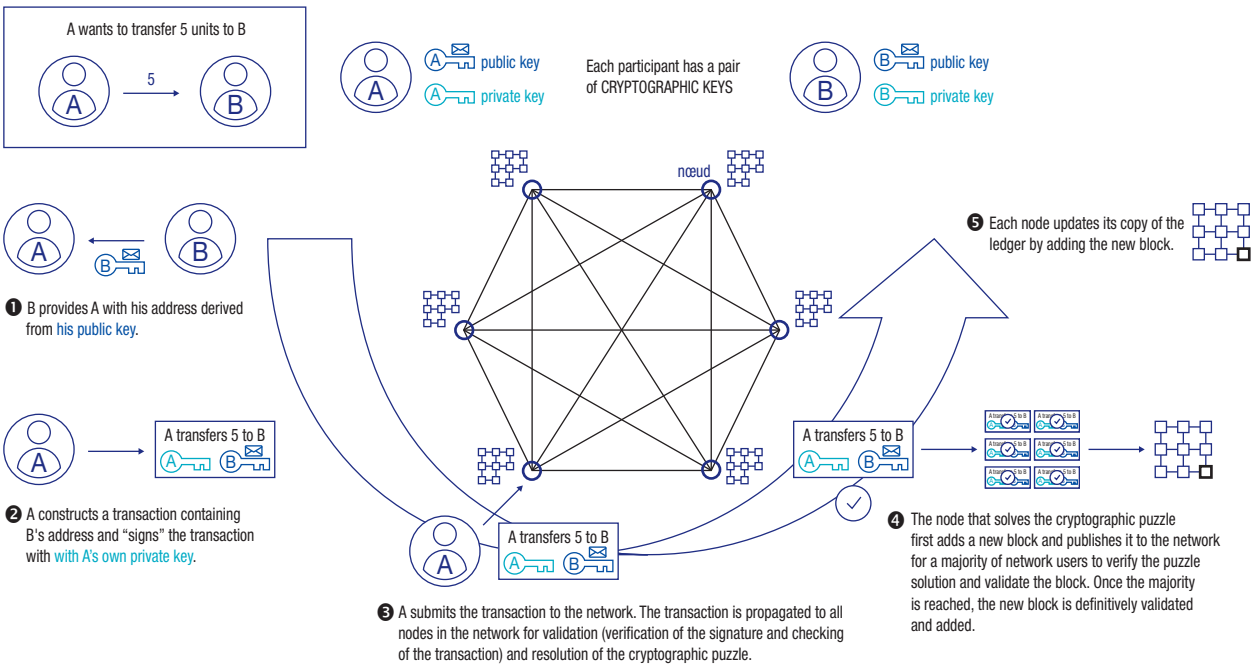
17 A network made up of machines/computers that contribute to the storage, validation/verification and exchange of transaction information.

18 Proof of work or proof of stake.

19 Cryptographic security is built into the blockchain protocol, so the end user has a private key to sign the transaction. Signature verification is a decentralised process, using a public key.

20 For example, for the main networks, the number of nodes is now up to 2,500 for Bitcoin, 1,400 for Ethereum, 5,000 for Solana, and 2,000 for Polygon.

D5 VALIDATION OF A TRANSACTION IN A BLOCKCHAIN WITH PROOF OF WORK



Source: Banque de France (Translation from ABC de l'Économie, *L'Éco en Bref*, « La *blockchain* »).

⇨ For low value transactions, network fees are not negligible and the transaction can take around ten minutes or longer to be validated, with a risk of network congestion. For these reasons, Layer 1-based payments using crypto-assets appear unsuitable for everyday purchases of goods or services, and are therefore not – or very rarely – used in this regard. This technical complexity notably explains the marginal – if not almost non-existent – use of crypto-assets in the strict sense among the payment solutions offered by merchants in France. They are therefore used almost exclusively as speculative assets for investment ends.

3.3.2 Application-specific blockchains

The introduction of an additional layer of blocks, known as "Layer 2", is intended to accelerate and improve the entire blockchain's performance. To do this, transactions are processed off-chain and then validated in Layer 1. The transactions are thus aggregated and processed in bulk, increasing the number of transactions that can be handled and reducing the associated costs.

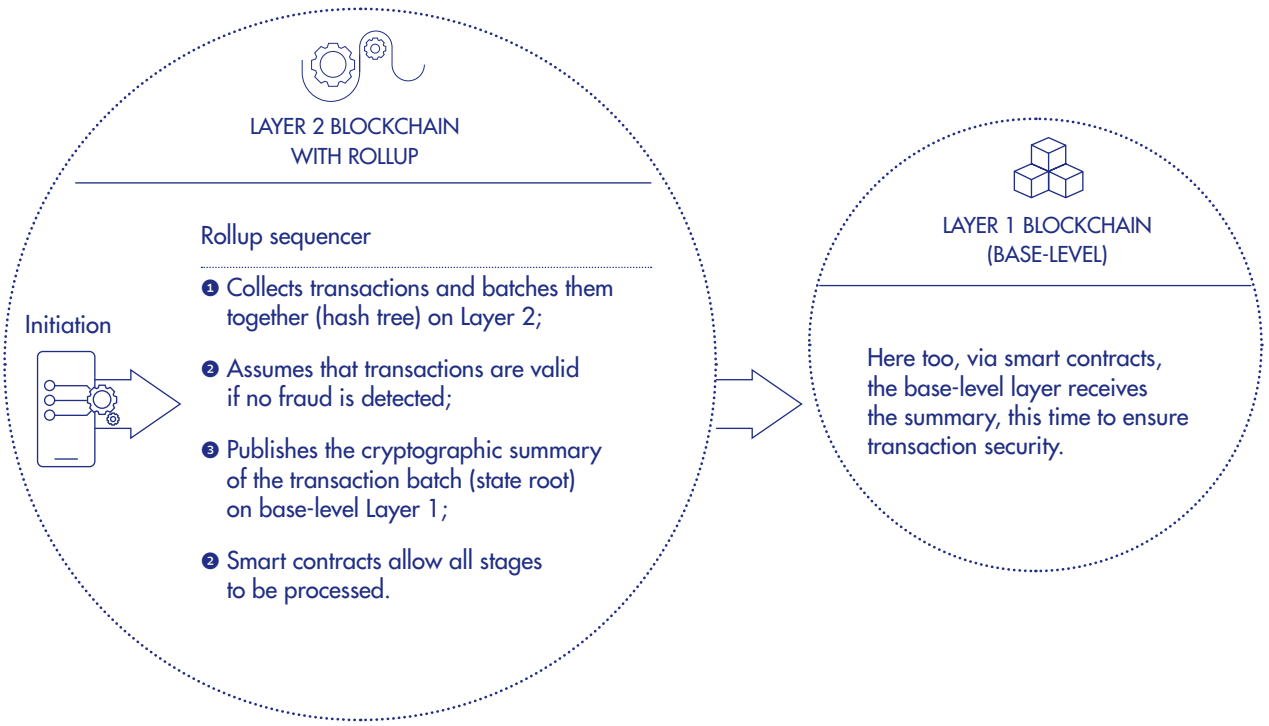
Layer 2 is constantly evolving with the pace of innovation, and several models currently exist. For example, the "optimistic rollup" protocol operates on the assumption that transactions are valid if the detection mechanisms identify no evidence of fraud. The sequencer, which is an operational component of rollups, collects, orders and executes several operations outside the blockchain, thus processing transactions more quickly, and thereby reducing fees. The sequencer batches the transactions together.[21] In this case, a summary of all transactions is published on Layer 1 and the transactions are not immediately verified on this Layer 1 (a detailed verification may take place retrospectively during a dispute period in the event of fraud, for example). On the Layer 2 blockchain, application-based "smart contracts"[22] allow all stages to be processed, and control "smart contracts" on the Layer 1 base chain then ensure security. Another method, used by Zero-Knowledge Rollups (ZK Rollups),[23] further secures operations by generating cryptographic proofs to ensure their validity. These proofs are thus recorded on Layer 1 without revealing the details of the transactions.

A "Layer 3" also emerged very recently. Layer 3 acts as an application layer that facilitates interoperability between layers. It is designed to connect blockchain Layers 1 and 2 with inherent applications and services, without the intervention of a third party.

These additional layers, which have been overlaid on the original blockchain, play an essential role in the development of these new technologies. They underpin the ecosystem's growth possibilities and ensure the interaction between its components.

⇨ Interoperability is an issue that is intrinsic to the technological aspects. Each blockchain network has its own standards, necessitating the use of gateways and therefore creating a first potential point of vulnerability in the payment chain.

D6 ILLUSTRATION OF THE "ROLLUP", A LAYER 2 BLOCKCHAIN PROTOCOL



Source: Observatory for the Security of Payment Means.

3.4 The security challenges

Payments using crypto-assets are exposed to two types of risk: (i) the "classic" risks affecting the use of traditional means of payment; and (ii) the risks more specifically associated with the use of crypto-assets, which relate to the inherent technical characteristics of these new settlement assets.

3.4.1 The "classic" risks

It may not be unique to payments using crypto-assets, but it is important to note from the offset that online scams and fraud involving crypto-assets have increased, and should therefore be a major concern for potential users.

21 They are grouped and organised according to a hash tree or Merkle tree. This is a data structure used in cryptography to reduce the amount of data that needs to be stored in a blockchain for verification purposes. The root hash summarises all the data contained individually in each transaction processed within the same batch.

22 An autonomous programme deployed on a blockchain that automatically executes predetermined rules.

23 The *Report on Decentralised Finance (DeFi)*, European Union Blockchain Observatory and Forum, 24 May 2022, describes a Zero-Knowledge (ZK) rollup as "a scaling solution that executes transactions off-chain and then publishes a cryptographic proof of validity on Layer 1. This proof guarantees the compliance of transactions without disclosing their data, reducing the amount of information to be published on the main blockchain".

In general, when payments using crypto-assets are made through the use of a traditional payment card, users are exposed to the risks associated with card transactions. In terms of security, ISO standards[24] are applied and cryptographically protected data fields are often used. In addition, payment data is encrypted using symmetric and asymmetric encryption algorithms (respectively, Advanced Encryption Standard [AES] and RSA [named after its three inventors] algorithms). Furthermore, the payment processing chain is certified under the Payment Card Industry Data Security Standard (PCI-DSS). However, not all current encryption methods are post-quantum and may therefore prove vulnerable to attacks.

⇨ Measures to adapt to post-quantum encryption must therefore be implemented – in accordance with the recommendations[25] already issued by the OSMP – to prevent this risk to operational resilience.

Similarly, the use of QR codes can also be a vulnerability, notably because fraudsters are able to falsify them (quishing). In this case, the fraudster replaces an authentic QR code with their own fake code in order to receive payments that should otherwise go to a merchant. This method has already been observed in the context of the use of this payment initiation mechanism. Some merchants provide their customers with a static QR code, though this is a factor of risk because static QR codes function indefinitely and can therefore be more easily falsified.

⇨ Dynamic QR codes, on the other hand, expire, thereby reducing the associated risk of fraud.

Generally speaking, the sheer number of players participating in the crypto-asset payment process, which was discussed above, affects the fluidity of the act of payment (and therefore lengthens the time it takes). Moreover, the multiplicity of stakeholders compromises the resilience of the payment chain by introducing an equal multiplicity of potential points of vulnerability.

Furthermore, these payment solutions are less resilient than traditional means of cashless payment. For example, a recent outage at a major cloud provider[26] caused service interruptions that affected several crypto-asset players. The malfunction impacted access to blockchain networks, payment application programming interfaces (APIs) and users' electronic wallets. Resilience also depends on the choice of hosting provider. Concentration around a limited number of critical service providers – that is, services that can influence the security and performance of the system – can indeed give rise to difficulties when data is replicated on two sites that both belong to the same cloud provider.

⇨ Strengthening the Emergency and Business Continuity Plan is therefore essential in light of the potential operational resilience risks that are significantly exacerbated by the use of crypto-assets as a means of payment and by the huge number of players involved in the payment journeys.

3.4.2 In addition to the "classic" risks, there are new risks specific to the use of crypto-assets

3.4.2.1 Blockchain security risk

Blockchains are based on the three principles of cryptography, decentralisation and consensus, which aim to intrinsically ensure their security qualities. However, these native principles are certainly not infallible, especially in the current context of layer accumulation, which aims to optimise blockchain functionality.

The security of blockchains therefore depends heavily on the robustness of the underlying technical infrastructure and protocols. The reliability of nodes, the resilience of cloud providers, the security of APIs and the dependability of "smart contracts" are all critical factors to take into consideration.

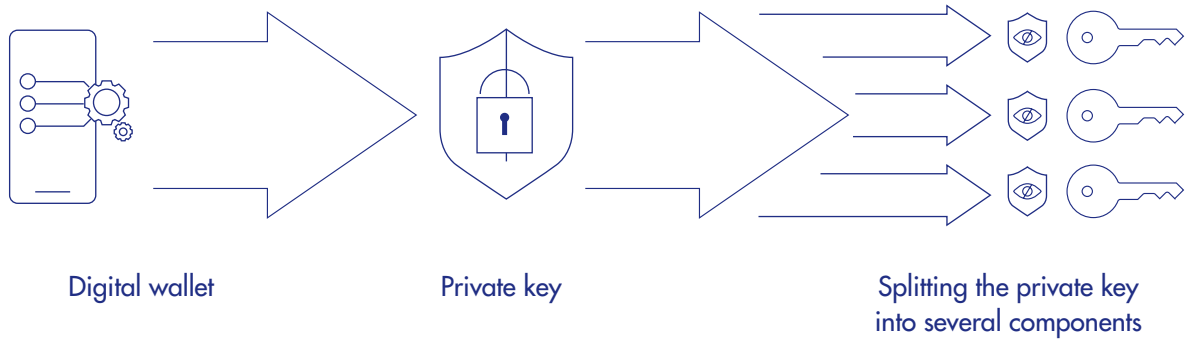
⇨ Given this context, a thorough assessment of the operational robustness of technical components is essential to ensure the security of payments using crypto-assets.

3.4.2.2 The risk of loss/theft of private keys and data leaks

There are different types of crypto-asset wallets. The two main types are physical (hard wallets) and digital (hot wallets or software wallets). Physical wallets have private keys stored on a medium such as a USB stick or secure chip. Digital wallets have private keys stored on a device connected to the internet, in the case of a non-custodial wallet, or online on a remote server, in the case of a custodial wallet.[27] Asymmetric keys are used to secure digital wallets, with a private key used to sign the transaction and a public key used to receive the funds. Consequently, for a purchase, the end user of the blockchain will have a private key to sign the transaction on their digital wallet, while the public key – similar to the bank details of a traditional account – comprises the address for the reception of funds. This public key can, for example, be communicated via the QR code presented by the merchant to the customer.

⇨ Private keys, whether stored on a physical or a digital wallet, constitute sensitive payment data and as such must be protected. They must therefore be secured in order to prevent irreversible loss of access to

S7 WALLET THAT USES A SECURE MULTI-PARTY COMPUTATION (MPC) TECHNIQUE



Source: Observatory for the Security of Payment Means.

crypto-assets or avoid their being compromised by a malicious third party to seeking carry out unauthorised transactions. This enhancement of security should notably include regular updates of devices and storage media for private keys to incorporate the latest versions, as well as protections against unsecured connections, such as unsecured public networks, by using a virtual private network (VPN), for example.

Furthermore, the fraud techniques used to obtain private keys, which give access to crypto-asset wallets and therefore the ability to make payments, are similar to those used for traditional payments: phishing, smishing, fake websites, etc.

⇨ However, more secure versions do exist, such as wallets that incorporate either multi-signature protocols or secure multi-party computation (MPC) techniques. A wallet using an MPC technique is a cryptographic solution more suited to retail payments, in which the entire private key is no longer stored in one single place. It is split by multi-party computation protocols between the payer, the service provider and, potentially, a trusted third party. Consequently, compromising the private key becomes more difficult.

3.4.2.3 The risks associated with smart contracts

Another potential point of vulnerability lies in the fact that payments using crypto-assets are most often made via systems that are automatically executed when predetermined terms and conditions are met at the blockchain level, known as "smart contracts". In practical terms, these are computer codes written in a programming language specific to the blockchain used. The objective is to predetermine the conditions for the execution of operations, whether they involve issuing crypto-asset units or other transactions, and to define the roles and functions of the parties involved. For example, with these smart contracts it is possible to make the execution of a payment conditional on the fulfilment of an external condition, such as the provision of funds in an account or the authorisation of a transfer, and to schedule the execution of recurring transactions. However, smart contracts can be modified during an external hack using conventional cyberattack methods, for example, or through internal fraud carried out by an individual able to act within the entity operating the smart contract. Once the contract has been modified, the fraudster can then commit a wide range of fraudulent activities: gaining access to asset portfolios, making fraudulent payments, etc.

The Open Web Application Security Project (OWASP) – an international non-profit organisation dedicated to improving web application security – has identified the top ten vulnerabilities found in smart contracts and has drawn up several security recommendations in response.[28]

24 Standards defined by the International Organization for Standardization (ISO) and applicable to products and services.

25 Chapter 3 (pages 37-53) of the *Annual Report of the Observatory for the Security of Payment Means 2023*: "Quantum computing and the security of bankcard payment systems".

26 IT service provider (infrastructure hosting services, data hosting services, etc.).

27 Private keys are stored on third-party servers, such as exchange platforms.

28 On the OWASP Smart Contract Security website.

Illustrations of the main vulnerabilities of "smart contracts"

1. "Reentrancy attacks": these can lead to the embezzlement of funds by a fraudster who manages to execute a programme function several times before the smart contract updates its internal state to reflect the completion of the transaction (as in the PenPie Hack in 2024).

2. Access control failure: the fraudster manages to access programme functions that should only be accessible to the administrator, such as refunds, in order to misappropriate funds (as in the Bybit Heist in February 2025).

3. A flaw in the overflow check within the liquidity calculation function: a flaw in the smart contract that allows a hacker to trick the programme into believing that more liquidity is being added than is actually the case. As a result, the smart contract price calculations become distorted, allowing the attacker to withdraw more assets than have actually been contributed (as in the Cetus Hack in May 2025).

Smart contract security is therefore a key challenge. As such, players have implemented certain best practices, such as having the smart contract audited by an independent third party, some of which are certified by the *Agence nationale de la sécurité des systèmes d'information* (ANSSI – the French national cybersecurity agency) as 'information system security audit providers' (Passi),[29] which attests to their expertise in cybersecurity.

⇨ Furthermore, the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French Prudential Supervision and Resolution Authority) and the *Autorité des marchés financiers* (AMF – the French Financial Markets Authority) have published a working group report on smart contract certification (*Rapport du groupe de travail sur la certification des contrats intelligents*). It sets out several suggestions to guide (i) the definition of certification standards for smart contracts, including the broader security principles that these could encompass, (ii) the use of existing audit methods in the context of this certification and the bodies and resources likely to implement them, and (iii) regulatory approaches that could be incorporated into a potential certification scheme.

3.4.2.4 Real-time monitoring of Layers 1 and 2

In addition to the risks associated with the primary blockchain (Layer 1), transactions carried out within Layer 2 must also be subject to monitoring, as they form external circuits to the primary blockchain, the results of which are then fed back into it. The bridge between Layer 1 and Layer 2 is thus also a potential point of vulnerability.

⇨ Payments using crypto-assets should therefore be monitored in real time, in the same way as traditional payments, in order to ensure operational security to counter attacks and detect fraudulent transactions, and thereby combat fraud effectively.

3.5 Compliance challenges

3.5.1 Challenges related to the security of the payment journey

Payment solutions using crypto-assets must comply with the regulatory requirements regarding payment journey security, which form the basis of this study, with all other regulatory aspects excluded. Application of the rules set out in the second European Payment Services Directive (PSD2) is therefore mandatory for crypto-assets, which are classified as "electronic money tokens" (EMTs) and thus treated as funds. However, their application is not strictly mandatory for payment solutions based on crypto-assets that are not classified as funds. These include first-generation crypto-assets or "asset-referenced tokens" (ARTs). As a result, certain unregulated players offer payment solutions using crypto-assets other than regulated EMTs, which therefore present a non-negligible risk to users.

⇨ Based on the "same activity, same risk" principle, it is recommended that all players, regulated or not, comply with these rules for their crypto-based payment solutions, regardless of the legal classification of the crypto-asset itself. This particularly applies to the requirements for strong transaction authentication.

The security regulations set out in PSD2 apply to crypto-assets classified as EMTs, in particular those relating to strong customer authentication (SCA)[30] for online payments, PIN code use for card transactions exceeding EUR 50, and biometrics for mobile transactions. Beyond payments, crypto-asset service providers (CASPs) must also ensure strong end-user authentication to make access to crypto-asset wallets and the execution of sensitive operations (password or IBAN changes, registration of a new trusted device, etc.) more secure.

⇨ In this regard, the review of the PSD3/PSR legislative package currently underway and its potential regulatory implications for players in the crypto-asset payment chain will have to be monitored very closely, as it is important to ensure that all players in the sector comply with the security requirements established by the coordinated PSD and MiCA frameworks, in particular through the clarification and structuring of the statuses of PSP and CASP.

In this regard, at the request of the European Commission, the European Banking Authority published an opinion in June 2025 that notably emphasised the need to comply with certain provisions of PSD2, including strong customer authentication for access to crypto-asset wallets and payment fraud reporting. The aim is to thereby ensure a high level of consumer protection, regardless of the means of payment used (EMTs or "traditional" funds). The EBA also pointed out that consumers and other market players need to be adequately protected and have a high degree of confidence in the stability of the market and the reliability of payment transactions in order to enable efficient and secure retail payments.

3.5.2 Challenges related to the security of the payment system

DORA (the Digital Operational Resilience Act), the European regulation on cyber resilience in the financial sector, imposes the same cybersecurity obligations on CASPs as on PSPs, as well as the implementation of tests and procedures to control and protect information systems. However, at this stage, as blockchain infrastructure is not regulated, the use of a new blockchain by a crypto-asset issuer is not subject to any governance framework and may therefore raise security issues. Any new use must therefore be brought to the attention of the authorities and crypto-asset holders in a white paper required under the MiCA Regulation and drawn up by the issuer.

⇨ In this respect, an additional best practice to be encouraged in order to make a blockchain infrastructure secure over time, is risk analysis, including an upstream audit and a regular downstream audit of blockchains, taking into account any new added features.

These resilience issues also apply to existing infrastructure. CASPs must therefore comply with MiCAR and DORA requirements and, in particular, put in place operational IT risk management policies.

3.5.3 Challenges related to the security of payment players and assets

Going beyond the security aspects, accepting payments using crypto-assets requires professionals – merchants or technical service providers integrated in the payment solution – to use a duly authorised third-party service provider.

⇨ The entity responsible for executing the transaction and converting crypto-assets into a legal tender currency must be approved (by the AMF if established in France) as a CASP.[31] The entity making the payment in euro to a merchant's accounts must be approved (by the ACPR if established in France) as a PSP or as a PSP agent.

Similarly, crypto-assets offered by operators must comply with the regulatory requirements. As such, merchants and their service providers must select assets before accepting them for payment and strictly refuse those that do not comply with regulations.

⇨ In this regard, several market authorities, including the AMF,[32] are calling for a strengthened European framework for crypto-asset markets (with a potential adjustment of the MiCA Regulation). They recommend that consideration be given to issues such as strengthening the rules for platforms operating outside the European Union, better supervision of platforms given cyber risks, and direct supervision by the European Securities and Markets Authority (ESMA) for significant CASPs. Their aim is to ensure that the rules for European players are applied uniformly.

29 Référentiels d'exigences pour la qualification – Référentiel Passi.

30 The European rules on strong customer authentication are specified in a delegated act of PSD2: Regulation (EU) No 2018/389 detailing the transactions subject to these rules.

31 The issuance of electronic money tokens is restricted to credit institutions (CIs) and electronic money institutions (EMIs). The provision of crypto-asset services, the list of which is defined in Article 3 of the MiCA Regulation, is restricted to crypto-asset service providers (CASPs).

32 AMF, 15 September 2025: *"Les autorités de marché française, autrichienne et italienne appellent à un cadre européen renforcé des marchés de crypto-actifs"*.

RECOMMENDATIONS

The Observatory would first like to stress that crypto-assets present numerous risks (associated with volatility, liquidity, default, money laundering and terrorist financing, high transaction costs, etc.), which do not fall in the strictest sense within the security issues addressed in the recommendations below. They require heightened vigilance on the part of their users and the competent authorities.

On the basis of this monitoring study, the OSMP is issuing the following recommendations on the security of payment solutions using crypto-assets in the context of everyday purchases of goods and services.

RECOMMENDATIONS FOR CONSUMERS AND MERCHANTS

Recommendation No. 1
Stay alert to attempted fraud

The Observatory recommends that users interested in payment solutions using crypto-assets verify the regulatory authorisations of the providers and the crypto-assets used. Crypto-assets that are not authorised in the European Union should be refused.

The Observatory also reiterates its general security recommendations: never respond to unsolicited approaches, never click on sponsored links (visit the website directly), never validate transactions that you did not initiate, etc.

Regulatory authorisations for crypto-asset service providers (CASPs) and for payment service providers (PSPs) can be checked on the websites of the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA), respectively. Providers who are operating illegally can also be identified through the ACPR and AMF blacklists.[33]

Recommendation No. 2
Ensure the security of sensitive payment data

The Observatory recommends that end users of payment solutions using crypto-assets protect their stored private keys, in accordance with the type (physical or digital) of wallet:

- by keeping their device in a secure location, not saving their recovery phrase online, and making sure their password is strong;[34]
- by strongly authenticating themselves on the exchange platform or non-custodial wallet provider;
- by never disclosing their sensitive payment information in the event of a request by telephone or email from a third party;
- by regularly updating devices and private key storage media to the latest, most secure versions;
- by protecting themselves against unsecured connections, such as unsecured public networks, and by using a secure internet connection and a virtual private network (VPN) to protect their data on the internet and allow them to browse anonymously.

Recommendation No. 3
Favour payments using regulated assets such as electronic money tokens

The Observatory recommends that users and merchants interested in these solutions favour crypto-assets issued by entities governed by MiCA Regulation, such as electronic money tokens, for everyday payments, in order to benefit from the security provided by the regulatory framework governing them.

Recommendation No. 4
For merchants, favour the use of dynamic QR codes

Static QR codes made available to customers pose a risk of fraud (quishing). Consequently, static QR codes for cash register systems without digital displays are less secure.

RECOMMENDATIONS FOR PARTICIPANTS IN THE CRYPTO-ASSET PAYMENT SECTOR

First, the Observatory recommends the proposals[35] **published in 2025 by the "Working Group on Smart**

Contract Certification", under the aegis of the ACPR-AMF Fintech Forum, on the auditing, governance and regulation of smart contracts.

Second, the Observatory also recommends that crypto-asset payment solution providers follow its 2023 recommendations for anticipating quantum risks (take stock of the security measures in place, test post-quantum algorithms, and draw up a roadmap for anticipating risks related to quantum computing).[36]

Recommendation No. 5
Ensure an equivalent level of protection, by regulated and unregulated players alike, by implementing strong customer authentication rules within the meaning of PSD2 for all payment solutions using crypto-assets, including non-EMT crypto-assets

Payments using crypto-assets necessitate the participation of a large number of players. By strictly following the security principles set out in the second European Payment Services Directive (PSD2), the Observatory reiterates that strongly authenticating the payment process (access to accounts or wallets, initiation of a remote payment, sensitive operations such as changing passwords, IBANs or trusted devices) is essential.

It is therefore all the more important to apply these rules to all players offering payment solutions using crypto-assets, whether regulated or not, given the assets offered (EMT and other crypto-assets) for payment transactions using crypto-backed cards or crypto-asset wallets, as well as the need to protect sensitive payment data.

Recommendation No. 6
Ensure a degree of real-time monitoring of payments using crypto-assets equivalent to that in place for traditional payments

The Observatory invites the players in the crypto-asset payment chain to ensure a degree of monitoring equivalent to that applied to traditional payments (in particular by assessing the individual risk level of each transaction) in order to effectively combat fraud.

Recommendation No. 7
Favour the use of wallets that incorporate MPC private key management techniques

Using wallets that have MPC computation technology significantly enhances the operational security of payments using crypto-assets. Having this technology integrated into a wallet therefore avoids the vulnerability associated with using traditional wallets.

Recommendation No. 8
Carry out a risk analysis before using any new blockchain and continue to monitor it over time, particularly as the blockchain evolves

In order to ensure the security of the infrastructure, the Observatory recommends that crypto-asset issuers wishing to use a new blockchain as part of their activities first carry out a risk analysis and ensure that the chain offers a high level of security. It is also important to audit the blockchain regularly, as it inevitably evolves over time as functional updates are made. Naturally, the scope of these analyses must extend to the processes external to the blockchain that aim to improve its operational performance.

33 Assurance Banque Épargne Infoservice: "*Listes noires des autorités*".

34 Plateforme MesServicesCyber, Anssi, "*Recommandations relatives à l'authentification multifacteur et aux mots de passe*".

35 These proposals are primarily aimed at decentralised activities, but can also apply more broadly to centralised activities.

36 Chapter 3 (pages 37-53) of the *Annual Report of the Observatory for the Security of Payment Means 2023*: "Quantum computing and the security of bankcard payment systems".

APPENDICES

Appendices 1, 3 and 5 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-2025

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

All tables in Appendix 5 can be downloaded in French at the following address:
https://www.banque-france.fr/system/files/2026-09/Dossier_statistique_du_rapport_2025_de_l_OSMP.xlsx

A1 Security recommendations for the use of payment means

A2 Responsibilities and organisation of the Observatory 60

A3 Members of the Observatory

A4 Methodology for measuring fraud involving cashless means of payment 62

A5 Statistical data on means of payment use and fraud

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 L. 141-4, 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

The remit of the *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) covers all cashless payment methods. This scope results from the legislative changes introduced by Article 65 of Law 2016-1691 of 9 December 2016, which extended the remit of the *Observatoire de la sécurité des cartes de paiement* (OSCP – Observatory for Payment Card Security) to include all means of payment other than cash.

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).

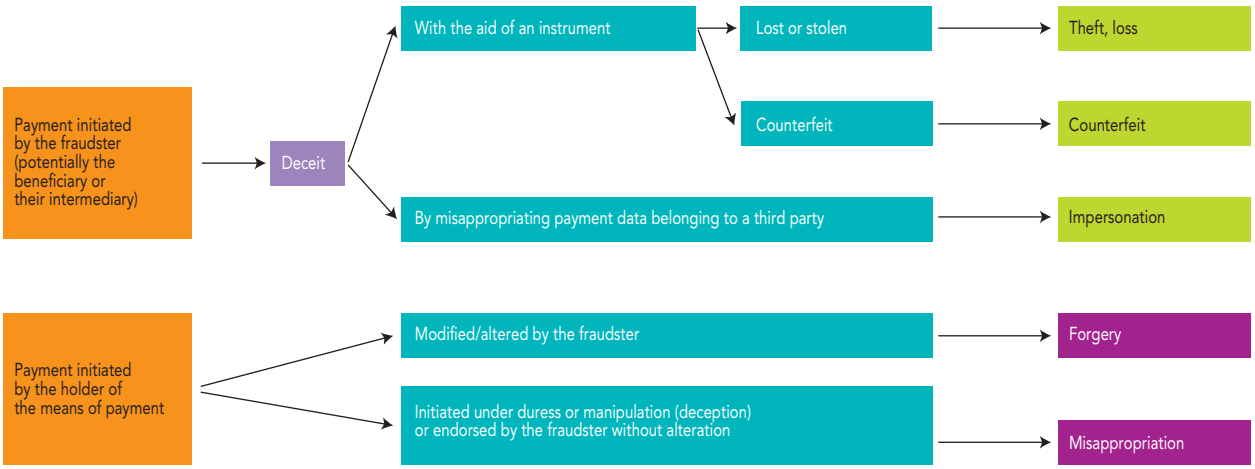
Fraud is assessed using the "gross-fraud" approach. It takes the initial defrauded amount in a payment transaction without taking into account any measures that may subsequently be taken by the counterparties to reduce the loss (for example, interrupting the delivery of products or the provision of services, 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 "PSD2").

Schematic presentation of the types of payment fraud



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 automated 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 automated 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 Second European Payment Services Directive – PSD2 (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 PSD2 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 (PSD2),[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 PSD2: 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

Transactions 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 automated teller machine (ATM).
Payment Initiation Service Providers (PISPs)	Transfer orders initiated via a PISP at the customer's request.

MEASURING DIRECT DEBIT FRAUD

Transactions 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, both in total and broken down by type, is calculated using the new gross-fraud approach, which takes into account fraud detected after the cheque has been presented for payment.

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

Transactions 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

Transactions 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 (PSD2), 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)

Transactions 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 PSD2, 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

Transactions 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.

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, Cyril Ronfort, Marine Soubielle, Valérie Tallarita, Armand Thomas

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 2026
ISSN 2557-1230 (online version)

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).