OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2023

BANQUE DE FRANCE
EUROSYSTÈME

Observatoire
de la sécurité
des moyens de paiement

www.observatoire-paiements.fr

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2023

addressed to
The Minister of the Economy, Finance and Industrial and Digital Sovereignty
The President of the Senate
The President of the National Assembly

by François Villeroy de Galhau,
Governor of the Banque de France,
President of the Observatory
for the Security of Payment Means

SEPTEMBER 2024

CHAPTERS

Chapter 2, Sections 2.1 and 2.4, boxes 2, 3, 4, 5 and 6; and Appendices 1 and 3 are available in French only in the original version of the report, which can be found here: *https://www.banque-france.fr/system/files/2024-09/OSMP-2023.pdf*

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/2024-09/rapport-osmp-2023_dossier-statistique_annexe-5.pdf*

SUMMARY

The general increase in the use of cashless means of payment observed in recent years continued in 2023 (up 5.4% in volume) driven by the enthusiastic adoption of new payment methods, such as mobile payments and instant credit transfers, as well as continued robust growth in e-commerce.

Chapter 1 of this report, which presents statistical trends on cashless means of payment usage and fraud, shows that in value terms, fraud has remained stable, at less than EUR 1.2 billion. *However, trends differ depending on the means of payment.*

- ***The fraud rate for payment cards, which further consolidated their status as the main means of payment for everyday use, stabilised at the lowest level ever recorded by the Observatory (0.053%) for a total amount of EUR 496 million.*** Fraud rates have trended downwards across all electronic initiation channels for payments and withdrawals, with historic lows recorded in the fastest-growing segments, particularly contactless, mobile and internet payments (0.011%, 0.021% and 0.160%, respectively). The average fraud rate for cards remained stable, however, due to the increase in the proportion of payments made over the internet, which continue to be proportionally more exposed to fraud. ***Payment card security thus continues to benefit from the strong authentication rules set down in the second European Payments Services Directive (PSD 2).*** The implementation of these rules explains in large part the continuing decline in internet payment fraud, as well as fraud on mobile payments, for which the fraud rate has fallen by two-thirds thanks to the systematic use of strong cardholder authentication upon card enrolment with a mobile solution. Against this overall backdrop of card fraud containment, the most common fraud technique remains the usurpation of card numbers using phishing techniques (72% of fraud by value), sometimes combined with manipulation (known as social engineering) by telephone to push victims to authenticate fraudulent transactions.

- ***Cheque fraud continued to decline in value, falling to EUR 364 million in 2023 (down 8% year-on-year).*** This is largely due to the prevention mechanisms deployed by banks, in accordance with the roadmap drafted by the Observatory, and in particular ***systems for blocking or delaying cheque settlements, which neutralised EUR 222 million in fraudulent transactions in 2023*** (a 38% improvement on 2022). However, due to the ongoing decline in cheque use in terms of value (down 13.4%), the fraud rate was up in 2023 to 0.078% (compared with 0.073% in 2022). The main type of fraud by far remains the misappropriation of lost or stolen cheques, whether presented directly for payment by a fraudster or used as a means of payment with merchants or private individuals (accounting for 66% of fraud by value and 89% of fraudulent transactions by volume).

- Overall, ***credit transfer fraud has remained relatively stable (down 0.5% year-on-year)*** at EUR 312 million in 2023, despite an 18% increase in the number of fraudulent transactions. Due to the large amounts exchanged with each transfer, the fraud rate remained extremely low at 0.001%. Private individuals and professionals are both affected by fraud, primarily through their online banking activities. Fraudsters have two main approaches: first, fraud involving social engineering (in particular false bank adviser scams) to trick the victim into validating fake transfer orders (43% of total fraud by value); and second, fraud involving misappropriation in which the fraudster alters a legitimate invoice or payment order to steal funds (48% of total fraud). ***Lastly, the adoption of payments by instant credit transfer (up 46% in value terms) has been encouraged by the fact that fraud is held tightly in check, with a downward trending fraud rate (of 0.040%) which is lower than that for payment cards.***

The work undertaken by the Observatory to prevent fraud is presented in Chapter 2, with a particular focus on three key areas:

- ***The Observatory has carried out an assessment of resources and best practices with regard to credit transfer and direct debit payment security***, and has drawn up an initial set of recommendations to make these instruments more secure, particularly in terms of data sharing between institutions, and improving user awareness.

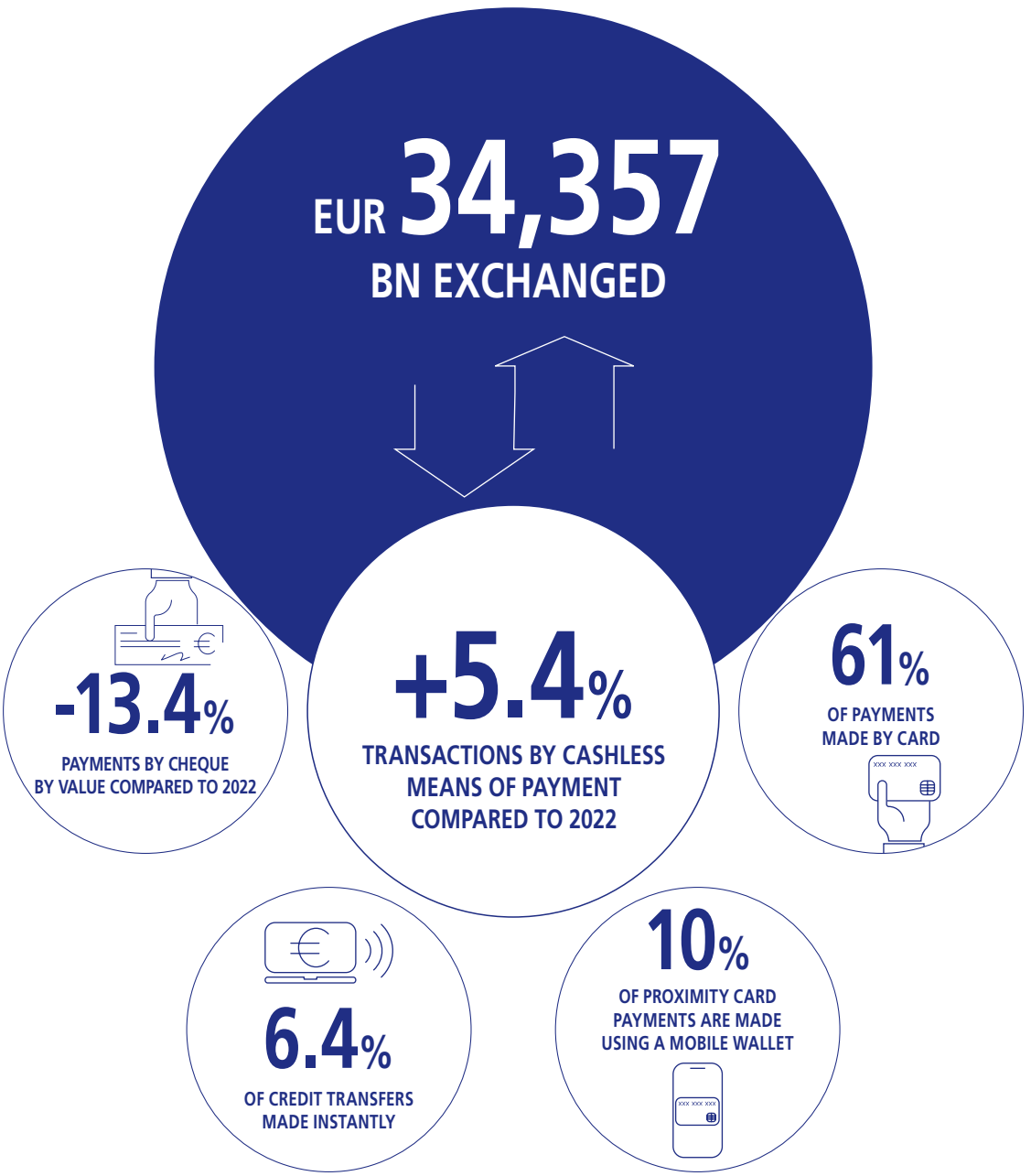
- ***The Observatory has adopted a remote card payment action plan aimed at enhancing the security of non-authenticated payments issued without using the 3-D Secure protocol***, which are still two to three times more likely to fall victim to fraud than transactions that are 3D-Secured. The first measures came into force on 10 June 2024, primarily with the introduction of a EUR 500 acceptance ceiling per card and per merchant. The ceiling will be lowered to EUR 250, and later EUR 100, before the end of 2024, with exemptions for certain sectors of activity.

- Given the proliferation of fraud schemes that involve social engineering and the usurpation of bank or public entity identities via telecommunications networks, ***the Observatory has stepped up its work with the telecommunications sector to monitor the implementation of preventive measures.*** This includes the French MAN (number authentication mechanism) programme, which is intended to ensure that caller ID numbers are authentic.

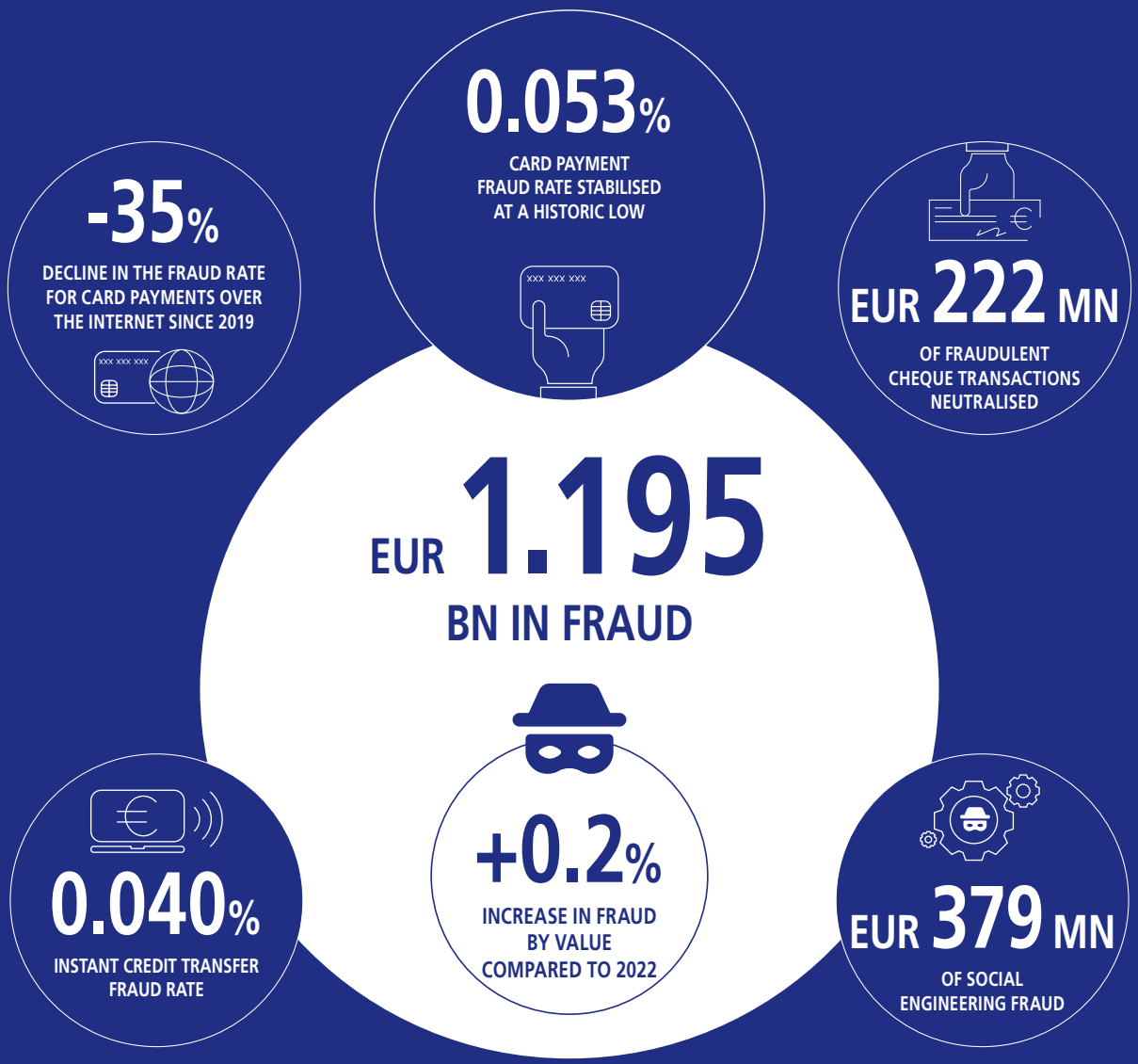
Chapter 3 outlines the work carried out by the Observatory *as part of its technology monitoring duties* ***on quantum computing and the security of bankcard payment systems****. The possibilities offered by quantum computing across a wide range of fields (finance, logistics, meteorology, chemistry, etc.) are promising, but at the same time raise new challenges, particularly in terms of digital security. The use of quantum computing techniques to break encryption schemes for secure electronic communications and protocols under current standards, including those used for payments, could become a reality in the next ten to twenty years. As such,* ***it is a serious threat to national security, which has already been subject to careful consideration by the public authorities in France*** *(French Military Programming Act of August 2023, for example), and must be addressed immediately by the payments sector given the life cycles of card payment hardware and software (chips, electronic payment terminals, servers, etc.).* ***The Observatory has therefore adopted a set of recommendations designed to ensure that the French payments market is properly prepared in the long term for this "quantum menace".***

Against a backdrop of rapidly evolving payment methods and fraud techniques, the Observatory remains committed to ensuring the security of all payment methods, thereby guaranteeing genuine freedom of choice for all users, from individuals to businesses, in their day-to-day transactions. As part of its work programme for 2024 and 2025, the Observatory will look in particular into the possibilities for sharing information to enhance the methods used to combat transfer fraud, and will pursue its initiatives undertaken with players in the telecommunications and distance sales sectors. Finally, the Observatory will direct its technological monitoring activities towards the use of transaction scoring models and artificial intelligence as part of the fight against fraud.

THE USE OF MEANS OF PAYMENT IN 2023



FRAUD TRENDS IN 2023



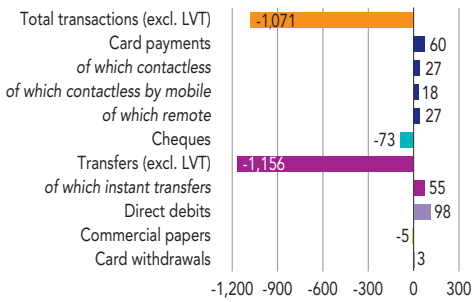
1

FRAUD IN 2023

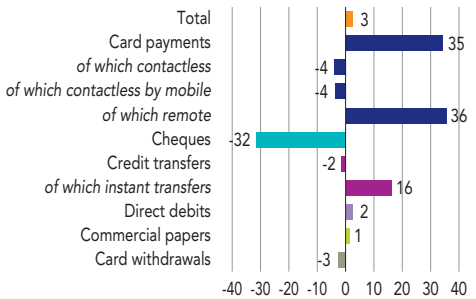
Key data

C1 Changes in means of payment between 2022 and 2023

a) Payment flows (in EUR billions)

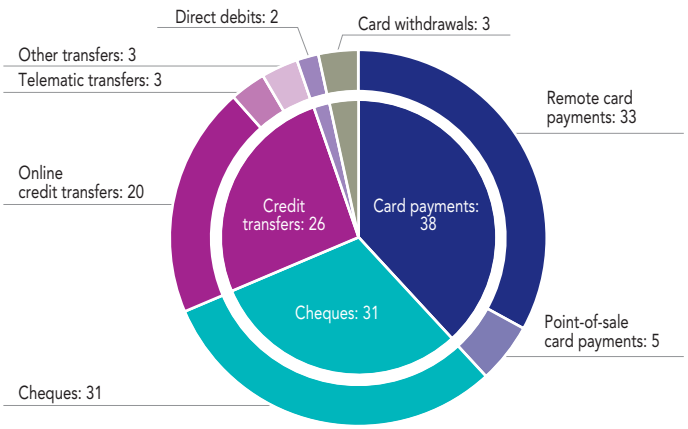


b) Fraud (in EUR millions)



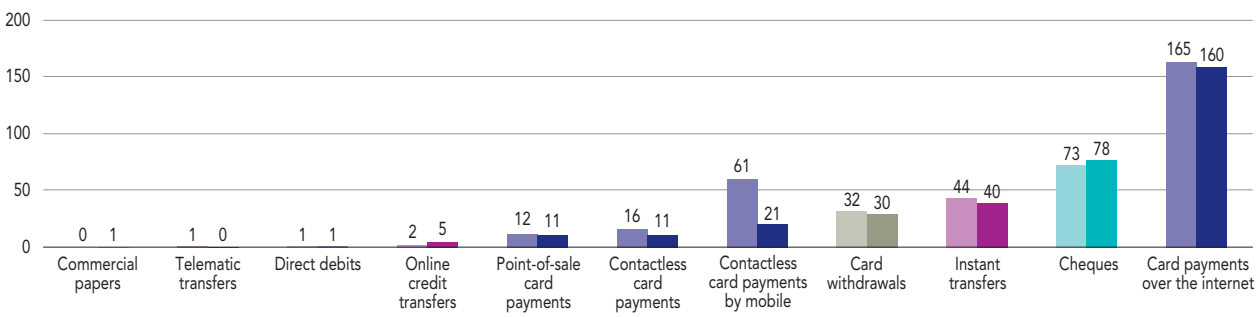
Source: Observatory for the Security of Payment Means.
Note: LVT, large-value transfers.

C2 The main sources of fraud in value terms (%)



Source: Observatory for the Security of Payment Means.

C3 Vulnerability to fraud of the main payment channels in 2022 and 2023 (in EUR defrauded per EUR 100,000 of transactions)

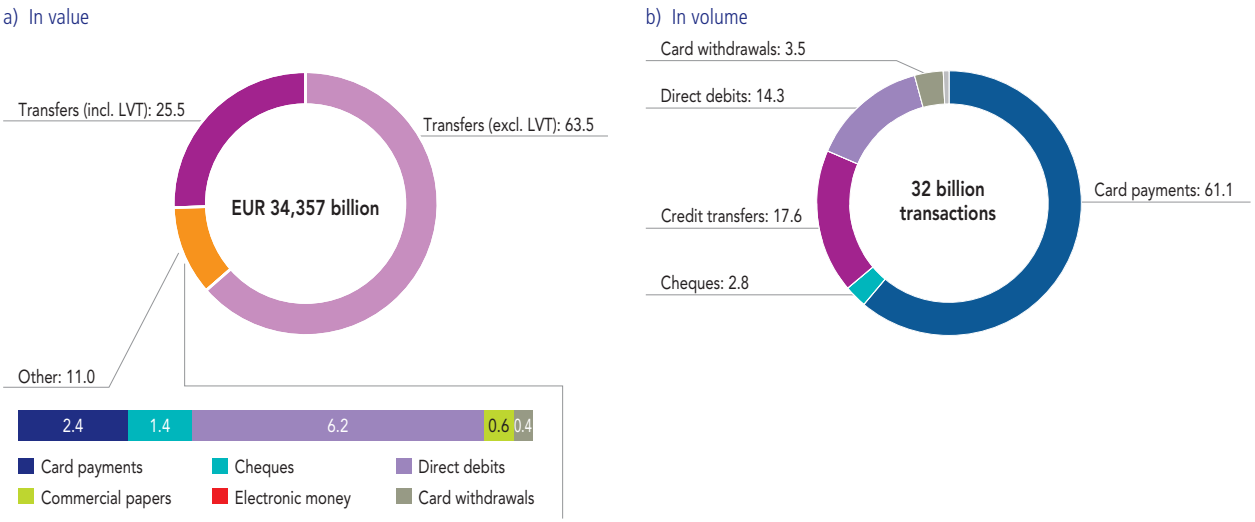


Source: Observatory for the Security of Payment Means.

1.1 Overview

1.1.1 An overview of means of payment

C4 Use of cashless means of payment in 2023 (%)



Source: Observatory for the Security of Payment Means.
Note: LVT, large-value transfers.

In 2023, 32.2 billion cashless payment transactions were carried out by individuals, businesses and public authorities (up 5.2% from 2022), with a total value of EUR 34,357 billion (down 19.3% from 2022). The total cashless payment transaction value was down significantly by more than EUR 8,000 billion mainly due to a contraction in large-value transfers (LVTs),[1] which decreased by 45% year-on-year. This variation is largely attributable to changes in the cash management practices of certain public authorities as interest rates returned to positive territory, and, more marginally, to changes in economic activity. Cashless payment transactions excluding LVTs fell only slightly by 4% (a EUR 1,071 billion decline).

Credit transfers continued to account for the vast majority of total flows, stable at 89%, with LVTs generating 29% of transferred amounts, but only 1.3% of transfer volumes. Instant transfers continued to increase rapidly (up 84% in volume and 46% in value) and accounted for 6.4% of all transfers in volume terms in 2023 (compared with 3.8% in 2022).

Bankcards are still the preferred cashless payment method in France. Their share of transactions (in volume), excluding withdrawals, continued to rise, from 59.6% in 2022 to 60.7% in 2023. Flow volumes also increased in contactless payments (accounting for 68% of payments at point of sale, compared with 61% in 2022), and particularly in payments by mobile phone (10% of payments at point of sale, up from just under 6% in 2022).

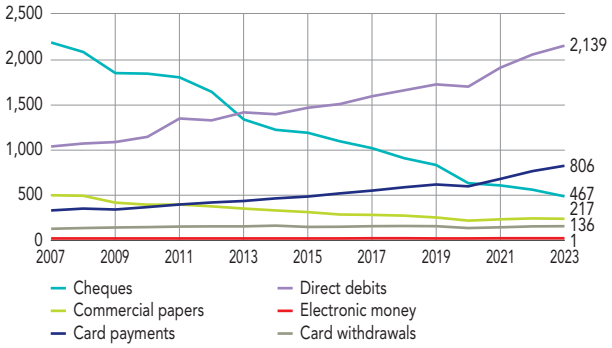
Cheque use continued to fall in terms of both total transaction value (down 13.4%) and volumes (down 11.6%) and they now account for less than 3% of cashless payment transactions.

Cash withdrawals by card remained relatively stable year-on-year (down 0.8% in volume and up 2.0% in value).

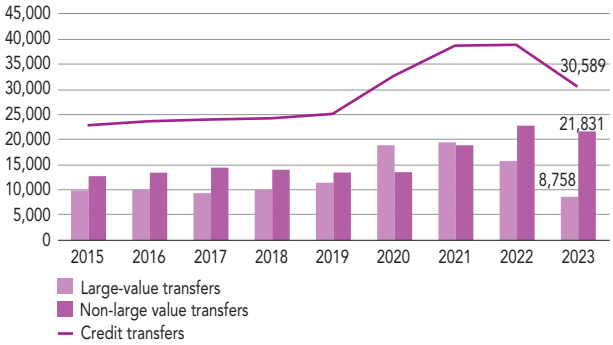
1 LVT: large-value transfers issued via large-value payment systems (Target 2, Euro1); professional payments only.

C5 Payment flows in value terms (in EUR billions)

a) By instrument (excluding credit transfers)

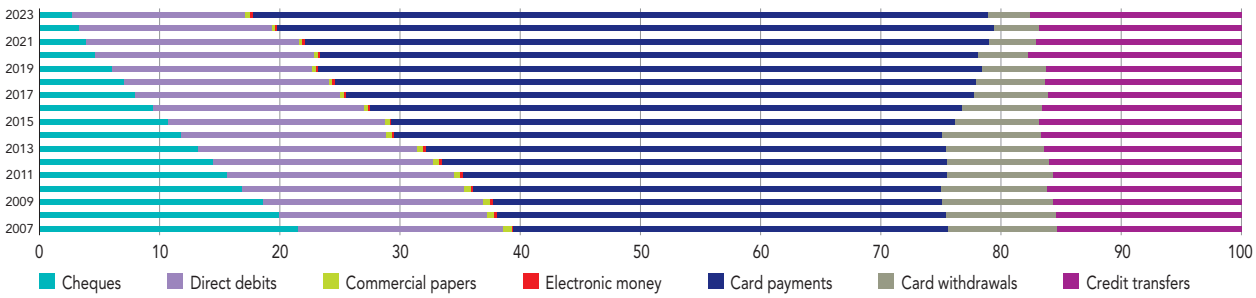


b) By credit transfer



Source: Observatory for the Security of Payment Means.
Note: LVT, large-value transfers.

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



Source: Observatory for the Security of Payment Means.

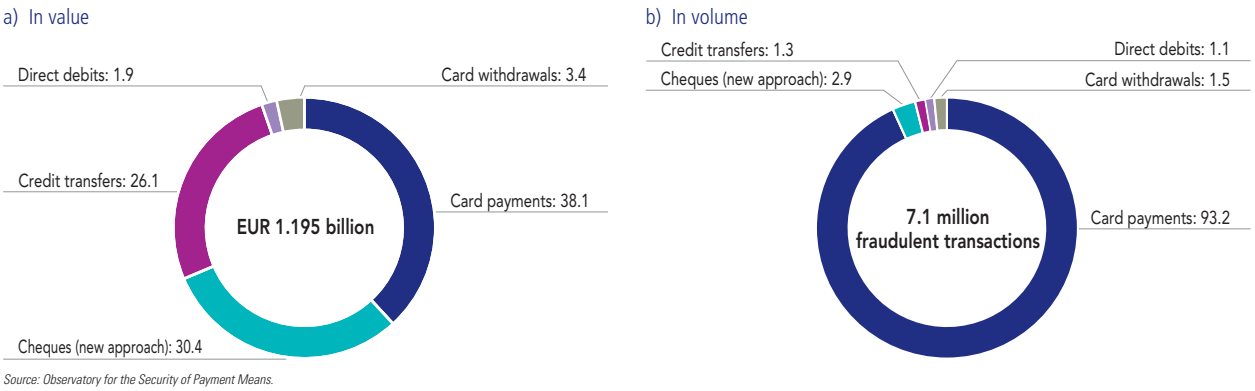
1.1.2 Overview of payment means fraud

Cashless payment fraud stabilised in 2023 with 7.1 million fraudulent transactions (down 0.6% year-on-year) and losses of EUR 1.195 billion (a 0.2% increase on 2022).

The two main trends behind this overall stability were (i) a fall in cheque fraud (down EUR 32 million) offset by (ii) an increase in card fraud (up EUR 35 million), particularly on remote card payments (up EUR 36 million).

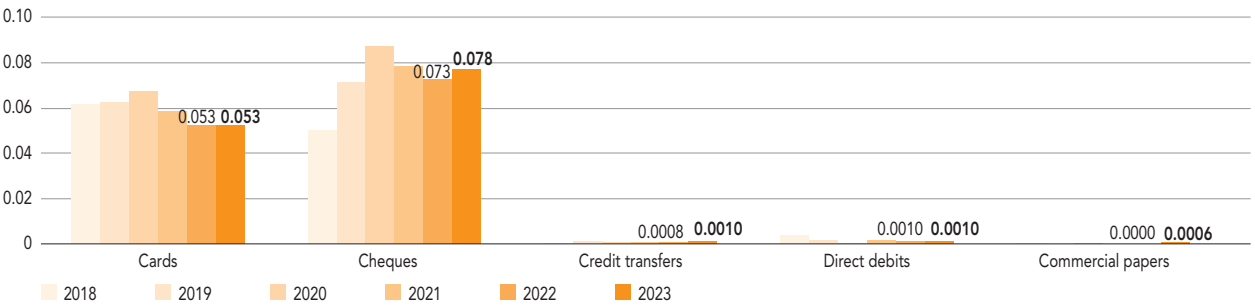
- Despite a downward trend in cheque fraud value, the fraud rate rose again, as the volume of cheque payments declined faster than the number of fraud cases (a 14% decrease in total transaction values compared with an 8% decrease in fraud amounts).
- Conversely, the overall payment card fraud rate stabilised at its lowest level ever recorded (0.053%), as fraud increased to match the growth in payment transactions (up 8% compared to 2022). Card fraud accounted for 38.1% of total fraud amounts in 2023, compared with 35.3% in 2022.

C7 Breakdown of fraud (%)



Source: Observatory for the Security of Payment Means.

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 the new approach. This excludes fraud thwarted after cheques have been presented and settled.

1.2 Current state of payment card fraud

1.2.1 Overview – Cards issued in France

Payment cards further consolidated their status as the main means of payment for everyday use, with flows continuing to increase in 2023, in terms of both volume and value (up 7%). Payments using mobile applications kept growing in popularity in 2023, accounting for 4% of card transactions in France, compared with 2% in 2022.

After declining and then stabilising over the previous two years, fraud was up in value terms in 2023, by 7% year-on-year to EUR 496 million. Internet card payments remain the most exposed channel, representing 71% of cashless payment fraud in terms of value, but only 23% of total transaction amounts. Furthermore, the proportion of contactless and mobile payment fraud continued to fall in 2023, from 3% to 2% and 2% to 1%, respectively.

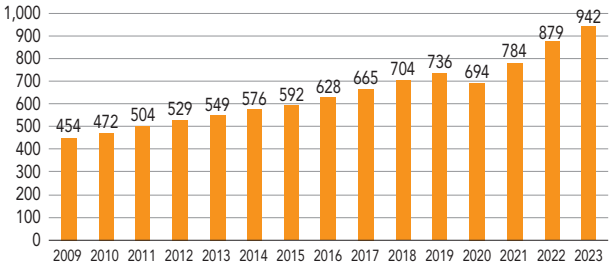
After falling by 10% over two consecutive years in 2021 and 2022 thanks to the widespread introduction of strong authentication for remote transactions, the fraud rate on payments by cards issued in France stabilised at 0.053% in 2023, the lowest level ever recorded by the Observatory.

Two offsetting effects underlie this trend: (i) a decrease of 2 basis points linked to the reduction in fraud rates across almost all payment initiation channels (with the exception of remote payments excluding the internet); and (ii), an increase of 2 basis points linked to the higher proportion of internet payments in the flows recorded, which are relatively more exposed to fraud.

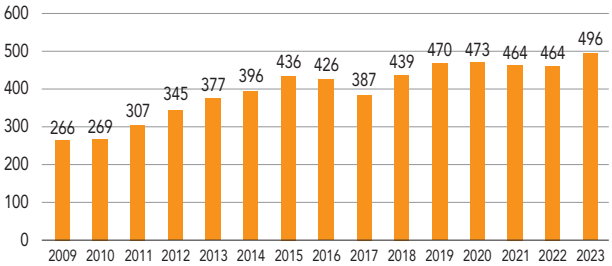
The fraud rate for payments over the internet continued to fall in 2023 to 0.160% (down 3% from 0.165% in 2022)

C9 Cards issued in France in 2023

a) Total value of transactions (in EUR billions)



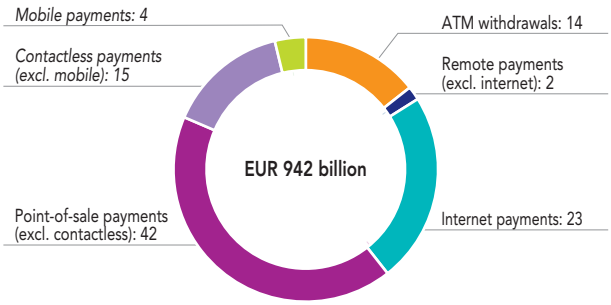
b) Total value of fraud (in EUR millions)



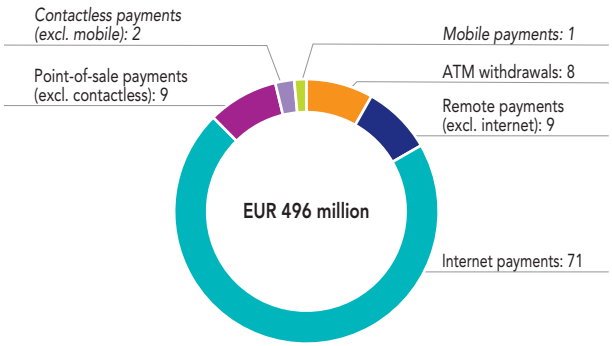
Source: Observatory for the Security of Payment Means.

C10 The use of cards issued in France by payment initiation channel in 2023 (%)

a) Breakdown of transaction amount



b) Breakdown of fraud amount



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

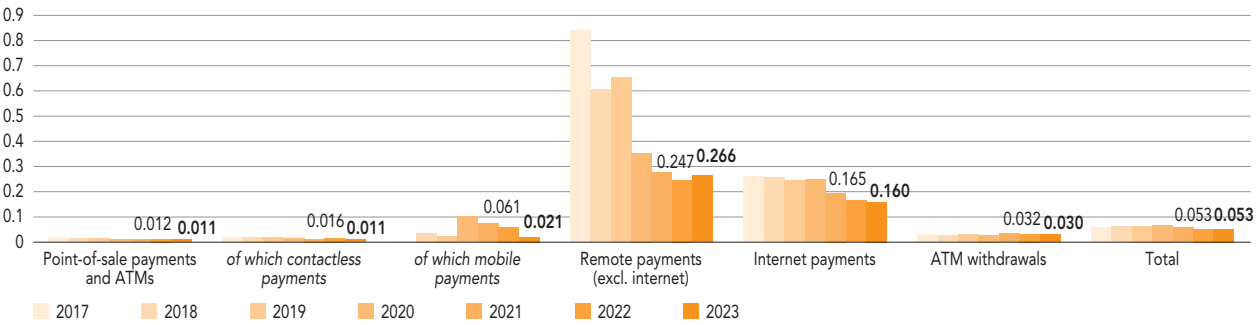
and thus hit a new all-time low. This confirms the very positive effect of the strong authentication rules set down in the second European Payment Services Directive (PSD 2), and of the improved risk measurement tools developed by operators in the electronic payments industry.

The fraud rate for remote payments excluding the internet rose from 0.247% in 2022 to 0.266% in 2023 after a steady decline since 2019. However, these types of transactions, which involve communicating a payment card number by post, telephone or email, account for less than 2% of card payments.

Lastly, the fraud rate for mobile payments in 2023 fell by two-thirds compared with 2022, from 0.061% to 0.021%, mainly thanks to the reinforcement of fraud risk management tools (particularly the systematic use of strong cardholder authentication upon card enrolment with a payment solution). This progress is all the more important given that payment by mobile has been booming in popularity since 2019, increasing more than 42-fold between 2019 and 2023 in terms of value. In 2023, it accounted for 6% of the total amount of point-of-sale payments and 20% of contactless payments.

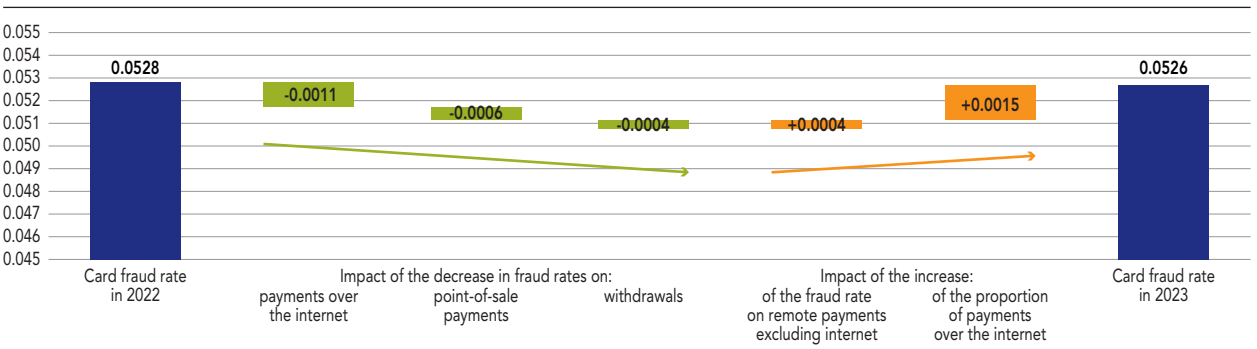
Contactless payment consolidated its status as the preferred point-of-sale payment method in 2023, accounting for 68% of transactions and 31% of total transaction amounts, while its fraud rate dropped to a historic low of 0.011%. The decline is mainly due to a reduction in the theft of cards that are then used for a few transactions under the EUR 50 limit.

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 (%)

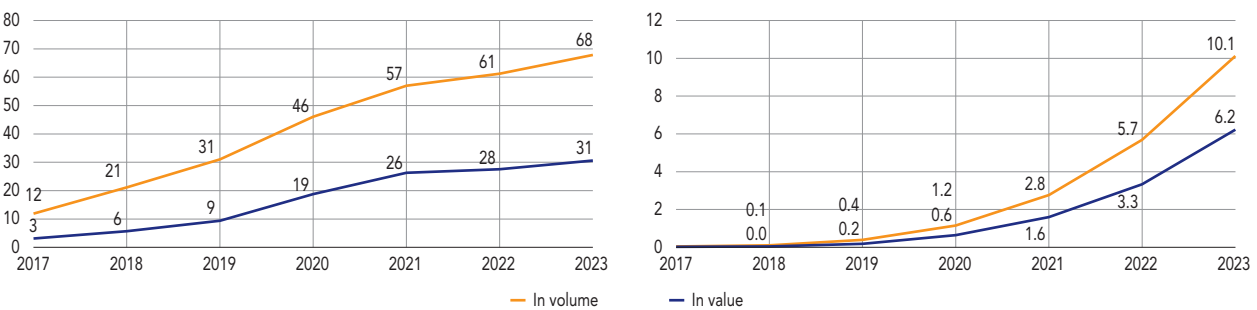


Source: Observatory for the Security of Payment Means.

C12 Card payments at point of sale (%)

a) Share of contactless payments

b) Share of mobile payments

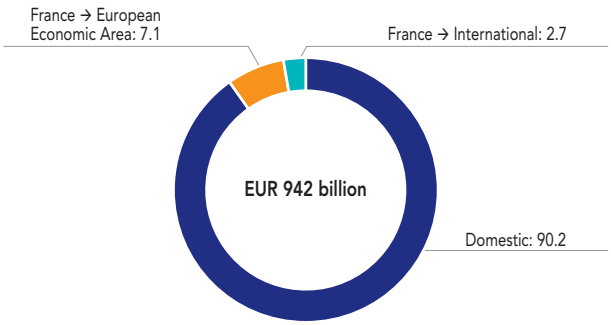


Source: Observatory for the Security of Payment Means.

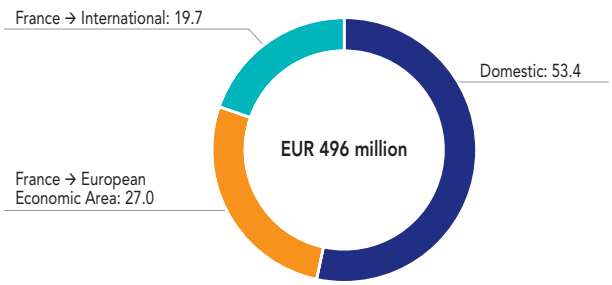
1.2.2 Breakdown of fraud by geographical area – Cards issued in France

C13 Cards issued in France by geographical area (%)

a) Breakdown of transaction amount

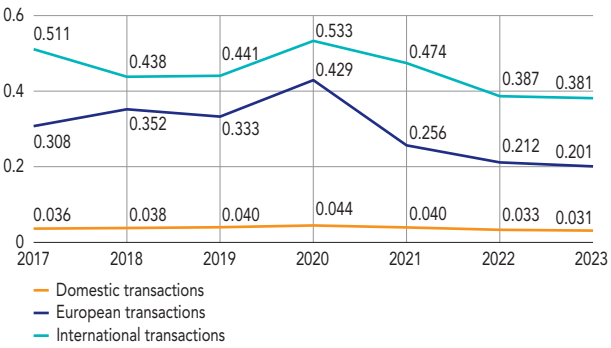


b) Breakdown of fraud amount



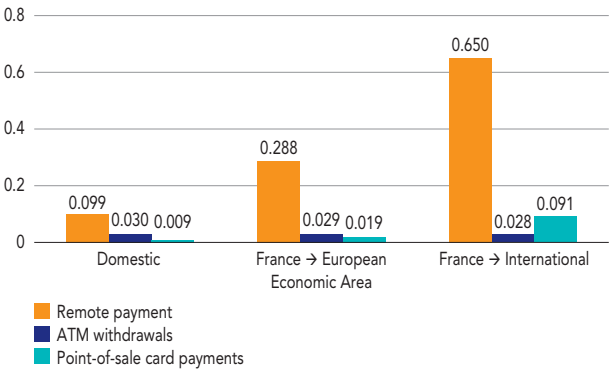
Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

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



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

In 2023, international transactions (including transactions to the European Economic Area) accounted for a relatively unchanged 10% (in value terms) of all transactions carried out using cards issued in France. However, they were the target of 47% of cashless payment fraud (compared with 43% in 2022) with EUR 231 million in incurred losses.

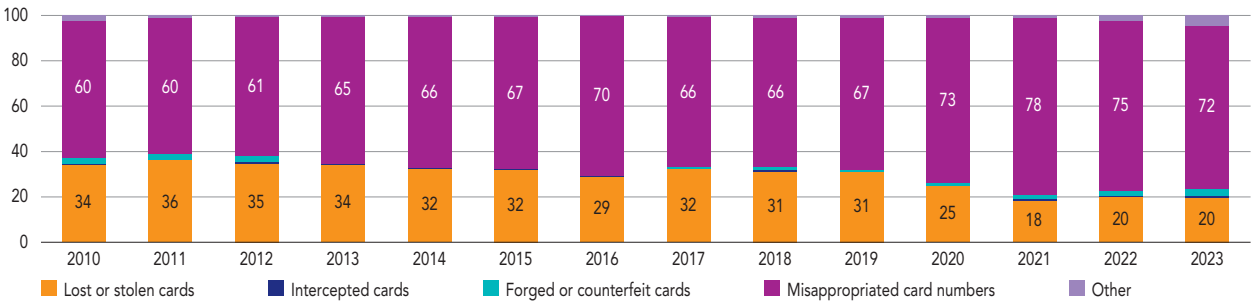
Nonetheless, although international card transactions are structurally more exposed to fraud, as they mainly involve remote payments, their fraud rate continues to improve. Consequently, the fraud rate for European transactions (i.e. with cards issued in France and payments processed in Europe) fell by 17% in 2023, while the rate for international transactions declined by 2%.

The channel with the highest fraud rate for all geographical areas was remote payments, and mainly payments over the internet. Although the rate of internet payment fraud within the European Economic Area fell by 8% in 2023 thanks to the effects of the strong authentication rules, it is still three times higher than France's domestic fraud rate (0.278% compared with 0.093%).

International payments at point of sale are more exposed to fraud, due to the use of less robust technologies (such as reading magnetic stripes or taking physical imprints of a card) that are therefore more vulnerable to counterfeiting.

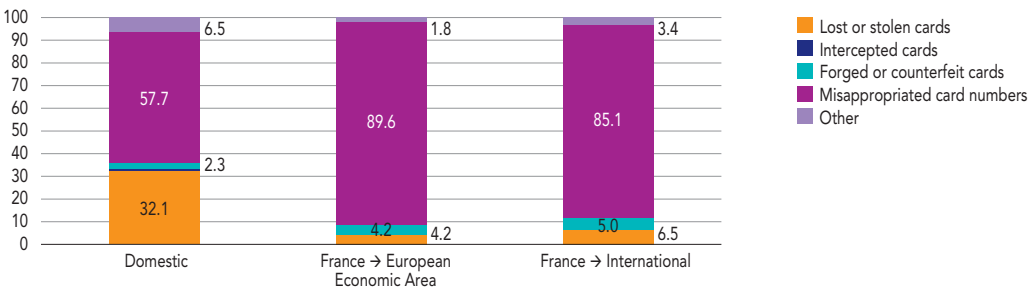
1.2.3 Breakdown of fraud by method – Cards issued in France

C16 Changes in types of fraud since 2010 in value terms (%)



Source: Observatory for the Security of Payment Means.

C17 Types of fraud by geographical area in value terms in 2023 (%)



Source: Observatory for the Security of Payment Means.

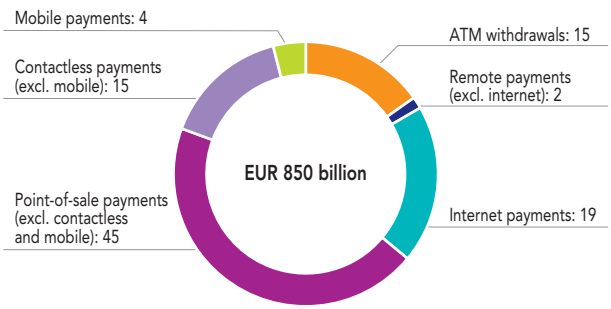
Card number theft using phishing techniques by email or SMS is still by far the most common type of fraud, even though it continued to decline slightly in 2023, to 72% from 75% in 2022.

The proportion of fraud linked to the loss or theft of a card stabilised, still at a modest 20%. Quite understandably, lost or stolen French cards are used first and foremost on French territory (32% of cases), while fraud involving card number theft takes place primarily over the internet with no regard to geographical location. Altered or counterfeit cards are mainly used in countries outside the European Union (EU), where the smart card standard is not yet widespread (in the EU it only accounts for 5% of fraud).

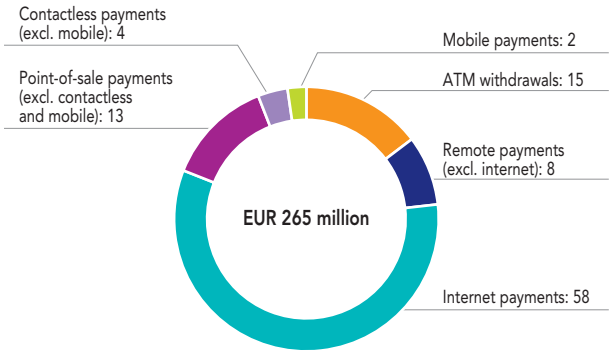
1.2.4 Breakdown of fraud on domestic transactions

C18 Domestic card transactions in value terms (%)

a) Breakdown of transactions

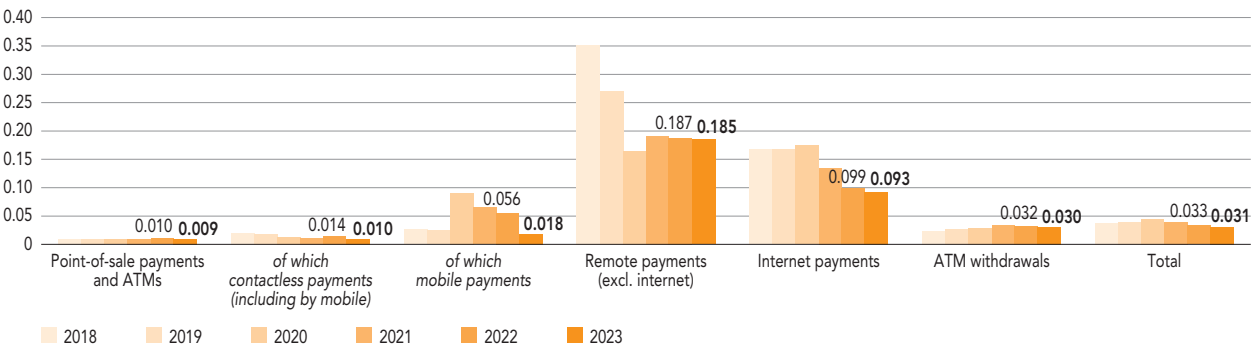


b) Breakdown of fraud



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.

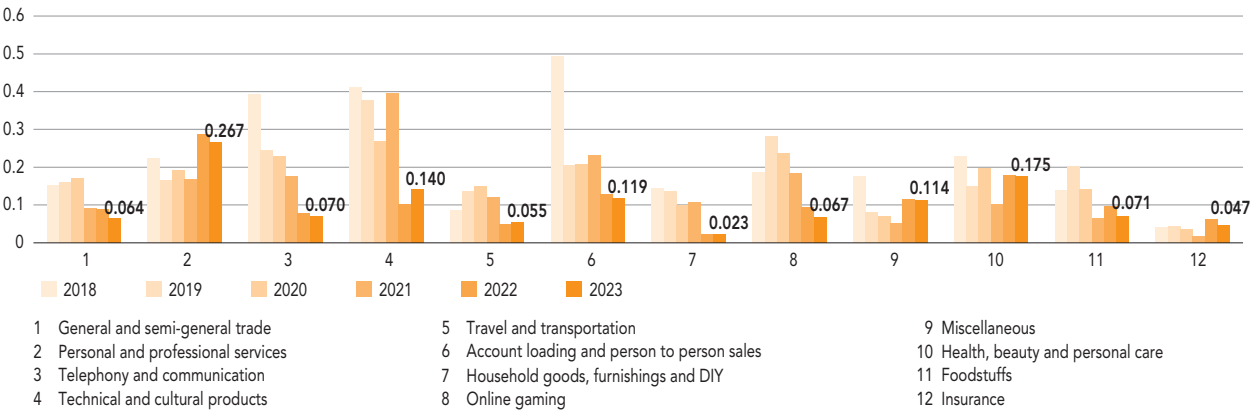
Remote payments accounted for 21% of domestic card transactions in 2023, relatively stable year-on-year, with the bulk of payments made over the internet (93%). Remote payment transaction scams also accounted for almost 66% of total fraud in France (up 3 points from 2022) and led to EUR 175 million in losses; 58% of those transactions involved internet payments. However, internet payments continued to benefit from the widespread introduction of strong authentication set down in the second European Payment Services Directive (PSD 2). The fraud rate for these payments fell again in 2023, by 6%, to 0.093%, its all-time low. The rate has thus halved in the six years since 2017 when the strong authentication rules came into force.

While mobile payments continued to grow in 2023 to account for 4% of domestic transactions, they only represented 2% of total fraud in value terms. The implementation of security measures, such as strong authentication at enrolment, brought the fraud rate down by almost 68% between 2022 and 2023, to 0.018%.

Overall, the fraud rate for domestic card transactions continued its downward trend, with a 6% decline in 2023 to 0.031%, after a 16% drop in 2022.

1.2.5 Focus on domestic card payment fraud on the internet

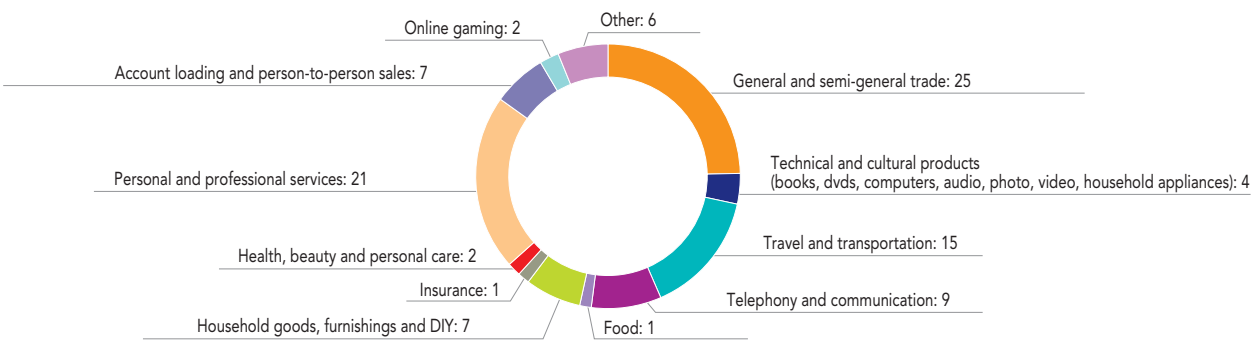
C20 Changes in fraud rates on domestic card payments over the internet, by sector (%)



1 General and semi-general 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 Foodstuffs
12 Insurance

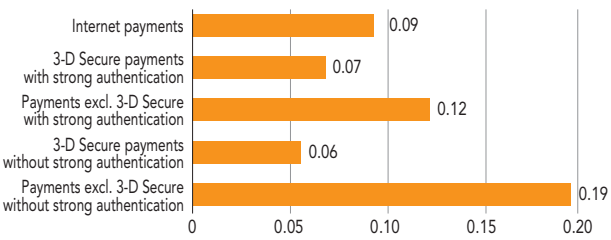
Source: Observatory for the Security of Payment Means.

C21 Breakdown of fraud on domestic card payments over the internet, by sector and in value terms in 2023 (%)



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.

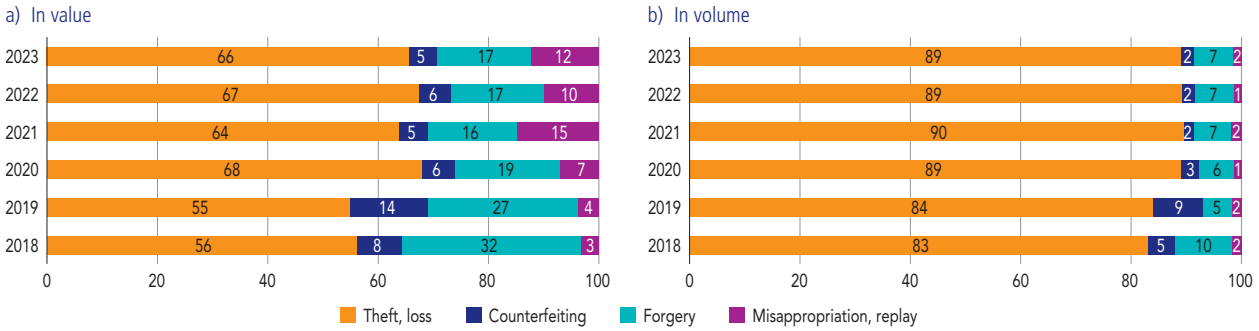
Domestic card payments over the internet that use the 3-D Secure exchange protocol (or an equivalent proprietary protocol) are proportionally subject to a third of the amount of fraud as those that do not. Non-3-D Secure transactions mainly include merchant initiated transactions (MITs), which are similar to direct debits but which use a card as the payment means (e.g. subscriptions, deferred payments or reservations), and certain transactions that are exempt from strong authentication.

For the first time in 2023, the card payment networks and banks subject to the regulations declared their non-3-D Secure transactions with strong authentication to the Banque de France. These are essentially payments made using X-Pay mobile wallets. Domestically, the corresponding fraud rate of 0.12% is on a par with the fraud rate for internet payments (0.09%).

Furthermore, the strong authentication exemption system is proving effective at a national level. In fact, exempt transactions processed through 3-D Secure have a slightly lower fraud rate than those subject to strong authentication (0.06% compared with 0.07%), underlining the fact that the planned exemptions target the least risky transactions.

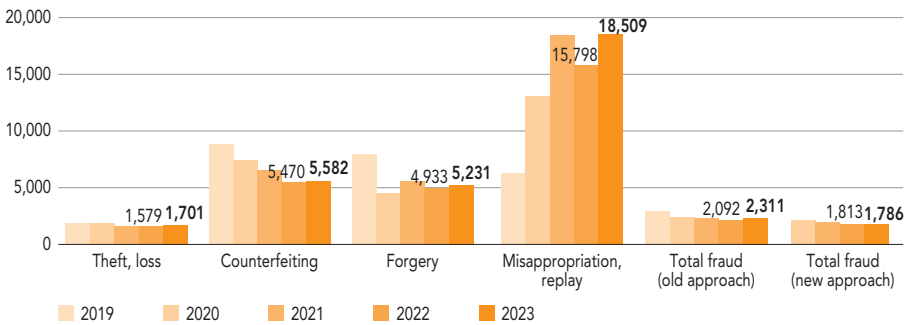
1.3 Current state of cheque fraud

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



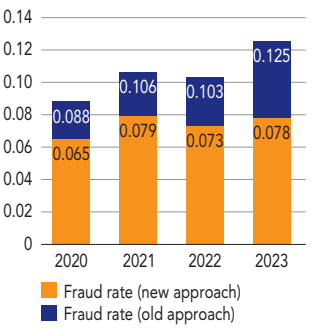
Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

Cheque fraud continued to decline in value in 2023, falling to EUR 364 million (down 8% year-on-year). This improvement is largely a result of the fraud prevention mechanisms introduced by banks in line with the Observatory's roadmap, particularly systems for blocking or delaying cheque payments, which neutralised EUR 222 million in fraud in 2023 (up 38% year-on-year).

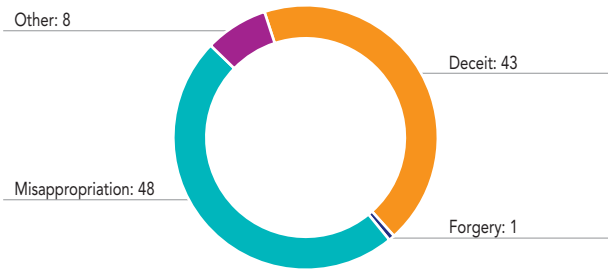
However, as the amounts paid by cheque dropped even more sharply during the year (down 13.4%), there was an upturn in the cheque fraud rate – after deducting thwarted fraud – to 0.078%, compared with 0.073% in 2022. The main type of fraud by far remains the misappropriation of lost or stolen cheques, whether presented directly for payment by a fraudster or used as a means of payment with merchants or private individuals (accounting for 66% of fraud by value and 89% of fraudulent transactions by volume).

The average defrauded amount for all types of cheque fraud increased, to EUR 2,311 (before adjustment for thwarted fraud). However, this figure falls to EUR 1,786 after deducting neutralised fraudulent cheque payments (thanks to banks more effectively detecting the largest fraud amounts).

Although the Observatory noted positive progress in 2023 following the recommendations it published in 2021, cheques still have the highest fraud rate of all means of payment; a rate that increased in 2023 by 7% compared with 2022.

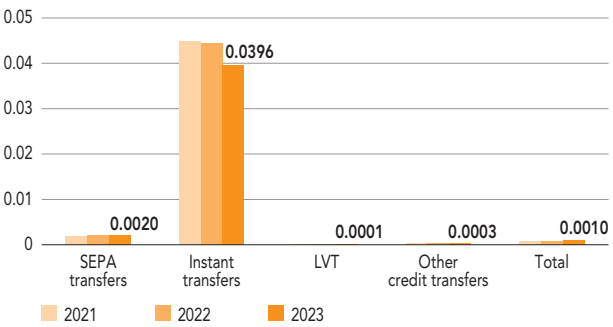
1.4 Current state of credit transfer fraud

C26 Breakdown of transfer fraud by type of fraud in value terms in 2023 (%)



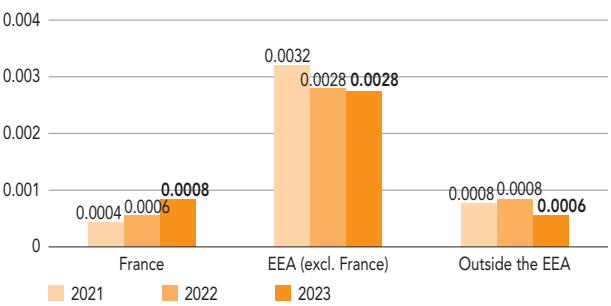
Source: Observatory for the Security of Payment Means.

C27 Transfer fraud rate by type of transfer (%)



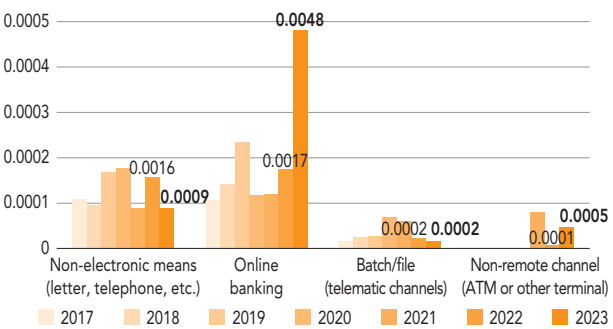
Source: Observatory for the Security of Payment Means.
Note: SEPA, Single Euro Payment Area; LVT, large-value transfers.

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.

Overall, credit transfer fraud remained relatively stable, decreasing from EUR 313 million in 2022 to EUR 312 million in 2023 (down 0.5% year-on-year), despite an 18% rise in the number of fraudulent transactions. As a result, the average transfer fraud amount fell to EUR 3,446 (down from EUR 4,075 in 2022).

Online banking continued to account for highest proportion of transfer fraud in 2023 with its fraud rate rising sharply to 0.0048% in 2023. This represents an increase of more than 180% and is the result of two interacting factors: (i) a steep increase in fraud (up 10% in 2023 to EUR 237 million, compared with EUR 216 million in 2022 and EUR 166 million in 2021); and (ii) a substantial reduction in transfer amounts (almost 60%, down to EUR 5 billion in 2023 from EUR 12 billion in 2022). The second factor can be traced back to changing cash management rules in certain large public administrations.

Conversely, the marked improvement in the security of transfers initiated by businesses and public authorities through telematic channels observed in 2022 continued in 2023, with the fraud rate stabilising at 0.0002% (down from 0.0006% in 2021).

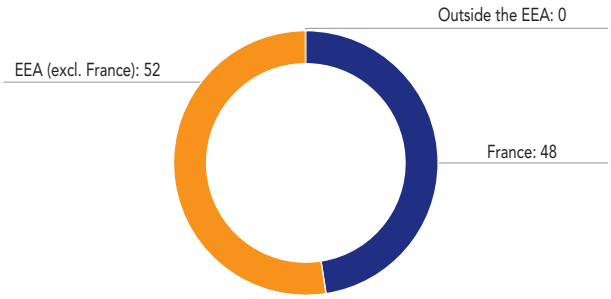
Transfer fraud methods continue to evolve. Fraudsters make greater use of accounts opened in France to retrieve their funds, even though European transfers are proportionally three times more defrauded than French domestic transfers. Moreover, fraudsters increasingly use both phishing techniques, to gain access to online banking, and telephone manipulation techniques (known as social engineering) to convince their victims to provide sensitive data or validate a transaction.

Instant transfer fraud remained firmly in check in value terms in 2023 considering the recent growth in their use, with fraud only increasing by 31% year-on-year despite transactions increasing by 46%. Consequently, the fraud rate fell significantly by 11% compared with 2022 and remained lower than the fraud rate for payment cards (0.040% compared with 0.053%). These two payment methods are widely used by consumers, and rely on similar security mechanisms, particularly the same strong authentication solutions for online payments.

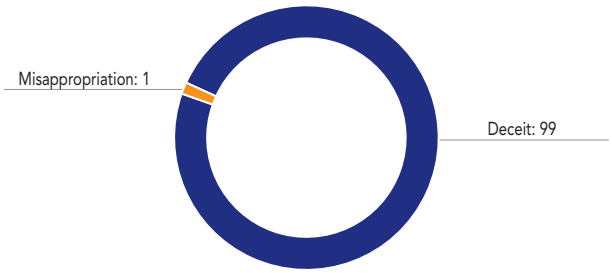
1.5 Current state of direct debit fraud

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

a) By geographical area



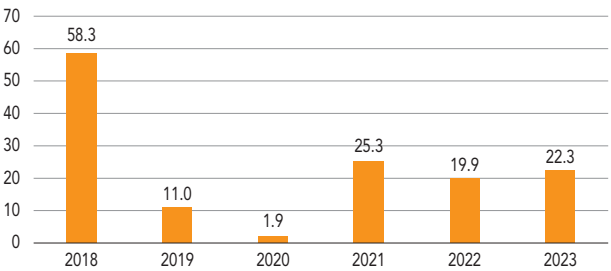
b) By type of fraud



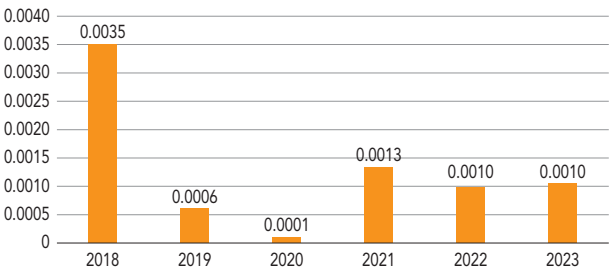
Source: Observatory for the Security of Payment Means.
Note: EEA, European Economic Area.

C31 Direct debit fraud

a) In value (EUR millions)



b) Rate (%)



Source: Observatory for the Security of Payment Means.

Direct debit fraud continues to fluctuate sharply from one year to the next. In 2023, it rose slightly in value terms to EUR 22.3 million (compared with EUR 20 million in 2022), while the fraud rate stabilised at 0.0010%. The fraud is perpetrated almost exclusively by fraudsters issuing fake orders, without having a direct debit order or an economic relationship with the victim.

The Observatory notes two notable changes compared to 2022:

- first, the fraud recorded by creditors' institutions only involved accounts opened in the European Economic Area (48% in France and 52% abroad), whereas in 2022, 94% of fraud was carried out via accounts opened in France;
- second, misappropriation fraud, where the fraudster usurps the identity and international bank account number (IBAN) of a third party to sign a direct debit order, fell sharply in 2023 to 1% of the total value defrauded, compared with 28% in 2022.

BOX

❶

Indicators, lessons and recommendations from the French Ministry of the Interior on payment means fraud in 2023

The French Ministry of the Interior is represented on the Observatory by the *Gendarmerie Nationale*'s cyber unit and the police's *Direction nationale de la police judiciaire* (DNPJ – the national directorate of judicial police). In 2023, as they do every year, these two bodies reported their main observations on payment means fraud to the Observatory.

1. Ministry of the Interior statistical study on fraud: a much broader scope than that of the OSMP, but with consistent and complementary findings

In 2023, the French Ministry of the Interior revised the methodology used for its statistical publications. The new method of tracking offences groups together payment means scams and fraud without distinction in order to maintain data consistency. Due to different coding practices between registration services, it is impossible to precisely distinguish payment means fraud data, as defined by the OSMP, from among the scams.

For the first time, on 10 July 2024, the *Service statistique ministériel de la sécurité intérieure* (SSMSI – the French ministerial statistical service for internal security) published a special study on scams reported to the security services.[1] It showed that fraud-related offences reported to the national police and *gendarmerie* services increased steadily from 2016 to 2023, and that among the offences recorded were certain types of payment means fraud. In 2023, the national police and *gendarmerie* services documented 411,700 victims of payment means fraud and scams – with total losses incurred by individuals estimated at EUR 4.5 billion[2] in 2023[3] – a 7.3% average annual increase since 2016 (up 64% over the seven-year period).

The SSMSI methodology for recording payment means fraud – which is now systematically aggregated with other scams – differs significantly from that of the Observatory. By grouping payment means 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 payment means fraud by the OSMP. Furthermore, the SSMSI calculates the number of victims[4] on the basis of complaints filed with the national police and *gendarmerie* services, whereas the OSMP tallies the fraudulent transactions reported by payment service providers and card payment networks. 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.[5] The OSMP, on the other hand, takes the precise fraudulent transaction amounts reported by the institutions concerned. These differences in methodology and scope mean that it is impossible to reconcile the data published by the SSMSI and the figures published by the Observatory.

Nonetheless, the SSMSI study confirms certain trends in **payment means fraud observed by the Observatory. We thus see that payment means fraud is increasingly based on the manipulation of victims (e.g. false bank adviser scams, CEO fraud, bank account details fraud, etc.), and that, in terms of incident numbers,**

1 *Service statistique ministériel de la sécurité intérieure* (SSMSI), "*Les escroqueries enregistrées par les services de sécurité entre 2016 et 2023*", *Interstats Analyse*, No. 68, July 2024 (in French only).

2 The estimated EUR 4.5 billion in losses suffered by individuals who are victims of payment means fraud includes offences reported to the French police and *gendarmerie*, as well as offences that went unreported. These unreported offences are estimated by the Ministry of the Interior's annual "*Cadre de vie et sécurité*" (security and living conditions) surveys, also known as "victimisation" surveys.

3 In its study published on 10 July 2024, the SSMSI estimated that the reported loss suffered by organisations that were victims of payment means fraud ranged from EUR 600 million to EUR 800 million over the seven-year period from 2016 to 2023.

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

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

it affects individuals more than organisations. According to the SSMSI study, 8.7% of victims of fraud were organisations, down from 16.1% in 2016.

The study also gave an insight into the profile of individual victims. According to the study, **young adults (25 to 34 years old) most frequently file complaints**, accounting for 17% of reported fraud but only 11% of the population. The profile of offenders has changed very little since 2016, with 31% aged 15 to 24, and 26% aged 25 to 34.

2. Focus on the Perceval and Thésée platforms (to report payment card fraud and to file fraud complaints online, respectively)

Since 2018, the *Gendarmerie*'s Perceval platform has been used to collect reports from users of the fraudulent use of payment cards on the internet. Its data can be more easily reconciled with the trends observed by the Observatory. There were 259,094 cases filed in 2023 (down 15% from 304,923 in 2022) with total losses of EUR 155 million (a 4% decrease compared with EUR 161 million in 2022). Each incident thus led to an average loss of EUR 598 (compared with EUR 529 in 2022, up 12%). It should be noted that one case reported on the Perceval platform may cover several different fraudulent transactions initiated using the same stolen card details.

A comparison with the Observatory's statistics shows that the number of frauds reported on Perceval was down in 2023. Only 44% of the card fraud on internet payments as quantified by the Observatory was reported on Perceval compared with 51% in 2022. Victims tend to report only the largest frauds: in 2023, the average value of a fraudulent transaction, according to the Observatory's statistics, was EUR 64, compared with EUR 150 according to Perceval (EUR 598 per complaint filed, which tend to include an average of almost four transactions).

The **Thésée platform** was launched in March 2022 and is managed by the *Office anticybercriminalité* (OFAC – the French national police's anti cybercrime office). It allows individual victims of internet scams and frauds to lodge a complaint online.[6] In 2023, 59,500 payment means fraud and scam complaints were made on the Thésée platform. This represents 14.5% of the total number of victims of payment means fraud and scams recorded by the SSMSI (up from 11.4% in 2022).

The Observatory would like to stress the importance of declaring fraud on the Perceval and Thésée platforms. The declarations are useful to law enforcement agencies, enabling them to gather the information they need to dismantle fraud networks.

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.

Figures from the *Groupement des cartes bancaires* (France's national interbank network) show a drastic fall in skimming over the last few years (see Chart). In 2023, only three attacks were reported for a total loss of EUR 19,563 (a drop of 90% compared with losses of EUR 192,540 in 2022). All three attacks targeted

6 Filing a complaint online via the Thésée platform eliminates the need to do so in person at a police station or *gendarmerie*. The data from the Thésée platform are factored into the estimation of the number of victims of payment means fraud reported by the SSMSI in its study published on 10 July 2024.

7 A skimmer is a device that slides discretely into the slot of an ATM while leaving enough space for a bankcard to be inserted. The device then copies the data stored on the magnetic stripe, without interfering with the bankcard transaction.

automatic fuel dispensers (AFDs), compared with 17 in 2022. There were no attacks on automated teller machines (ATMs). In 2022, there were three. These trends mirror those reported to the Observatory by payment industry operators.

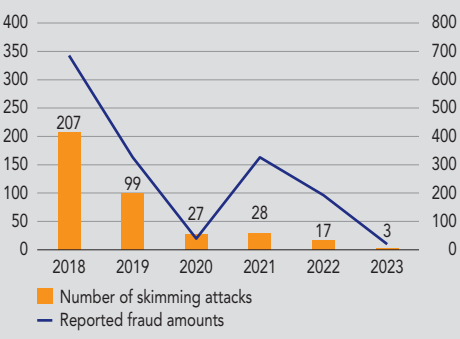
Nevertheless, service station managers, like ATM managers, must stay on their guard to prevent attempts to replace legitimate payment terminals with compromised terminals, or to install fraudulent external devices such as readers, cameras or keypads.

Shimming[8] relies on similar techniques to skimming, but targets the data stored in the card's chip. The technical complexity involved means that attacks remain limited. Total financial losses from shimming amounted to EUR 36,000 in 2023, down from EUR 50,000 in 2022.

4. Fake bank transfer orders: stable overall, but still needs to be watched by public authorities

According to law enforcement agencies, fake bank transfer order scams are a form of financial fraud in which the victim is coerced into making a transfer to a bank account managed by the perpetrator that he or she believes to be legitimate. The fraudsters usually operate by telephone or e-mail and use social engineering techniques to exploit the human and organisational vulnerabilities of their victims to push them to make fraudulent transfers. Companies and public authorities are mainly affected but individuals can also be targeted.

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



Sources: Groupement des cartes bancaires *(France's national interbank network).*

There are two main methods.

- Bank account details fraud: fraudsters impersonate a target's supplier and falsely tell them that there has been a change in the bank account details that they should use to pay their bills, thus diverting the payment into their own accounts.[9]

- 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, insisting it has to be done **urgently** and in strict **confidentiality**.

The health crisis in 2020, and the widespread introduction of teleworking and the pressing need to make certain payments more rapidly that came with it, led to a sharp rise in cases, as the rapid development of new operating and organisational methods enabled perpetrators to exploit new vulnerabilities.

The **number of incidents has remained high** since the end of the crisis, but **overall losses have declined**. This trend can be explained by the **increase in the number of frauds targeting public authorities**, which generally involve smaller individual amounts.

In 2023, 635 cases against organisations alone were reported to France's national directorate of judicial police (DNPJ) with losses totalling EUR 48 million (compared with 537 cases in 2022 and losses of EUR 68 million).[10]

These developments are consistent with the general trends reported to the Observatory by payment industry players: bank transfer fraud by misappropriation is tending to stabilise in value terms (up 1% year-on-year in 2023), while increasing in volume (up 47%).

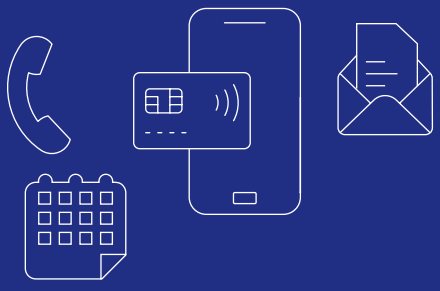
8 A similar device to a skimmer in that it is incorporated into a machine or dispenser, but which intercepts data – including the PIN code – from the bankcard's chip.

9 The legal and accounting professions are also targeted. For example, in the case of a notary's office, the fraudster may claim to represent the office that is to be paid for the purchase of a property, or impersonate the person entitled to the proceeds of the sale.

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

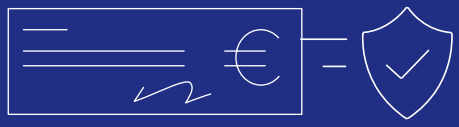
CHAPTER 2
SUMMARY OF THE WORK CARRIED OUT BY THE OBSERVATORY

Recommendations to enhance credit transfer and direct debit security, particularly new measures to raise user awareness and the development of mechanisms for information sharing between payment service providers



Adoption of an **action plan to combat fraud on unsecured remote card payments**, particularly by restricting acceptance of post or telephone payments, recurring payments or payments in instalments without authentication

Work alongside operators in the telecommunications industry to **combat spoofing attacks** (usurping another person's identity) **using communications networks**, particularly by developing a caller number authentication system and protecting SMS sender identifiers



Efforts demanded of banks to **step up the security of chequebook shipment and delivery and to make it easier to report loss or theft**

2

WORK CARRIED OUT BY THE OBSERVATORY ON FRAUD PREVENTION

Section 2.1 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-2023

2.2 Measures to prevent fraud on non-3-D Secure remote card payments

2.2.1 Background

Directive (EU) No. 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services, known as PSD 2[24] and transposed into French law in the *Code monétaire et financier* (the French Monetary and Financial Code),[25] stipulates the use of strong customer authentication for electronic payments as well as for transactions carried out using a remote means of communication with a high risk of fraud.[26] However, Delegated Regulation (EU) No. 2018/389 of the European Commission of 27 November 2017 (or RTS, regulatory technical standard) provides for exemptions,[27] particularly with regard to transactions carried out in favour of trusted beneficiaries, recurring transactions, low-value transactions or transactions that carry a low level of risk.

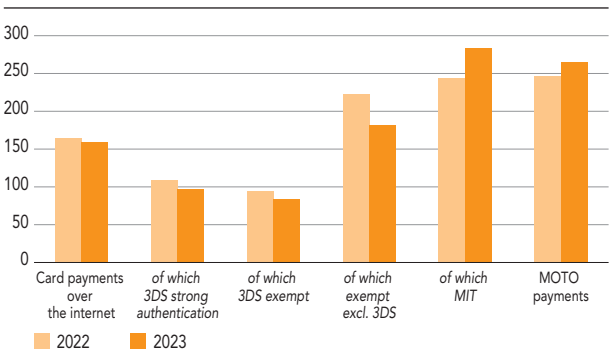
In France, strong authentication for remote payments made by bankcard has been gradually implemented as part of the migration plan adopted by the Observatory.[28]

This was made possible by the rollout of 3-D Secure 2.0, which processes transactions between merchants, cardholders and their payment service providers (PSPs) to authenticate payments over the internet. With 3-D Secure 2.0, remote payment strong authentication is possible using the various solutions that card-issuing PSPs currently make available to cardholders. Requests for exemption from strong authentication can also be processed.

The introduction of 3-D Secure strong customer authentication for remote payments has brought down the rate of fraud, which now appears to be in check for all payments concerned, including those exempted from strong authentication *(see chart)*.

However, the fraud rate is still structurally higher for non-3-D Secure remote payments, including MITs (Merchant Initiated Transactions) and MOTO (Mail Order, Telephone Order) payments.

Card payment fraud rate, 2022-2023 (%)



Source: Observatory for the Security of Payment Means.
3DS, 3-D Secure; MIT, Merchant Initiated Transaction; MOTO, Mail Order, Telephone Order.
Notes: The fraud rate corresponds to the amount of fraud in euro per EUR 100,000 of payments. MOTO payments are non-internet remote payments made by letter or email, or by telephone or fax.

As these payments require no authentication when they are issued, they are naturally far more exposed to fraud than payments made using the 3-D Secure protocol:

- Non-3-D Secure payments may be initiated by any person able to read the data on a bankcard (number and expiration date for MOTO payments, plus the card security code for MIT payments), without that person having to possess the card or to have access to the remote payment strong authentication system.
- Specifically, a merchant could transmit payment requests to a cardholder's PSP that do not correspond to any delivered product or service, for example by reusing payment card data previously used in legitimate transactions.
- MOTO payments in particular require the paying customer to provide their bankcard number and expiration date via an unsecured channel (telephone, email, letter, fax, etc.), which are then processed by an operator who enters the information on the merchant's payment terminal. This is fertile ground for internal or external fraud through the misappropriation of payment data.

While current technical solutions can theoretically enable strong authentication for MOTO payments, this functionality is not used in practice and no standardised method for their authentication has been identified to date.

Moreover, MOTO payments and non-3-D Secure internet payments are sometimes redirected from their original purpose so that merchants can accept Customer Initiated Transactions (CITs), thereby bypassing the strong authentication requirement imposed by PSD 2.

Based on these findings, the Observatory has made recommendations aimed at preventing fraud on remote payments made outside the 3-D Secure protocol.

2.2.2 Scope of the recommendations

These recommendations apply to all remote payments made without strong customer authentication and carried out outside the 3-D Secure solution, namely:

- MOTO payments;
- non-3-D Secure payments over the internet, including MITs (for which 3-D Secure strong authentication is only applied at the time the mandate is validated), and DTA – direct to authorisation – payments (CIT payments requesting exemption from passage through the 3-D Secure protocol).

By way of exception, these recommendations do not apply to:

- non-3-D Secure payments over the internet recognised as strong-authenticated by the issuing PSP, such as payments made using a mobile wallet[29] application incorporating a strong authentication solution that the card-issuing PSP recognises as PSD 2-compliant;
- electronic payments initiated by organisations using dedicated payment procedures or protocols made available to non-consumer payers only, where the competent authorities are satisfied that the procedures and protocols in place guarantee at least equivalent PSD 2-levels of security;[30]
- payments for which the acquiring PSP is located in a state that is not a party to the Agreement on the European Economic Area.

These recommendations are intended for implementation by merchants who accept payments within the above scope, by their technical acceptance service providers, by the various card schemes and by all issuing and acquiring PSPs.

2.2.3 Recommendations for non-3-D Secure remote payments

2.2.3.1 The use of MOTO payments and non-3-D Secure payments over the internet, strictly when no other payment method is possible

The high fraud rate for these payments means that MOTO payments and non-3-D Secure payments over the internet (other than those the issuing PSP recognises as authenticated, for example, when using a wallet solution) should be strictly restricted to their intended uses.

Internet payments that qualify for exemption from strong authentication, in particular, are expected to be processed through 3-D Secure. This protocol facilitates the management of exemption requests, and means that customers are asked for strong authentication when the exemption request is blocked by a soft decline.

24 Directive (EU) No. 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

25 Article L. 133-1 et seq.

26 Article L. 133-4 I of the French Monetary and Financial Code.

27 Articles 11 to 18 of Regulation (EU) No. 2018/389.

28 Chapter 1 of the *Annual Report of the Observatory for the Security of Payment Means*, 2018.

29 A wallet is an online payment tool that securely stores digital versions of the wallet owner's payment cards.

30 These payments are exempt from the strong authentication requirement pursuant to Article 17 of Regulation (EU) No. 2018/389.

Recommendation 1:

Restricting MOTO and MIT payments to cases where no other payment method is possible

Merchants should take care:

- to only accept MOTO (Mail Order, Telephone Order) card payments for contracts taken out remotely via a non-internet channel (telephone, letter, etc.) and to use a point-of-sale payment or a secure Internet payment whenever the nature of the contract, its terms and conditions and the delivery of the ordered goods or services ordered allow (for example, face-to-face payment for goods ordered by telephone and delivered directly by the retailer);
- to only accept 3-D Secure payments over the internet, except in cases where the issuer recognises the payment as authenticated (for example, via a wallet application that incorporates a strong authentication solution) and in cases where 3-D Secure cannot be used, such as Merchant Initiated Transaction (MIT) payments.

Specifically, merchants must never accept payments – other than 3-D Secure and MOTO transactions – when the payment is for a Customer Initiated Transaction (CIT) and is made over the internet.

Technical acceptance service providers and acquiring payment service providers should ensure that merchants with whom they have a payment acceptance contract comply with this recommendation.

2.2.3.2 Valid chaining for MIT payments

Using the 3-D Secure protocol for all Customer Initiated Transactions (CITs) over the internet should mean that non-3-D Secure internet payments other than those the issuing PSP recognises as authenticated (for example, via a wallet application that incorporates a strong authentication solution) should only be Merchant Initiated Transactions (MITs).

All MIT payments must have a valid chaining reference that enables the card issuer to check the cardholder's consent to the payment presented, or, when handling a complaint lodged by the cardholder, to cross-check payment with a previously strong-authenticated mandate.

While issuing PSPs are able to detect whether a chaining reference is absent at the time of payment acceptance, they cannot check that said reference is valid (that it corresponds to prior authentication) in real time. Therefore, invalid chaining references (that do not correspond to a strong customer-authenticated payment mandate), can only be detected by carrying out a check after-the-fact, which the Observatory invites issuing PSPs to gradually put into place.

Recommendation 2:

Valid chaining for MITs

When any MIT payment is issued, merchants send the chaining reference from the strong-authenticated mandate that authorises the payment to their PSP.

Issuing PSPs are invited:

- to gradually implement a mechanism to cross-check MIT payment chaining references to strong-authenticated payment orders;
- to alert merchants and technical acceptance service providers to any anomalies found in the chaining references in the MIT transactions issued, so that they can implement a remedial action plan;
- failing corrective measures, to apply the velocity limit defined in recommendation 3 to MIT payments submitted by merchants and/or technical acceptance service providers connected with invalid chaining references.

2.2.3.3 Velocity limits for MOTO payments and non-3-D Secure payments over the internet

In order to prevent fraud on MOTO payments and non-3-D Secure payments over the internet (except in cases where the issuer recognises the payment as authenticated, for example, via a wallet application that incorporates a strong authentication solution), velocity – the cumulative amount of purchases made with the same card from the same merchant over a rolling 24-hour period – must be limited.

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

Velocity is measured in two distinct ways for MOTO payments on the one hand and non-3-D Secure payments over the internet on the other.

The Observatory invites issuing PSPs to reject any transactions that exceed this limit, by a soft decline when allowed by the transaction type.

Velocity limits do not apply to:

- sectors of activity (included in the "exclusions list" set down in Box 6) that appear to justifiably use MOTO or MIT payments and that keep their fraud rates in check;
- MIT payments associated with a technically valid chaining reference and merchants and technical acceptance service providers that have not been found to have previously issued payments with anomalous chaining references.

In addition, exemptions may be granted individually, depending on the fraud rate observed for each retailer.[31]

Conversely, an issuing PSP may decide to revoke the exemption for as long as it chooses for a retailer whose Merchant Category Code (MCC) appears on the exclusions list, but which makes inappropriate use of MOTO payments or non-3-D Secure payments over the internet, or which has an associated fraud rate that the issuing PSP deems unacceptable.

The implementation of velocity limits will be supervised by a steering committee under the aegis of the Observatory's "strong authentication" working group.

Recommendation 3:

Velocity limits and implementation of a soft decline mechanism

Issuing PSPs reject, by a soft decline where possible, MOTO payments and non-3-D Secure payments over the internet not recognised as strong-authenticated by the issuer, when the amount of a payment would lead to the velocity limits defined in this recommendation being exceeded.

The velocity limit over a rolling 24-hour period is set at:

- EUR 500 for 10 June 2024 to 8 September 2024;
- EUR 250 from 9 September 2024 to 13 October 2024;
- EUR 100 from 14 October 2024.

Reducing the thresholds to EUR 250 and EUR 100 will depend on the Observatory's dedicated working group's judgement of the market's capacity to adapt.

Velocity is measured in two distinct ways for:

- MOTO payments on the one hand; and
- non-3-D Secure payments over the internet on the other. For this category of payment, the velocity measurement does not take into account CIT payments authenticated by the issuer (particularly by a mobile wallet solution) or MIT payments with a valid chaining reference.

This recommendation does not apply to:

- payments accepted by merchants who benefit from an exemption (for the type of payment involved) granted under the conditions set down in Box 6, unless the issuing PSP has revoked the exemption for the merchant concerned;
- MIT payments with a valid chaining reference;
- strong-authenticated MOTO payments.

The steering committee will be responsible for:

- checking that all legitimate cases of MOTO payments and non-3-D Secure payments over the internet have been taken into account and that applying the velocity limits does not lead to legitimate transactions being rejected;
- proposing any adjustments necessary to the implementation of this recommendation, particularly amendments to the list of activities excluded from its scope or modifications to the timetable and conditions for the second and third phases.

2.2.3.4 Security of payment data transmitted during MOTO transactions

Merchants that accept MOTO payments must take extreme care to ensure the security of the payment data they receive in order to prevent misappropriation.

In the case of telephone orders, using a computerised telephone system eliminates the need for a human operator to handle the data: paying customers enter their payment details directly on the keypad of their dual-tone multi-frequency (DTMF) phones (whether a landline, mobile or smartphone), which are then automatically transmitted to the payment terminal for processing.

Depending on the circumstances, customers may either (i) be connected directly to an interactive voice response system (for example, entering an invoice number before entering the payment details to settle an invoice), or (ii) be placed in contact with an operator to whom they specify the type of goods or services they wish to order before being transferred to an interactive voice response system to make payment, or entering the payment details on a DTMF keypad during the conversation with the operator.

Recommendation 4:

Enhancing the security of payment data

Merchants that accept MOTO payments should take care to ensure the security of the payment details provided by customers. As much as possible, merchants that accept telephone orders should ensure that customers communicate their payment details via an automatic system or by direct entry on a telephone keypad rather than verbally to an operator.

Acquiring payment service providers should ensure that merchants with whom they have a payment acceptance contract comply with this recommendation.

31 When a card payment is issued, a merchant is identified by the entry in the Merchant ID field included in the payment data.

2.2.3.5 Trialling MOTO payment authentication

Implementing the simplest of authentication mechanisms, even with only one authentication factor, would improve the level of security of MOTO payments, as they are not currently subject to any formal verification.

In some cases, existing systems could be used. For example, a one-time password received by SMS could be used or, for cardholders enrolled in a strong authentication solution via a mobile wallet application recognised by their PSP, payments made by telephone could be authenticated using the app.

However, some strong authentication solutions designed for payments over the internet would appear to be incompatible with payments by telephone, which cannot accept alphanumeric passwords. The type of customers who make payments by telephone must also be taken into consideration: often they have neither internet access nor a mobile phone.

Recommendation 5:

Trialling MOTO payment authentication

The Observatory encourages merchants and payment service providers (PSPs) to suggest authentication solutions for MOTO payments adapted to each payment initiation channel and to each type of customer concerned.

2.3 Work with telecommunications operators

2.3.1 Background

Following the introduction of strong authentication solutions and risk scoring for individual transactions, driven by the second European Payment Services Directive (PSD 2), **fraudsters have adapted and have developed social engineering attack techniques**. False bank advisers scams, for example, are perpetrated by fraudsters that either coerce victims into validating fraudulent transactions themselves, or misappropriate strong authentication tools to carry out fraudulent transactions directly.

Fraudsters rely on a host of techniques to hijack telecommunications tools and infrastructures, particularly:

- phishing or smishing – spoofing identifiers to send a legitimate-looking electronic messages or SMS and creating mirror sites that duplicate legitimate sites to then obtain customers' personal data;
- spoofing – hijacking caller numbers to deceive the targeted contact as to the origin of the call received (for example, by displaying the number of a bank adviser, a bank switchboard or a bank's card blocking service);
- SIM swapping – duplicating a victim's SIM card and thus enabling the fraudster to receive SMS messages with authentication information in the victim's stead.

Drawing on its recent enhanced collaboration and dialogue with the telecommunications sector, the Observatory is now working to identify ways to curb fraudsters' use of these techniques. The Observatory has opted for a concerted approach, with the creation of a working group with representatives from payment service providers (PSPs), the main telephone operators, and the various authorities concerned (namely, the Banque de France, the *Autorité de contrôle prudentiel et de résolution* [ACPR – the French Prudential Supervision and Resolution Authority], 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], and the French Treasury).

2.3.2 Combating spoofing: the MAN programme and other measures

The drive to combat spoofing in France revolves primarily around the implementation of the MAN (number authentication mechanism) programme, overseen by the *Association des plateformes de normalisation des flux interopérateurs* (APNF – a French association working on inter-operator flow standardisation), which comprises representatives from all telephone operators allocated numbers in the French numbering plan. The MAN programme,[32] intended to implement the requirements of Article L. 44 IV of the *Code des postes et des communications électroniques* (the French postal and electronic communications code) pursuant to the "Naegelen" law,[33] involves two distinct phases.

- First, the rollout of a common technical infrastructure to enable operators to authenticate telephone calls. The infrastructure and the connectivity required for all operators was fully implemented on 1 June 2024. The authentication is certificate-based, using digital certificates to guarantee that a call is indeed coming from the line associated with the presented calling number.
- Second, disconnection, with the routing of unauthenticated calls interrupted as from 1 October 2024. Due to the continuity required during the Paris Olympic Games, operators chose not to cut off unauthenticated calls until after the summer of 2024.

While Arcep is responsible for monitoring compliance with the Naegelen law, the Observatory is paying particular attention to the MAN programme's implementation timetable due to the consequences of spoofing on payment means fraud. The Observatory will also work to identify fraud scenarios that are likely to emerge during the rollout of the MAN programme as fraudsters seek to adapt to the new conditions. It will also ensure the prompt reactivity of all the players involved in order to prevent operator non-compliance or any phenomena associated with delayed fraudulent activities.

Alongside its monitoring of the MAN programme's implementation, at the request of PSPs, the Observatory has initiated a review of measures to support the fight against spoofing. These measures should focus on the protection of particularly high-risk telephone numbers, such as those dedicated to blocking lost or stolen bankcards.

The new measures could be based on a Do Not Originate (DNO) mechanism, by which operators stop calls made from a number reserved exclusively for inbound calls. Each PSP would be responsible for identifying the numbers it uses for inbound calls only and for providing their DNO lists to the telephone operators.

A study is currently underway to identify the DNO numbers of all the PSPs concerned, and to measure the volume of calls made from them. Their use for presumed fraudulent purposes can then be quantified.

2.3.3 Combating smishing: protecting Originator Address Codes (OAdCs)

"SMS phishing", contracted to "smishing", used to steer victims towards fake sites or phone numbers, is all the more effective when (i) the fraudulent SMS has an Originator Address Code (OAdC) as the sender (i.e. an 11-character alphanumeric code rather than a number starting with 06 or 07), and (ii) the OAdC makes the person receiving the SMS believe that it has come from a legitimate sender (a bank or public utility company, for example), in the same way as spoofing.

The *Association française pour le développement des services et usages Multimédias Multi-opérateurs* (AF2M – French Mobile Multimedia Association),[34] in conjunction with SMS service providers, has set up a mechanism to protect OAdCs.

- OAdCs corresponding to existing brands, businesses or public utility companies are reserved solely for their legitimate use. They can only be used with the authorisation of the registered owner.
- Using OAdCs that may give rise to confusion with an existing brand, business or public utility company is prohibited. To this end, AF2M has drawn up a blacklist of codes, whose similarity to sensitive OAdCs means that they could be deceptive. Operators are required to block any SMS messages sent from these codes.

The list of sensitive and prohibited OAdCs is updated regularly, particularly on the basis of complaints sent to the 33700 short number (the French national platform for reporting unsolicited SMS messages set up by AF2M).

As the OAdC protection mechanism is already operational, the Observatory's work focuses on potential opportunities to step up coordination between the payments sector and AF2M. This mainly deals with the management of lists of OAdCs linked to the payments sector and the procedures for reporting fraudulent SMS messages (for example, improving efficiency, raising awareness of the 33700 short number, or setting up a new reporting channel suitable for professional use).

2.3.4 Combating SIM swapping: the "SIM Verify" multi-operator API

Operators currently offer an application programming interface (API) known as "SIM Verify", which is intended to prevent line subscribers being affected by SIM swapping. SIM Verify indicates whether a SIM card has recently been renewed on a given telephone line. It is a multi-operator API and now covers almost all French mobile lines.

PSPs can therefore integrate a SIM Verify check into their fraud detection and prevention tools when they use "enhanced SMS" transaction authentication (a combination of a one-time code sent by SMS and static password). This approach is particularly effective in the case of a transaction identified as high risk and for which a recent SIM card reissue is an aggravating factor that could justify the transaction being rejected by a PSP.

32 See *https://www.fftelecoms.org/nos-travaux-et-champs-dactions/calendrier-de-mise-en-oeuvre-du-mecanisme-dauthentification-des-numeros/*

33 Article 10 of Law No. 2020-901 of 24 July 2020 to regulate telephone canvassing and combat fraudulent calls.

34 AF2M has represented the telecommunications sector on the Observatory since the OSMP's creation.

Observatory-led discussions have given operators and the AF2M the opportunity to share very positive feedback from several PSPs on this tool's effectiveness in preventing fraud in real time. Proposals to enhance the API have been submitted to the AF2M for consideration (for example, disclosing the place or timestamp of a SIM card's reissue, or taking account of inter-operator portability).

2.3.5 New avenues of exploration

Discussions organised by the Observatory have helped to identify new avenues that would enhance joint action between the payments and telecommunications sectors with a view to combating fraud more effectively:

- **Setting up a benchmark procedure to ensure optimal shutdown of the numbers of bogus call centres** operated by fraudsters, irrespective of how they are detected (by individuals, banks, or operators, for example).
- **Carrying out an opportunity study on the development of a "Scam Signal"-type API** that would enable a PSP to know whether its customer is speaking on the phone at the time of validating a payment, in order to spot the possibility of fraud by social engineering. While a solution currently exists thanks to mobile terminals' operating systems, which allow a banking application to access the information, its operability depends on the rights granted by the terminal user to the banking application. This factor obviously falls outside of a PSP's control. This type of multi-operator API, which exists notably in the United Kingdom, would have the advantage of ensuring complete coverage of all mobile users.

The Observatory's role is to act as a catalyst with regard to these new developments, ensuring the involvement of all stakeholders concerned. For example, when considering the feasibility of an API scam signal, participants were encouraged to contact their British counterparts for feedback. And with regard to shutting down bogus call centres, the Observatory would naturally involve the national police and *gendarmerie* services.

Section 2.4 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-2023

BOXES

Boxes 2, 3, 4, 5 and 6 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-2023

3

QUANTUM COMPUTING AND THE SECURITY OF BANKCARD PAYMENT SYSTEMS

The possibilities offered by quantum computing for finance, logistics, meteorology, chemistry and a host of other applications are promising. However, **a particularly problematic use case has been identified for the coming ten to twenty years: the use of quantum computing techniques to crack the encryption schemes for secure electronic communications, including those used for payments**. This poses a serious threat to national security, and as such, has already been subject to careful consideration by the public authorities (the National Security Memorandum of May 2022 in the United States, or the Military Programming Act of August 2023 in France, for example). The payments sector must immediately address this issue, and at the highest level, given the life cycles of card payment hardware and software (chips, electronic payment terminals [EPTs], servers, etc.).

Two types of algorithm guarantee the confidentiality and integrity of card payments:

- Asymmetric encryption algorithms (RSA, ECC, etc.), which are used to authenticate devices (cards, EPTs, etc.) and servers, and to exchange symmetric encryption keys, and whose level of security would be reduced to nothing with the advent of quantum computing (Shor, 1995).
- Symmetric encryption algorithms (AES, Triple-DES, etc.), which are used to encrypt cold data and data in use and whose level of security (expressed in bits) would be halved (Grover, 1996).

This study aims to map the main algorithms used in the card payment system and analyse their exposure to the risks posed by the "quantum threat". Without measures to develop the resilience of the encryption and signature algorithms of card payment systems and thus enhance their resistance to the processing power of future quantum computers, the most significant risks in the long term are:

- The theft of private and even confidential data from hacked merchants, raising issues for security and economic intelligence.
- Fraudulent payments generated by the manufacture of Yes Cards for "offline" payments.
- A loss of confidence in payment infrastructures, as card schemes and issuing banks would no longer be in control of their payment card certification policy – every time a high-level encryption key is cracked, large numbers of cards would have to be recalled and reissued.
- The simple fact of the public becoming conscious of the risks, which could trigger a widespread crisis of confidence, threatening economic stability.

Our study shows that technical solutions exist. However, implementing them – in the case of asymmetric algorithms – will not be a trivial affair. The OSMP therefore recommends that payment industry operators immediately:

- **inventory** of the various security measures in place in their information systems;
- **rank** data according to their sensitivity;
- **pilot** the implementation of asymmetric algorithms based on hybrid and crypto-agile solutions;
- **draw up** a roadmap with high-level validation;
- **inform** the standardisation authorities that define payment protocol security, so they can agree on hybridisation and crypto-agility options and set milestones;
- **work** towards the creation of a permanent high-level working group, ideally at European level, manned by the major payment institutions and public supervisory and standardisation authorities.

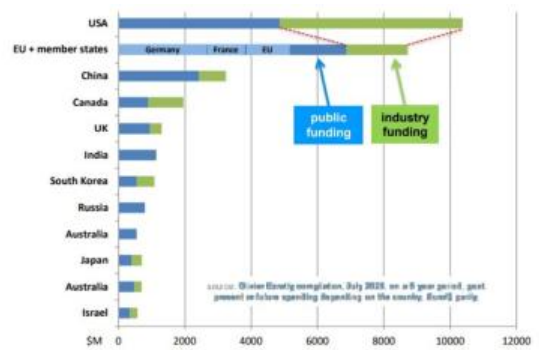
3.1 Introduction

Many scientific fields will benefit from the technological advances that quantum computing will offer. But quantum computing could also undermine the security of information systems if encrypted data are not adequately protected. The purpose of this chapter is to lay the groundwork for an assessment of the risks that progress in quantum computing and its decryption capabilities could pose to the electronic payment industry.

The principle of the quantum computer, first suggested by Richard Feynman in 1982, is based on the laws of quantum mechanics. Notably, the principle of quantum superposition of states means that a bit, which in conventional computing takes a Boolean data type of 0 or 1, can be replaced by the notion of a qubit (a "quantum bit"), the value of which is comparable to a type of probability of being 0 or 1. Qubits are manipulated by quantum operators known as quantum gates. Their simulation and the maximisation of resimulations exponentially increase the efficiency of optimisation calculations, which can be found in fields as varied as meteorology, biochemistry, finance, logistics and so on.

However, quantum computing is still in its infancy. Currently operational quantum computers offer only a limited number of qubits and are exposed to a non-negligible probability of error, due both to the very principles of quantum physics and to the problems of controlling the environment of the machine, which must remain completely isolated from any external influence. Numerous avenues of technological development are being explored, including the applications of superconducting circuits, ultracold atoms and silicon. IT manufacturers and hundreds of start-ups, particularly in France, have entered the race, competing directly with GAFAM.[1] Since 2020, private investment in start-ups worldwide has soared to over USD 2 billion in the past two years. At the same time, government bodies in all developed countries – ledl by the United States, but also China, India and Russia – have launched massive investment programmes to support the development of quantum technologies. In 2021, the French government, too, drew up an investment plan worth EUR 1.8 billion over five years.

C1 Consolidated public and private investment in quantum computing research over the past five years
(USD millions)



Source: Olivier Ezratty (speaker, lecturer, government advisor on quantum technologies and author of Understanding Quantum Computing, November 2018).
Notes: Consolidation of public and industry funding; despite the already extremely broad scope, there is no guarantee that it is completely exhaustive. July 2023, past, present and future expenditure, depending on the country, over a five-year period. EU + member states: European Union + Member States.

While the development of quantum computing offers very encouraging possibilities for the future, one specific use case could compromise the security of information systems, possibly as early as 2030: the decryption of the keys to encryption algorithms. Hackers could use this technology to crack the encryption on all current electronic communications, or to usurp a person's identity after decoding the secret key to his or her electronic signature. This risk is referred to as the "quantum threat".

There are two main families of encryption algorithms:

- symmetric algorithms, based on the exchange of a secret key known only to the communicants in an information exchange;
- asymmetric algorithms, based on paired private and public keys, where the private key is secret but the public key, calculated from the first, can be shared freely *(see Section 2 below)*.

In both cases, the more bits in the key, the more difficult it is to decipher.

The strength and security of the encryption depends:

- in the case of symmetric algorithms, on the security of the key exchange procedure and the difficulty involved in identifying the secret key from a ciphertext;
- in the case of asymmetric algorithms, on the difficulty involved in identifying the private key, either from a public key or from a ciphertext.

These algorithms are used extensively in the initiation of all secure communications (such as electronic signatures, SSL and TLS internet connections or corporate VPNs)[2] but their vulnerability to the quantum threat differs.

In 1995, the mathematician Peter Shor[3] demonstrated that a sufficiently powerful quantum computer could radically simplify the mathematical computations underpinning

current asymmetric cryptography: the time needed to work out the encryption key could be reduced from several years to a few hours.

Therefore, only the replacement of current algorithms with new algorithms based on different mathematical computations would offer a satisfactory level of security.

The following year, another mathematician, Lov Grover,[4] demonstrated that the complexity of an exhaustive attack on symmetric key-encryption could be substantially reduced. However, experts agreed that doubling the size of keys would be enough to contain any threat in the medium term.[5]

Electronic payments have developed considerably over the past few decades, notably due to the proliferation of online retailing. Securing communications in the payment chain plays an essential role in protecting sensitive data and user confidence. The two main payment means used by individuals are bankcards and transfers, accounting for 60% and 17%, respectively, of cashless transactions[6] in volume terms in 2022. Encryption algorithms are widely used to guarantee authentication by senders and recipients, and to ensure the confidentiality of transaction data, such as personal identification numbers (PINs).

According to experts, weaker security for this type of data could give rise to three major risks:

- **"harvest now, decrypt later"**: acquiring and storing highly sensitive encrypted data and communications (relating to national security, for example) awaiting decryption technology that would render it readable in the future;
- **identity theft**: over time, any organisation with a sufficiently powerful quantum computer could impersonate a legitimate business, particularly with the intention of cheating victims of money, thereby creating significant reputational risks;
- **a crisis of confidence**: as the general public becomes more aware of the risks associated with the quantum threat, a widespread crisis of confidence could rapidly bring payment transactions to a halt, threatening economic stability.

It is thus becoming imperative to precisely assess the true risk posed by advances in quantum computing to the security of electronic payment systems. But doing so is a colossal task. This study focuses on the most commonly used means of everyday payment in France: the bankcard. In the interests of brevity and clarity, mobile point-of-sale payments and clearing are excluded from its scope.

3.2 The main encryption algorithms and associated security arrangements

The aim of this chapter is to present an overview of the fundamental principles of cryptography, which structure the security of communication systems and therefore of the payments industry.

3.2.1 Traditional symmetric (secret key) and asymmetric (public-private key pair) encryption algorithms

3.2.1.1 The principle of symmetric encryption

Security in symmetric cryptography hinges on the confidentiality of a key known only to legitimate users. A symmetric encryption mechanism uses a secret key **K** to encrypt a plaintext message **M** into a ciphertext **C**. Access to ciphertext **C** (over a public communication channel, for example) without access to secret key **K** leaves message **M** encrypted and therefore unreadable. Key **K** can be used to decrypt **C** in order to reveal **M**.

Symmetric encryption algorithms are designed to deter attacks by making them complex and time-consuming. Without the secret key **K**, the most effective method for cracking encrypted data is still "brute force", an exhaustive attack that involves systematically trying as many different keys as possible until the correct one is found.

Algorithms are therefore designed in such a way that the number of keys to be tested is so large that a conventional computer could not carry out an exhaustive attack.

For a given key length, the "work factor" (the effort required to carry out a brute-force attack) can be quantified on the basis of processing power, memory, energy and cost. The work factor involved for a sufficiently long secret key means that a brute force attack would be impractical given the number of attempts that would fail.

1 GAFAM is the acronym for the web giants, Google, Apple, Facebook, Amazon and Microsoft, five major American companies that dominate the digital market.

2 SSL, Secure Sockets Layer, a protocol for encrypting data traffic between a browser and a website. TLS, Transport Layer Security, is the equivalent of SSL, but uses more advanced encryption algorithms. VPN, Virtual Private Network, is a secure connection protocol, but which also authenticates the legitimacy of users connecting to the site.

3 See *https://arxiv.org/abs/quant-ph/9508027*

4 See "A fast quantum mechanical algorithm for database search", *Proceedings*, 28th Annual ACM Symposium on the Theory of Computing, May 1996, p. 212.

5 Another possibility is to increase the size of the hash functions by 3/2.

6 Excluding cash transactions.

However, quantum computing, with its vastly increased processing power, could considerably reduce the effort required, to such an extent that in principle it would be the same as halving the length of the key used (i.e. a square-root reduction in the number of keys to be tried).

For example, for a given key length with 100,000,000 possible encryptions to try, halving the key length would leave a residual work factor equivalent to only 10,000 possibilities.

The most frequently used symmetric algorithms are AES[7] and Triple-DES[8] *(see Diagram 1).*

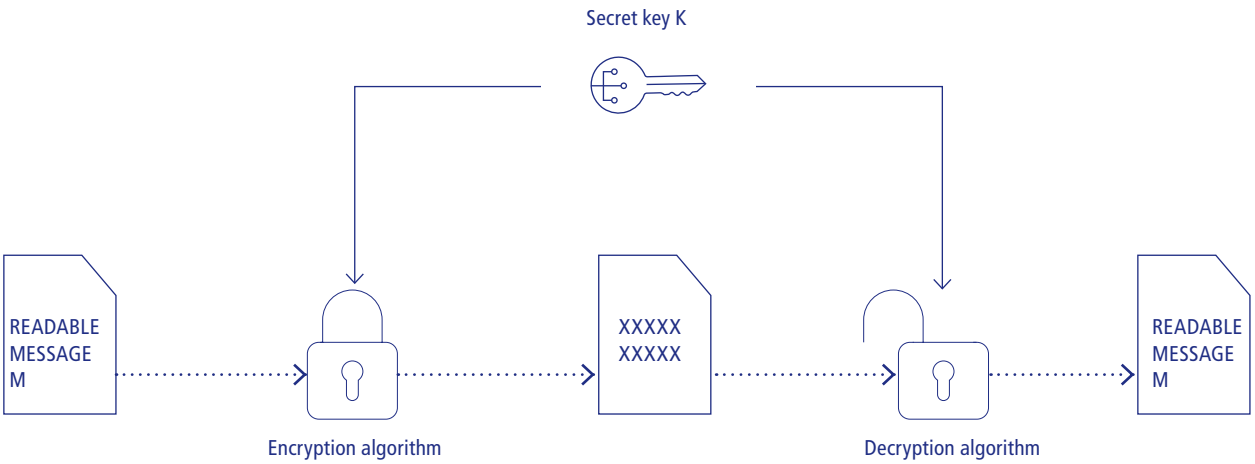
3.2.1.2 The principle of asymmetric encryption

Asymmetric encryption is based on the pairing of a public key and a private key. Normal practice is to make public key **Pu** known to a specific group of people, singled out on the basis of their potential need to communicate with the user of private key **Pr**. The private key **Pr**, meanwhile, is only known to a single, clearly identified user.

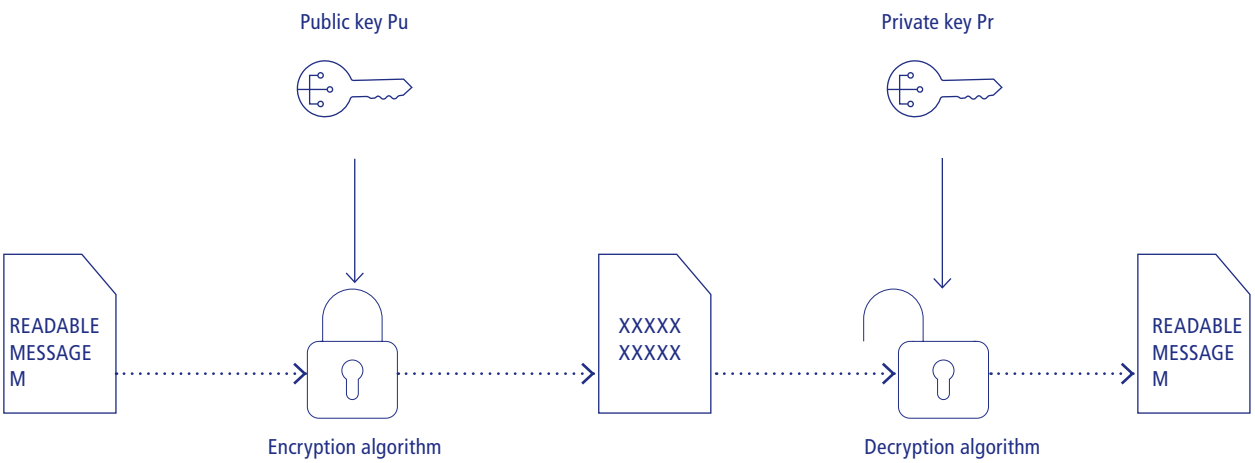
Asymmetric encryption allows anyone with access to public key **Pu** to send confidential messages to the holder of private key **Pr**. Public key **Pu** can be used to encrypt a plaintext message **M** into a ciphertext **C**. Only the holder of private key **Pr** is then able to decrypt ciphertext C and read the message **M**.

Likewise, asymmetric encryption can be used to authenticate the sender of a message. Senders encrypt their message **M** using their private key **Pr** to obtain a ciphertext **C**. Any holder of the public key can decrypt **C** to read **M**, and thus identify the message's sender who, as the holder of private key **Pr**, would be the only party able to encrypt message **M**.

D1 Symmetric encryption



D2 Asymmetric encryption



T1 Security recommendations for the currently most widely used algorithms in the payments industry

Encryption algorithm	Family	Obsolete	Recommended until 2023	Recommended	Recommended in a post-quantum environment
DES(Data Encryption Standard)	Symmetric	DES-2keys	Triple-DES	x	x
AES (Advanced Encryption Standard)	Symmetric			128/192/256	256
RSA (initials of the names of the designers: Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman)	Asymmetric	<2,048 bits	<3,071 bits	3,072 bits or more	x
ECC (Elliptic Curve Cryptography)	Asymmetric				x

Source: Agence nationale de la sécurité des systèmes d'information *(ANSSI – the French national cybersecurity agency) – https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf.*

Asymmetric encryption is based on computations involving the factoring of prime numbers: the operations are easy to perform in one direction, but far more complex in reverse. For example, calculating 1,303 x 1,307 is straightforward but identifying which two numbers were multiplied to obtain 1,703,021 is infinitely more challenging. Rather than the exhaustive brute force attack employed against symmetric encryptions, attacking an asymmetric encryption involves solving these computational problems, and consequently, a combination of quantum computing and sorting techniques could significantly reduce the time and effort required.

The most frequently used asymmetric algorithms are RSA[9] and Elliptic Curve Cryptography (ECC). Most communication protocols are based on asymmetric encryption, particularly when securing an initial exchange of symmetric keys between communicating partners *(see Diagram 2)*.

3.2.1.3 Algorithm families threatened by quantum computing

In practice, the quantum threat is still theoretical. The most powerful quantum computers have a processing power of 399 physical qubits,[10] but some researchers have suggested that given the imprecision of current qubits, 20,000,000 would be required to crack a standard-length RSA key in eight hours.[11]

In time, and depending on improvements in error correction, the same processing power could be achieved with a smaller number of qubits, with experts estimating that sufficient capacity could be achieved with around 2,035 qubits.[12]

Symmetric encryption algorithms such as AES, on the other hand, are less threatened. Using a brute-force search with Grover's algorithm, quantum computing could reduce their level of security[13] – defined by the length of the secret key – by half. Consequently, the *Agence nationale de la sécurité des systèmes d'information* (ANSSI – the French national cybersecurity agency) recommends increasing the encryption key length for AES algorithms to 256 bits to ensure that they will be able to resist future quantum cybersecurity attacks *(see Table 1)*.

3.2.2 Security features in the card payment sector

3.2.2.1 The hashing principle

A hash function is a one-way process used to produce a sequence of bytes, i.e. a fingerprint called a hash, representing a given set of data. For any set of original data, the hash value obtained is always the same. The hash function can therefore be used to ensure data integrity.

3.2.2.2 The HMAC principle

A hash-based message authentication code (HMAC) is a type of message authentication code that combines a cryptographic hash function and a symmetric secret key: the hash function enables two communicating partners to verify the integrity of the data, while the symmetric secret key authenticates the sender.

3.2.2.3 The digital signature principle

A digital signature scheme consists of three algorithms:

- a key generation algorithm that constructs an asymmetric "bi-key", an electronic key made up of a private key **Pr** mathematically linked to a corresponding public key **Pu**;
- a signature generation algorithm that uses the hash of a message **M** and a private key **Pr** to produce a signature **σ** *(see Diagram 3)*;

7 Advanced Encryption Standard.

8 Data Encryption Standard. Unlike AES, the latter is no longer recommended by ANSSI due to certain identified weaknesses (p. 15, *Guide de sélection des algorithmes cryptographiques,* ANSSI, 2021).

9 Initials of the names of the algorithm designers: Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman.

10 *IBM Development Roadmap IBM, https://www.ibm.com/quantum/technology*

11 Craig Gidney and Martin Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits" (2021): *https://quantum-journal.org/papers/q-2021-04-15-433/*

12 See *Quantum threat timeline report* 2022, Global Risk Institute, pp. 21-67: *https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/*

13 Other, more powerful algorithms are being studied that could do more, further reducing the resistance of a symmetric algorithm.

- a signature verification algorithm that enables the receiver of message **M** to validate a signature (true/false response) by comparing the hash of message **M**, which the receiver recalculates itself, with the hash of **M** contained in signature **σ** which it decrypts using a public key **Pu**, to ensure that the hashes are identical *(see Diagram 4)*.

3.2.2.4 The certificate principle

This mechanism is used to substantiate an entity's identity to a relying party through a certificate authority.

To do so, the entity must initiate a dedicated procedure with a certificate authority recognised by its relying parties. Following an evaluation, the entity (now owner) receives a certificate, which consists of two parts: unencrypted information (plaintext) about the owner (notably its name, address and public key) and a signed hash of that information (i.e. encrypted) with the private key of the certificate authority. The certificate authority's public keys are distributed to all potential parties.

During the identification procedure between two entities, the receiver first checks that the issuing entity's certificate has not expired or been revoked. It then confirms the signature's validity by using the certificate authority's public key to decrypt the hash in the certificate, which it compares with a hash that it calculates itself from the plaintext information. If the two hashes are identical, the receiver approves the identity of the sender.

Based on the same principle of using public keys, the certified entity can itself issue subordinate certificate authorities (sub-CAs) for entities under its trust umbrella. This generates a chain of nested sub-CAs, with the integrity of the certificate at the end of the chain backed by the integrity of the earlier certificates.

Consequently, all the trust placed in a public key infrastructure (PKI) is dependent on the integrity of the certificate authority, which has no alternative but to self-sign its own certificate with a private key (the "root certificate").[14]

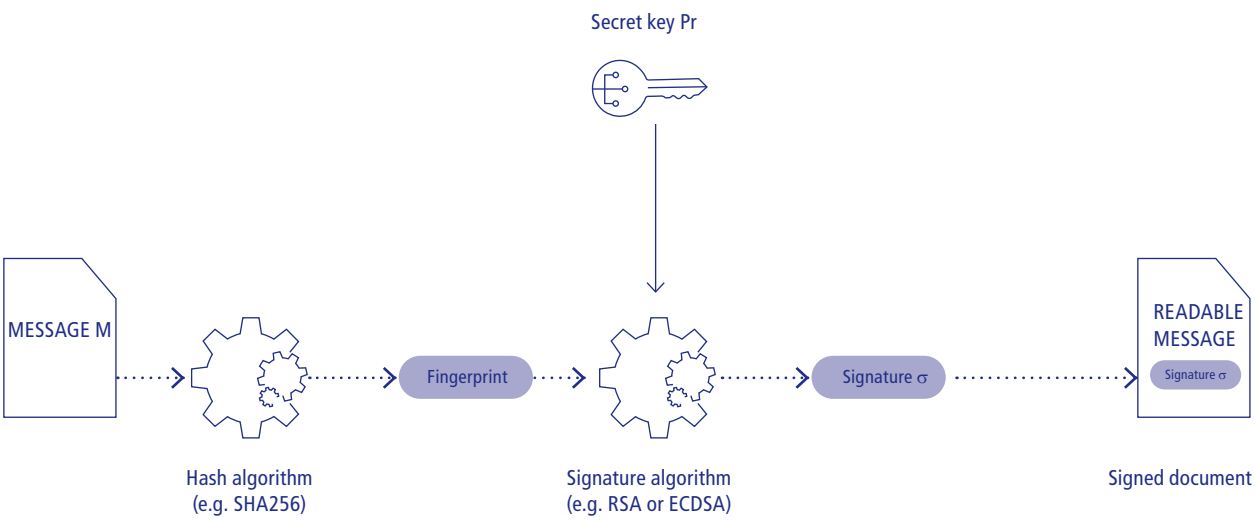
3.2.2.5 The secure connection principle (SSL/TLS)

Secure connections between a computer and a server or between two servers have become common in recent years, and are notably designated by a padlock icon next to a site name in the address bar of web browsers.

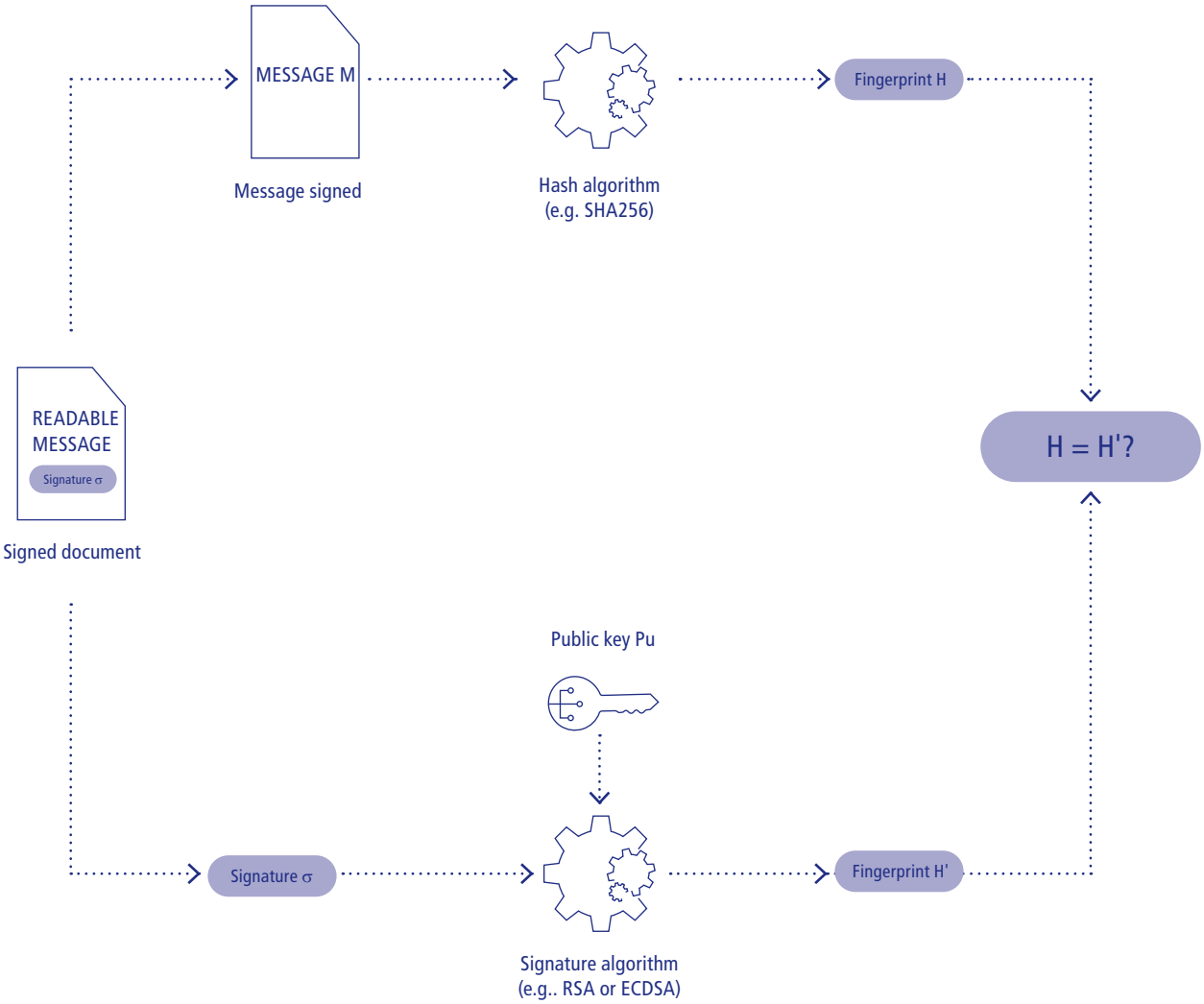
Using SSL/TLS protocols, the legitimacy of the machine connecting to a server can be authenticated. Implementing SSL/TLS involves several steps that ensure secure communication. The first step is server certificate recognition, for which the certificate authorities' public keys are first installed on users' web browsers and the website servers. The second step is to transmit a symmetric secret key used to encrypt and decrypt data communicated during the exchange. The most widely used method to ensure encrypted communication between two parties is the Diffie-Hellman (DH) key exchange.

VPN connections, on the other hand, are more secure as they also apply strong authentication protocols to validate the legitimacy of the user of the machine connecting to a server.

D3 Signature of a document



D4 Signature authentication



3.3 The potential risks to card payment systems in the absence of corrective action

Card payments refer to three different types of transactions:

- point-of-sale payments using electronic payment terminals (EPTs);
- cash withdrawals from automated teller machines (ATMs);
- remote payments over the internet.

The first two transaction types rely on EMVCo technology embedded in card chips.

3.3.1 The security of encryption algorithms for transactions involving EMVCo technology

The following presentation is based on the EMVCo security standards that are currently most commonly applied in point-of-sale card payments and cash withdrawals. Recent upgrades to EMVCo's specifications have led to a gradual migration to new encryption algorithms, but the nature of the quantum threat remains the same.

14 When the latter is compromised, all chains dependent on this certificate authority become suspect, which can create a large-scale crisis of confidence and therefore considerably alter the fluidity of electronic exchanges.

3.3.1.1 A brief overview of the information system associated with EMVCo payments

The smooth functioning of point-of-sale bankcard payments and cash withdrawals depends on **three interconnected secure communication systems** *(see Diagram 5 below)*.

The **first communication system** is integrated into the payment card chip and complies with the international security standards set by the EMVCo[15] standardisation body. These standards impose at least two security functions associated with encryption algorithms:

- Two authentication certificates based on RSA 1984-bit[16] asymmetric encryption are built into the payment card chips:
  - The certificate of the card issuer (usually a bank) is signed by the private key of the card's network (Mastercard, Visa, etc.) while the corresponding public key is distributed to the EPT and ATM platforms.
  - The card's certificate is signed by the card issuer's private key. EPTs can validate a card's legitimacy using the public key contained in the card issuer's certificate. The card certificate also contains a public key used by EPTs when they need to send information to the card, particularly when checking the PIN *(see "Offline PIN", defined in section 3.3.1.2 "Point-of-sale payment and withdrawal transaction methods")*.
- A cryptogram is calculated by the card using the Triple-DES (2k-TDEA) symmetric encryption algorithm for each transaction.[17] The master key is saved in the card issuer's authorisation server. A derived key (from the master key) is uploaded in the card chip which generates a sub-key to encrypt the cryptogram for each transaction it sends to the authorisation server via an EPT or ATM.[18] In turn, the authorisation server uses the master key to encrypt an authorisation request message which it sends to the card. The card simultaneously validates the integrity and authenticity of the payment information contained in the message so that it can then approve the payment or withdrawal.[19]

The **second communication system** connects the EPT or ATM with the server of the owner company (generally the institution acquiring the payment transaction):

- The security of the connection between an EPT and the payment server of the acquirer relies on the *Carte bancaire accepteur acquéreur* (CB2A) protocol. This notably requires the TLS protocol: the EPT and the server are authenticated using certificates incorporating an RSA 2048[20] signature algorithm, and AES-128 secret symmetric keys are also exchanged using an RSA key exchange algorithm or a Diffie-Hellman method.
- For cash withdrawals, ATMs connect to an owner company's cash withdrawal server using the TR-34 and TR-31 protocols, specific to the payments industry, which involve the exchange of asymmetric keys (RSA) and symmetric keys (Triple-DES or AES, depending on the configuration).

Finally, the connection between the authorisation servers of the acquirer and the card issuer is managed by the e-RSB interbank payment network, under STET supervision. The connection between the banks of the acquirer and the card issuer is established using the *Carte bancaire acquéreur-émetteur* (CBAE) protocol.[21] The security system employs AES 128 symmetric encryption, with secret keys managed by specialised security officers.

3.3.1.2 Point-of-sale payment and withdrawal transaction methods

There are three different methods of point-of-sale card payment, all of which have different security features:

- **Transactions with online authorisation request and offline PIN verification**: the EPT can validate the legitimacy of a card using the certificate system[22] while the PIN entered by the cardholder on the EPT's secure keypad is transmitted to the card for offline verification. Issuers may also choose to encrypt the channel between the card and the terminal using the certificate system. Transaction security is supplemented by a Triple-DES encrypted cryptogram produced by the card chip and included in the authorisation request sent to the issuer's authorisation system. This type of transaction is mainly used for payments that require the systematic entry of a PIN (amounts over EUR 50).
- **Offline transactions**: the card is authenticated and the PIN is verified as described above. However, the security offered by the Triple-DES cryptogram is not available so the exchange of information relies solely on asymmetric keys. The decision to process the transaction in offline mode depends on several factors, such as the availability of the internet network (which may be inaccessible to validators in public transport or white areas, or due to server downtime or network outages) and the risk policy of the issuer and/or acquirer. In March 2023, these transactions accounted for approximately 30% of point-of-sale transaction volumes.
- **Transactions with online authorisation request and online PIN verification**: (i) the card is authenticated at the EPT using the certificate system, and (ii) the transaction and PIN are validated by the issuing bank's authorisation server using their own Triple-DES cryptograms (or AES encryptions for the PIN, depending on the issuing bank). This is the most secure transaction method. Although the

number of transactions involved remains marginal, there is considerable potential for growth over the next decade thanks to the development of Software Point of Sales (SoftPOS) technology, which means that a smartphone can replace a traditional EPT.

Lastly, the operational security features for cash withdrawals are very similar to those of the "**Online authorisation with online PIN verification**" mode.

3.3.2 The security of encryption algorithms for transactions involving 3-D Secure technology

Within the framework of the implementation of the second Payment Services Directive (PSD 2), the increasingly widespread use of strong authentication using the 3-D Secure protocol has enhanced the security of remote card payments.

The system is based on a network of complex connections between several servers, which is summarised below.

i. **Initiation of the transaction**: when cardholders make online purchases, they fill in their payment details – the card number (PAN, Primary Account Number), expiration date and card security code – on the merchant's website.
ii. **Routing of the request to the issuing bank's authentication server**: if the merchant participates in the 3-D Secure system, the website sends an authentication request to the Directory Server (DS). Each card scheme has its own DS, which acts as an intermediary between the merchant's server and the authentication server of the cardholder's card issuing bank, referred to as the Access Control Server (ACS).
iii. **Generation of proof of authentication by the ACS**: the bank's ACS receives the authentication request and sends a message to the cardholder so strong authentication can be completed. In the vast majority of cases in France, this step is carried out via a notification sent to cardholders' mobile phone prompting them to connect to their banking application or enter a temporary code sent by SMS in addition to a second secret code (the "enhanced SMS" principle). If the bank's ACS confirms that authentication has been successful, it generates proof of authentication. In the event that authentication fails, the transaction is immediately refused. Regardless of the outcome, the ACS sends a response to the DS, which forwards it to the merchant's website.
iv. **Routing of the payment authorisation request** (similar to the point-of-sale payment process): upon successful authentication, the merchant's website generates an authorisation request that includes the cardholder's proof of authentication. The authorisation request is sent to the card issuer's authorisation server via the sender's authorisation server and the interbank payment network. The applicable controls are comparable and also include verification of the validity of the proof of authentication. Once the transaction has been approved by the card issuer, the cardholder receives payment confirmation from the merchant and the transaction is completed.

The two main embedded security features are:

- connections between merchant sites[23] and the DS, and between the DS and the senders' ACS, secured by certificate exchanges incorporating RSA 2048-type asymmetric encryption algorithms and AES 128 session keys;
- proof of authentication, processed by the ACS and verified by the sender's authorisation system, dependent on an HMAC-SHA-256[24] algorithm with a 256-bit secret key.

3.3.3 The potential impact of quantum computing on the security of card payment encryption systems

ANSSI expresses the level of security of a cryptographic mechanism notably by means of a resistance index that reflects the complexity of cracking an encryption algorithm's key. The index is calculated on the basis of the number of operations required by the best attack known against a given mechanism.

For example, in the case of a symmetric algorithm, a security level of 128 bits of security means that 2^{128} operations are potentially required to crack a mechanism.[25]

15 EMVCo is co-owned by Mastercard, Visa, American Express, Discover, JCB (Japan Credit Bureau) and UnionPay (China).

16 The maximum permitted by EMVCo. In the new specifications, RSA-type encryption is replaced by ECC-type encryption, which is also exposed to quantum risk.

17 In the new specifications, Triple-DES encryption keys are replaced by AES 128 or AES 256 encryption.

18 Authorisation ReQuest Cryptogram (ARQC).

19 Authorisation ResPonse Cryptogram (ARPC).

20 112 bits of security when compared with a symmetric cryptographic primitive.

21 *Carte bancaire acquéreur-émetteur* (CB acquirer-issuer): a protocol for authorisation, remote collection and parameterisation, and network management.

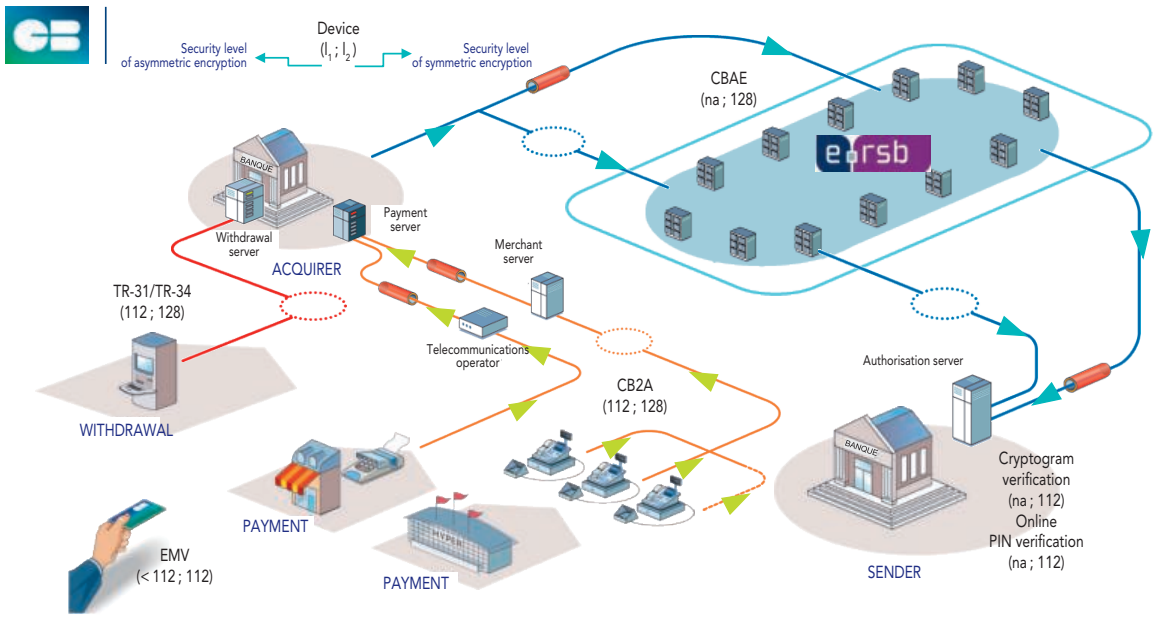
22 An option based on senders' choices.

23 Often through the server of a technical acceptance service provider.

24 SHA (Secure Hash Algorithm) is a cryptographic hash function used by administrative authorities to sign certificates.

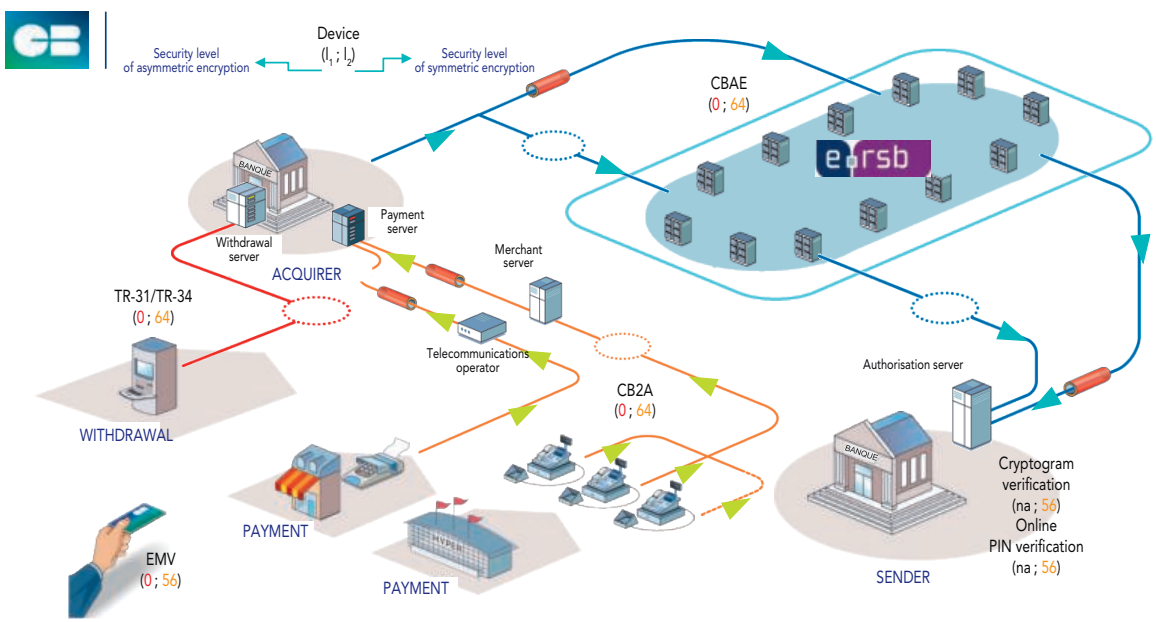
25 See *Guide de sélection d'algorithmes cryptographiques – Guide ANSSI*, pp.47-58, *https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf*

D5 Resistance indices of security devices for point-of-sale card payments and withdrawals



Source : Groupement des cartes bancaires *(France's national interbank network).*
Note : CBAE, *Carte bancaire acquéreur-émetteur* ; CB2A, *Carte bancaire accepteur-acquéreur* ; EMV, EuropayMastercard Visa ; nd, non disponible.

D6 Indices of resistance to quantum computing attacks



Source: Groupement des cartes bancaires *(France's national interbank network).*
Note: CBAE, *Carte bancaire acquéreur-émetteur*; CB2A, *Carte bancaire accepteur-acquéreur*; EMV, Europay Mastercard Visa; na, not available.

The resistance indices of security devices for point-of-sale card payments and withdrawals are shown in Diagram 5. For information, the security afforded by an asymmetric RSA 2048 algorithm is equivalent to a level of 112 bits of security for a symmetric algorithm.

Certificate-based security essentially relies on asymmetric RSA algorithms, which are vulnerable to quantum computing, and on symmetric algorithms, which have less security strength than AES 256. Consequently, a sufficiently powerful quantum computer would degrade security levels as follows *(see Diagram 6)*.

- The EMV cryptogram, generated by a card at each transaction and verified by the issuing authorisation system, would be weakened from 112 to 56 bits of security.
- The card authentication and offline PIN verification mechanisms would be completely compromised, dropping from a level of 112 bits of security to 0.
- The secure link between acceptance systems (EPTs and ATMs) and acquiring systems could be weakened. These links mainly rely on RSA algorithms to exchange symmetric session keys, and should the RSA mechanism be compromised, an attacker could recover the session keys.
- Security implemented at the level of the authorisation network would be diluted, declining from a level of 128 bits of security to 64.

The impact on the resistance indices associated with the 3-D Secure system would be the same, with the security strength associated with asymmetric encryption falling to zero and the security strength associated with symmetric encryption halved.

3.3.4 The risks to card use of quantum computing

If the card payment system fails to adapt, it will eventually become completely vulnerable to:

- **The theft of private and even confidential data**: peoples' identities[26] and the particulars of their transactions could be stolen and decrypted. In the case of a payment transaction with online authorisation request and offline PIN verification, the PIN could be exposed because its confidentiality relies solely on the certificate system when it is transmitted encrypted to the card.
- **The generation of fraudulent payments via the manufacture of Yes Cards**: offline point-at-sale payments are at risk because they rely solely on certificate schemes that depend on asymmetric algorithms.
- **A general loss of confidence in payment infrastructures**: if the root private keys that structure the entire certificate authentication system were cracked, card schemes and issuing banks would no longer be in control of their payment card certification policy. If a high-level encryption key were to be cracked, the impact would be considerable, as its decommissioning would mean that a potentially huge number of cards would have to be recalled and reissued.

However, this assessment may be qualified. Alternative encryption solutions already exist and they could be adopted before the threat materialises.

For example, current implemented symmetric algorithms will have to migrate from Triple-DES or AES 128 to AES 256, in compliance with ANSSI's recommendations. This will safeguard a certain security level associated with authorised online payments, as transactions with online PIN verification will be impervious to quantum computing. This type of transaction should play an increasingly significant role in everyday payments, thanks to the development of SoftPOS technology.[27] While there are no particular technical difficulties associated with this migration, the time required for the upgrades, which can stretch to several years, is a constraint that needs to be taken into consideration if system blockages are to be avoided.

However, the technical considerations with regard to the post-quantum migration of asymmetric encryption algorithms (verification of certificates at card level, TLS connection, etc.) are more complex, which is why research and development efforts are already gathering pace, particularly in the payment industry.

3.4 Experiments in implementing "post-quantum" cryptography

In 2023, ANSSI published a non-comprehensive list of encryption and signature algorithms deemed to be able to stand up to the processing power of future quantum computers.[28] These are commonly referred to as "post-quantum" cryptographic algorithms.

26 For contactless payments, the cardholder's name is not readable.

27 Technology that facilitates the replacement of traditional electronic payment terminals with smartphones.

28 See "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)", ANSSI, 21 December 2023.

Signature	Key exchange method
CRYSTALS-Dilithium (or Dilithium)	CRYSTALS-Kyber (or Kyber)
Falcon	FrodoKEM
SPHINCS+	
XMSS / LMS	

Source: Agence nationale de la sécurité des systèmes d'information *(ANSSI – the French national cybersecurity agency).*

3.4.1 Integrating post-quantum algorithms in bankcard chips

The architecture, memory size and chip components must allow for payment execution that complies with EMVCo standards. In particular, the execution time must not exceed 300 milliseconds (ms). The industry has launched a series of experiments to assess how implementing post-quantum algorithms will impact compliance with these standards.

With regard to memory footprints, the results show that current random access memory (RAM)[29] is insufficient, especially for post-quantum signature algorithms:

- the various trials on integrating Falcon and Dilithium algorithms in a chip all found that five to eight times more RAM is needed than for RSA if security strength is to be maintained;
- the Kyber key exchange algorithm requires four to six times more RAM.

With regard to communication times and volumes of data exchanged, the increase in key size and signature parameters requires an almost proportional increase in the volume of data, and therefore in the communication times between the card and the EPT.

With regard to cryptographic calculation times, they remained quite competitive for smart cards compared with conventional encryption algorithms with a relatively high level of security, such as RSA 3072 for signatures and Diffie-Hellman 3072 for key exchange. The results of the comparative experiments are as follows:

- The signature times of the Dilithium algorithm are equivalent to those of RSA 3072, but only as an average, as the times become non-deterministic – they can vary significantly and randomly. Signature times for the Falcon 512 algorithm, on the other hand, are relatively stable, but twice the average time for Dilithium.

T2 Difference in resources between conventional and post-quantum encryption algorithms at equivalent 128-bit security levels

Post-quantum algorithms		RAM needed for RSA/ECC	Processing time for RSA/DH
Signature	Falcon	x 5 to 8	x 2
	Dilithium		≈
Key exchange	Kyber	x 4 to 6	/ 10
	SABER		/ 10

Sources: Thales and STMicroelectronics.
Note: RAM, random-access memory; RSA, (Ronald) Rivest, (Adi) Shamir and (Leonard) Adleman (initials of the names of the algorithm designers); ECC, Elliptic Curve Cryptography; DH, (Whitfield) Diffie-(Martin) Hellman (initials of the names of the designers of a key exchange method).

- Key exchange times for Kyber 512 and SABER[30] are ten times faster than those associated with Diffie-Hellman 3072.

These post-quantum algorithm implementation trials reveal the limits of current market constraints. Further progress will be required to address the following issues.

- The size of the RAM in the chips will need to be upgraded. There are cards already on the market that have chips with the required amount of RAM, but they are not yet used in payments. Upgrading is therefore technically possible.
- Depending on future developments in the processing technology integrated in chips,[31] the 300 ms standard may have to be adapted to match performance in terms of payment processing times. These times could also vary significantly, for example if the Dilithium algorithm is implemented. Finally, during an intermediary period of post-quantum migration, implementing hybrid algorithms will probably have to be considered. This will ensure that the new chips are compatible with all reading devices, regardless of their compliance with post-quantum technologies. However, the execution time will increase because it will stem from the processing time of the conventional algorithm plus that of the quantum-safe algorithm.
- The performance of contactless payment, which has been expanding rapidly since 2020, could be compromised because contactless technologies operate with a low amount of energy. This restricts processing performance and therefore also limits the post-quantum encryption algorithms or hybridisation techniques that can be implemented.

3.4.2 Integrating post-quantum algorithms in HSMs

Hardware Security Modules (HSMs) are electronic security service devices that generate, store and protect cryptographic keys.

HSMs are essential to any key management infrastructure, particularly to safeguard certificate authorities' master keys. HSMs are in essence units that self-destruct, destroying their data in the event of physical tampering. In terms of software, it provides a mechanism for the distribution of the private secret key among several designated parties. The master private key can only be used for operations when those parties are physically present, thereby guaranteeing its integrity.

These features have direct applications for the payments industry, particularly as card schemes and issuing banks act as authorities for the certificates integrated into payment card chips.

Specific "libraries" (a collection of read-only programme resources) are needed to implement asymmetric post-quantum encryption algorithms in HSMs. Trials have shown that the performance of certain types of HSM has to be improved[32] if they are to be used to their full potential in the post-quantum era. Technically, boosting performance is not a problem but it comes at a cost.

3.4.3 Integrating post-quantum algorithms in VPN servers at central banks

A Virtual Private Network (VPN) is a software that can be installed on several internet-connected devices to create a secure communication tunnel between a client[33] and a server. Its use has become increasingly common in recent years, particularly with the expansion of teleworking.

The Banque de France and the Bundesbank, working closely with the Bank for International Settlements (BIS), have experimented with the transmission of payment messages via a strongSwan IPsec VPN.[34] strongSwan uses X.509 public key certificates, which are widely used to secure electronic communications.[35] The aim of the experiment was to demonstrate that post-quantum algorithms are compatible with public network use.

The experiment was designed based on the assumptions that:

- the HSM, the modules and cryptographic programme libraries were compatible with the post-quantum algorithms used;
- the certificate authorities supply hybrid post-quantum certificates (with Dilithium keys), alongside conventional certificates (with RSA keys).

For the purposes of the project, the teams adapted the certificates on an ad-hoc basis, generating hybrid configuration certificates (parallel hybridisation, *see definition in Section 5.1*). The first, conventional type, incorporates an RSA 2048 algorithm for the digital signature and key exchange mechanism while the second uses post-quantum algorithms. Various combinations of post-quantum algorithms and security strengths[36] were tested *(see Table 3)*.

Each configuration was run around a hundred times. Overall, the difference in connection time for the hybrid post-quantum VPN compared with a conventional algorithm was found to be relatively marginal *(see Chart 2)*. Once the tunnel is configured using AES-256, there is no difference in the connection time when sending a message containing a one-megabyte (MB) XML file as the encryption uses conventional symmetric algorithms.

There is always a trade-off between VPN security and performance: the greater the security required, the longer it takes to establish a VPN tunnel. It was found that where performance is prioritised over security, a combination of the Kyber and Falcon algorithms was the best compromise.

Nevertheless, the experiment was carried out on one single connection at a time. A large number of simultaneous connections would probably require a resizing of the servers, and the estimated connection time for other use cases, particularly TLS connections, would have to be re-examined.

29 RAM is the memory in which calculations are performed.

30 SABER is a post-quantum key exchange algorithm not currently on ANSSI's recommended list.

31 Computational accelerators speed up the performance of costly functions based on RSA and ECC algorithms but do not yet exist or are have not yet been integrated into current smart cards for post-quantum algorithms.

32 HSMs implemented on mainframe servers, widespread in banks, already have sufficient power.

33 A user or a server.

34 **IPsec**: a fairly widespread type of VPN that uses specific authentication and key exchange protocols. **strongSwan**: a free software that facilitates the implementation of IPsec VPNs on various platforms.

35 Current X.509 certificate applications include: SSL/TLS and HTTPS for authenticated and encrypted web browsing, signed and encrypted email via S/MIME (Secure/Multipurpose Internet Mail Extensions) protocols, code signing, document signing, customer authentication, government-issued electronic ID, etc.

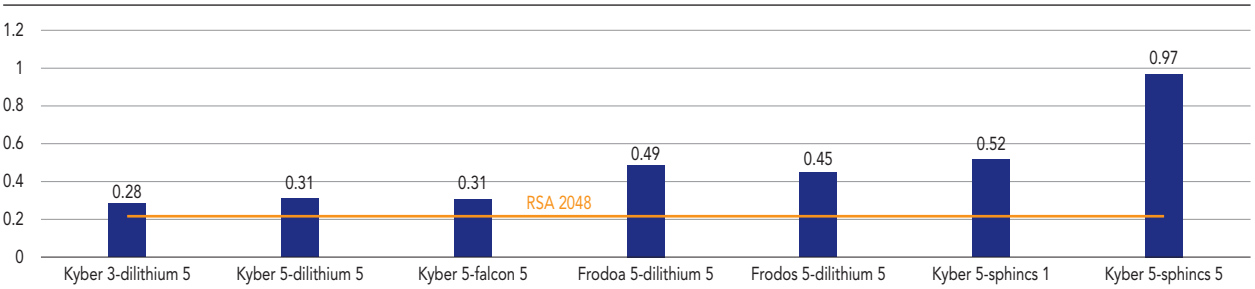
36 These security strengths are determined according to a scale drawn up by the National Institute of Standards and Technology (NIST).

T3 Combinations of conventional and post-quantum algorithms tested in the experiment

Key encapsulation mechanism	Security strength against quantum computing	Digital signature	Security strength against quantum computing
RSA 2048	0	RSA 2048	0
CRYSTALS-Kyber	3	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	Falcon	5
FrodoKEM (AES)	5	CRYSTALS-Dilithium	5
FrodoKEM (Shake)	5	CRYSTALS-Dilithium	5
CRYSTALS-Kyber	5	Sphincs+	1
CRYSTALS-Kyber	5	Sphincs+	5

Source: Banque de France.
Note: CRYSTALS, Cryptographic Suite for Algebraic Lattices.

C2 Average connection time between two servers using different combinations of post-quantum algorithms (in seconds)



Sources: Banque de France and the Bank for International Settlements (BIS).

3.5 The technical challenges of migrating to post-quantum algorithms

Migration presents a number of technical constraints, but time is the most crucial factor. The equipment in operation (EPTs, ATMs, HSMs, etc.) often has a relatively long lifespan, of seven to ten years in general. For cards, the time constraint is less significant because their three to five-year uselife means they are better managed.

Migration will therefore be carried out at a different pace depending on the infrastructure and over a relatively long period. And during that time, post-quantum algorithms could throw up as-yet unknown security flaws. The design of post-quantum encryption mechanisms must therefore be hybrid and agile, in accordance with ANSSI recommendations.[37]

3.5.1 Hybridisation

The principle behind hybridisation is to simultaneously combine the use of current algorithms with post-quantum algorithms, with a two-fold objective.

- Ensuring compatibility with information systems that have not yet migrated to a post-quantum environment.
- Mutually reinforcing the security provided by conventional algorithms and asymmetric post-quantum algorithms. During the migration period, security will continue to be guaranteed by mature conventional algorithms (that have been tried and tested for several decades) and post-quantum algorithms, which will only gradually develop in maturity.

Hybridisation can encompass a host of methods and be carried out either at the level of communication protocols (TLS, IPsec, etc.), or at the level of cryptography objects such as certificates. Taking the example of X.509 certificates, there are currently at least three possible forms of hybridisation, each with its own advantages and disadvantages.

- **Hybrid certificates – catalysts**: this format has additional quantum-safe extensions encoded within it. With the exception of these extensions, it is identical to a traditional certificate. This means that a server that has not yet been migrated to post-quantum can still

analyse and authenticate the certificate using traditional protocols. However, this assumes that non-critical and unknown extensions be treated as opaque data. This format is thus "backward compatible", but the security guaranteed by the post-quantum algorithm can therefore be circumvented.

- **Hybrid certificates – concatenation**: this concatenates a conventional algorithm with a quantum-safe algorithm, replacing the conventional algorithm alone. The exchange protocol between the client and the server remains unchanged but the server must first have migrated to post-quantum programmes to be able to process the concatenated algorithms. Security is therefore enhanced, but the system is no longer backward compatible.
- **Hybrid certificates – parallel hybridisation**: this is an intermediate solution consisting of two linked certificates, one conventional and the other purely quantum-safe. This solution is flexible over time in terms of managing hybrid or pure post-quantum solutions. However, the authentication protocol between the client and the server has to be upgraded to accept its implementation. Furthermore, in the event that the client and the server are migrated, two certificates have to be processed in parallel, in all likelihood lengthening connection times.

The adoption of hybrid solutions is strongly recommended by the European security agencies. In light of this, ANSSI has announced that French security visas will be delivered for products that integrate these hybrid solutions from 2024-25.[38]

With regard to hybridisation, there are a host of format options and combinations of algorithms and they all have repercussions on the entire Public Key Infrastructure (PKI),[39] on the applications that use this post-quantum PKI, and on the protocols and therefore their programming. These choices therefore need to be decided and integrated into organisations' migration plans.

The recommendation for a phase of hybridisation will remain in effect until the competent authorities acknowledge the maturity of post-quantum algorithms.

3.5.2 Cryptoagility

Today, cryptography is often incorporated directly into the source code of software or hardware.

The principle of cryptographic agility – or "cryptoagility" – is to make this cryptography more evolutive and configurable. The particular challenge for algorithms is to predict the ability to switch from a post-quantum algorithm that has been compromised to one that remains secure. The new post-quantum algorithms are based on computational models at varying levels of maturity that have not yet proved their long-term robustness, meaning that in years to come, the scientific community could identify mathematical or implementation weaknesses. By way of an example, two encryption algorithms (SIKE[40] and Rainbow[41]) were recently successfully hacked using conventional computers, as part of the dedicated preselection process organised by the NIST.[42]

Currently, the approvals granted to card manufacturers and the time taken to renew them require algorithms to remain resilient over a period of six to eight years. However, a period of six to eight years could prove to be too long if a flaw in security is discovered in a given post-quantum algorithm.

Replacing post-quantum algorithms with a more robust quantum-safe algorithm requires agile interfaces and generic code, from the library of basic programmes right through to end applications. Migration would therefore involve limited efforts to overhaul transaction protocol specifications.

The principle of cryptoagility in real time could be implemented by embedding an active algorithm and dormant algorithms in the payment card chip, with the different combinations activated via a sender script. It would also be necessary to build secure, and therefore post-quantum, channels for remote updates of software implemented in EPTs and ATMs.

37 See "*Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*", 14 April 2022 and "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)", 21 December 2023.

38 See *https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf*

39 PKI is a set of technologies, procedures and software designed to securely manage digital certificate life cycles.

40 SIKE (Supersingular Isogeny Key Encapsulation), see Castryck and Decru, "An Efficient Key Recovery Attack on SIDH", *Lecture Notes in Computer Science*, Vol. 14008, Springer: *https://link.springer.com/*

41 See Ward Beullens, "Breaking Rainbow Takes a Weekend on a Laptop", *Paper 2022/14*, IBM Research, 2022: *https://eprint.iacr.org/2022/214*

42 The National Institute of Standards and Technology (NIST) is a United States Department of Commerce agency charged with supporting the economy by developing technologies, metrology and standards in co-operation with industry players.

3.6 Conclusions and recommendations

This study has demonstrated that if card payment infrastructures cannot demonstrate their resilience in the face of the threat posed by the development of quantum technology, they will be exposed to major risks: an end to payment transaction confidentiality, data theft, fraudulent payments generated without the possibility of prior identification, significant reputational risks and a potential crisis of confidence among users. This conclusion can be extrapolated across all payment infrastructures and therefore poses a threat to economic stability.

However, despite this doomsday scenario, there are still a host of unknowns, particularly as to when quantum computers powerful enough to crack algorithm encryption keys will become a reality. Experts believe that this could take ten to twenty years.

On 4 May 2022, the President of the United States signed a national security memorandum instructing federal agencies to inventory the security systems in place with a view to drawing up a roadmap, in cooperation with industry and academia, for migration to post-quantum algorithms recognised by the NIST.[43] As the financial and payments sectors are also vulnerable, the US Federal Reserve is contributing to these efforts and a working group dedicated to post-quantum encryption has been set up within Accredited Standards Committee X9 of the American National Standards Institute.[44]

In France, the Military Programming Act of 1 August 2023[45] calls for technical and operational analyses of the transition to post-quantum cryptography as part of the armed forces' innovation programme.

Besides the security issues, the quantum threat represents a major industrial opportunity for French and European businesses in the IT sector, and an opportunity for payment industry players to seize a leadership position in the standardisation of their protocols.

The Observatory for the Security of Payment Means (OSMP) recommends that all payment industry players immediately start to work on two levels of preparation to ready their migration projects.

3.6.1 Anticipating the needs of payment industry players

1) **Inventory the various information system security measures in place, and assess vulnerabilities, particularly in relation to current standards and quantum risk.**
   Organisations should draw up an inventory of the cryptographic algorithms used in all their applications and software, both internally and externally via the internet. Some establishments already have this type of mapping in place. If not, tools for the automated detection of asymmetric algorithms in information systems should be installed and where necessary, manual checks should be performed.
2) **Rank data according to their sensitivity.**
   Sensitive data that need very long-term confidentiality should be listed and ranked to ensure that their encryption method will remain sufficiently robust over the required timeframe.[46]
3) **Pilot the implementation of asymmetric algorithms.**
   Selecting cryptographic options is not a trivial affair when it comes to asymmetric algorithms. Their implementation requires a certain amount of experience. Migration will have repercussions on a host of protocols and infrastructures, and will raise many issues ranging from software libraries to server sizing. The change, and even the increased complexity of the codes, associated with cryptoagility and hybridisation, respectively, should be backed by testing and the use of specific tools to analyse the reaction of IT devices (TLS protocols, VPNs, electronic signatures, etc.). These trials should be launched starting with the most sensitive applications in order to prioritise their migration.
   In the long term, an in-house monitoring system should be put in place to ensure that post-quantum algorithms are implemented appropriately and continuously with regard to parametrisation, configuration and overall protocol consistency.
4) **Draw up a roadmap for each player in the payment chain.**
   A roadmap or post-quantum transition plan, validated at the highest level in each institution, should guide the choices made by technical teams in terms of renewing equipment and software, taking into account their different life cycles and prioritising measures for the most sensitive fields. For the largest institutions, it is

estimated that it will take at least four or five years to migrate their entire information system.

Upstream, a dedicated project team should be set up to optimise migration scenarios, associated budgets and the staff training required, bearing in mind that competition for the services of engineers and technicians is likely to be stiff.

3.6.2 Promoting economies of scale in the payment sector

5) **Inform the standardisation authorities that define payment protocol security.**

Like the NIST in the United States, domestic and European certificate authorities should help organisations to identify "where" and "how" asymmetric encryption algorithms are used in their information systems. They should help to reduce the risk by proposing, as a minimum, tools, guides and best practices (on staff training, procedures and technology) to organisations for use in planning for the replacement and upgrading of hardware, software and services that are vulnerable to the quantum threat. This should be done in close co-operation with public and private sector professionals.

More specifically, in the payments sector, standardisation bodies are invited to share key findings from their migration tests, highlighting issues relating to intra-sector migration choices. The definition of standards for post-quantum encryption algorithms will need to be flexible and adaptive to factor in the need for hybridisation and cryptoagility. Finally, a process of selection among post-quantum algorithms will be required to avoid creating overly complex products that would hinder migration.

6) **Work towards the creation of a permanent high-level working group, ideally at European level, involving the major payment institutions and public supervisory and standardisation authorities.**

Its mandate should be to define an overall roadmap for the migration of the payments industry, based on clearly defined targets, and to be responsible for its monitoring.

In the longer term, this high-level working group could serve as a forum for reflection for the payments sector on the deployment of the quantum internet – the internet of the future – whose main property would be to prevent any attempt at external attack on data confidentiality.

43 See *https://www.whitehouse.gov/*

44 See *https://x9.org/quantum-computing/*

45 French Law No. 2023-703 of 1 August 2023 on military programming for 2024-30 and containing various provisions relating to national defence.

46 AES-256 encryption is recommended by ANSSI for cold data storage.

APPENDICES

Appendices 1 and 3 are available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/system/files/2024-09/OSMP-2023.pdf

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/2024-09/rapport-osmp-2023_dossier-statistique_annexe-5.pdf

A2 RESPONSIBILITIES AND ORGANISATION OF THE OBSERVATORY

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

SCOPE

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

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

- **Credit transfers** are made possible by a payment service provider holding the payer's payment account. The provider credits, after an instruction from the payer, the account of the indicated payee by means of a transaction or a series of payment transactions carried out from the payer's payment account.

- **Direct debits** are used to debit a payer's payment account when a payment transaction is initiated by the payee on the basis of consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.

- **Payment cards** are payment instruments that enable the holder to withdraw or transfer funds. There are different types of cards:
  - Debit cards are cards linked to a payment account enabling the cardholder to make payments or withdrawals that will be debited according to a timeframe set out in the contract for the card;
  - Credit cards are backed by a line of credit, with a rate and a limit negotiated with the customer, and can be used to make payments and/or cash withdrawals. They allow the holder to defer payment to the issuer for a certain period, while the payee is paid directly by the issuer, with no delay;
  - Commercial cards, issued to companies, public bodies or self-employed individuals, are limited to business expenses, with payments made using this type of card billed directly to the account of the company, public body or self-employed individual.

- **Electronic money** is monetary value stored in electronic form, including magnetic form, representing a claim on the issuer, which is issued (by credit institutions or electronic money institutions) against the delivery of funds for payment transactions and which is accepted by a natural or legal person other than the electronic money issuer.

- **Cheques** are documents by which a person, the drawer, instructs a credit institution, the drawee, to pay a certain sum at sight to the drawer or to a third party, known as the payee.

- **Trade bills** are marketable securities that state that the bearer holds a claim for payment of a sum of money and serves for that payment. Trade bills include bills of exchange and promissory notes.

- **The remittance of funds** is a payment service where funds can be sent and received without creating a payment account in the name of the payer or payee. A remittance of funds has the sole purpose of transferring a corresponding amount to a payee or another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of the payee and made available to the payee.

RESPONSIBILITIES

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

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

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

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

COMPOSITION

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

- a member of the French Parliament and a French Senator;
- eight representatives of the French government;
- the Governor of the Banque de France or their representative;
- the Secretary General of the French Prudential Supervision and Resolution Authority;
- a representative of the French Data Protection Authority (*Commission nationale de l'informatique et des libertés*);
- 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 by their expertise.

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

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

The Chairman is appointed from among these members by the French Minister for Economy and Finance. Their term of office is three years, renewable. 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. The sessions are not public. The measures proposed by the Observatory are adopted if an absolute majority is reached in a session. Each member has one vote; in the event of a tie, the chairman has the casting vote. The Observatory has adopted a set of internal rules setting out the conditions under which it operates.

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

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

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

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.);
  - how the means of payment or associated data were used (remote or proximity payments, withdrawals, etc.);
  - the geographical region of issuance or use of the means of payment or related data;
- **and irrespective of the fraudster's identity**: a third party, the account-holding institution and/or issuer of the means of payment, the lawful holder of the means of payment, the legitimate beneficiary of the funds, a trusted third party, etc.

Transactions covered

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

Also excluded from fraud are:

- irregular use of a means of payment due to a lack of sufficient funds, or a closed account resulting in an unpaid balance;
- using a false or assumed identity to open an account or obtain a means of payment in order to make payments;
- situations where the legitimate holder of the means of payment authorises a payment but then objects to its settlement, abusing lawful procedures by making a dispute in bad faith. These include commercial disputes (such as the case of a bankrupt site not delivering sold products, or abusing the fact that an item purchased does not conform to its order);
- cases where a legitimate payer makes a payment to a beneficiary who is a swindler or an accomplice of a swindler, and the product or service purchased does not exist and is therefore not delivered (for example, illicit sale of financial products such as investment products or taking out loans).

The approach used to assess fraud is called "gross-fraud". It entails looking at the initial defrauded amount in a payment transaction without taking into account any measures that may subsequently be taken by the counterparties to reduce such loss (for example, interruption of the delivery of products or the provision of services, amicable agreement to reschedule payment in the event of improper payment rejection, damages to follow up legal action, etc.).

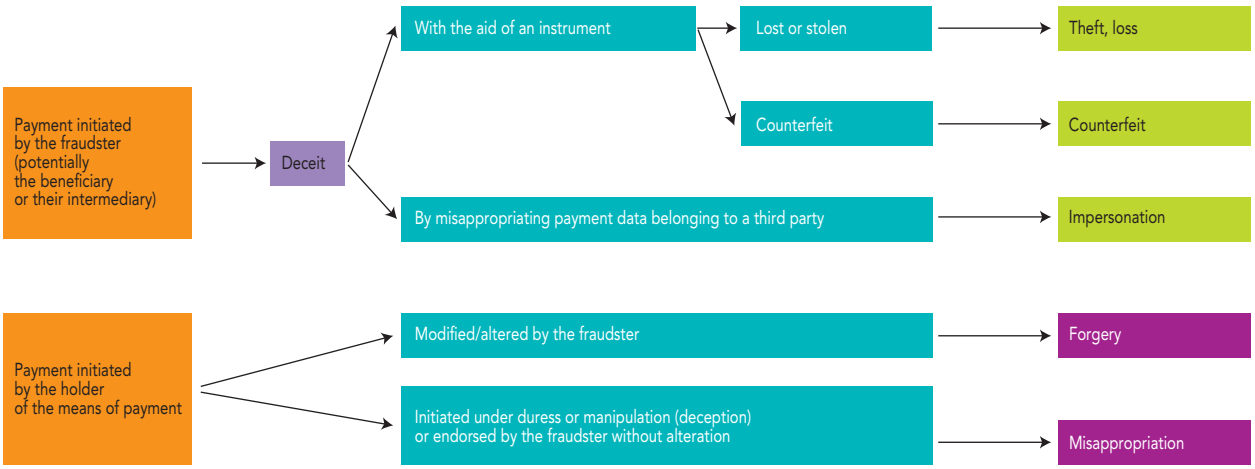
Sources of fraud data

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

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

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

Schematic presentation of the different types of fraud



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

Types of payment fraud

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

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

Geographical breakdown of payment fraud

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

MEASURING PAYMENT CARD FRAUD

Transactions covered

Payment card fraud, as measured in this report, concerns payment transactions (local and remote) and withdrawals made with payment cards and carried out in France and abroad whenever one of the counterparties in the transaction is French, this includes cards issued by a French institution, or a merchant or ATM/ABM located in France that accepts the transaction. No distinctions are made according to the nature of the payment channel used (interbank[3] or private[4]) or the category of card involved (debit card, credit card, commercial card or prepaid card).

Sources of fraud data

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

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

Elements in the analysis of fraud

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

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

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

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

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

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

Types of payment on the internet	Description
3-D Secure payment with strong authentication	Payment made over the internet using the 3-D Secure infrastructure with strong cardholder authentication.
Payments excl. 3-D Secure with strong authentication	Payments made online over the internet, outside the 3-D Secure infrastructure, with strong authentication delegated to a third party, in accordance with the outsourcing requirements applicable under PSD 2 (e.g. an X-Pay-type mobile wallet offered under the responsibility of the issuer, delegation of strong authentication to the merchant under the responsibility of the issuer, etc.).
3-D Secure payment without strong authentication	Payment made over the internet using the 3-D Secure infrastructure without strong authentication by applying an exemption provided for by the European regulations resulting from the second European Payment Services Directive (PSD 2) or in the event of an incident that does not allow the implementation of strong authentication. Single-factor authentication (for example: SMS OTP – one time password – alone) are also included in this category.
Unauthenticated payment	Any payment made outside the 3-D Secure infrastructure, including: • payment not subject to European rules on strong authentication (PSD 2),[a] such as a payment initiated by the creditor on the basis of a pre-existing agreement between the payer and the creditor (e.g.: Merchant Initiated Transaction – MIT) and "One-leg" payments (where the issuer or the acquirer of the payment is located outside the European Union); • payment subject to European rules on strong authentication, but for which the reason for exemption is formalised in the authorisation flow; • payment subject to European rules on strong authentication, but not compliant.

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

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

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

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

MEASURING TRANSFER FRAUD

Payment instruments covered

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

Sources of fraud data

Data on credit transfer fraud is provided by the Banque de France and comes from the regulatory half-yearly fraud declarations made to it by approved payment service providers[5] as contributions its "Census on cashless payment fraud". This data is reported by PSPs in their capacity as the institution servicing the payer in the transaction.

Elements in the analysis of fraud

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

5 Institutions authorised to maintain payment accounts on behalf of their customers and to issue means of payment under the following statutes in accordance with French and European regulations: i) credit or similar institutions (institutions referred to in Article L. 518-1 of the French Monetary and Financial Code), electronic money institutions and payment institutions governed by French law; ii) credit institutions, electronic money institutions and payment institutions governed by foreign law authorised to operate on French territory and established on French territory (i.e. present in France in the form of a branch).

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

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

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

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

MEASURING DIRECT DEBIT FRAUD

Payment instruments covered

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

Sources of fraud data

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

Elements in the analysis of fraud

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

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

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

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

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

MEASURING CHEQUE FRAUD

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

Scope of fraud

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

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

Sources of fraud data

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

Elements of fraud data analysis

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

Specificities of the gross-fraud approach for cheques

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

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

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

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

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

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

MEASURING COMMERCIAL PAPER FRAUD

Payment instruments covered

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

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

Typology and sources of fraud data

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

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

MEASURING FRAUD IN MONEY REMITTANCES

Payment services covered

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

Sources of fraud data

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

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

Payment services covered

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

Sources of fraud data

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

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

SPECIFIC PROVISIONS FOR FRAUD INVOLVING ELECTRONIC MONEY TRANSACTIONS

Payment instruments covered

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

There are two categories of electronic money media:

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

Sources of fraud data

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

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

A5 STATISTICAL DATA ON MEANS OF PAYMENT USE AND FRAUD

You can download the tables in this appendix and additional tables at the following address:
https://www.banque-france.fr/system/files/2024-09/rapport-osmp-2023_dossier-statistique_annexe-5_0.pdf

OVERVIEW OF MEANS OF PAYMENT

T1 Cashless payment means used in France in 2023

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

	Number of transactions (volume)			Amount of transactions (value)			Average value
	2023	Change 2023/2022	Share	2023	Change 2023/2022	Share	
Payments by card[a]	19,685	7.8	61.1	806	8.1	2.3	41
of which contactless	*10,792*	*18.6*	*33.5*	*175*	*18.0*	*0.5*	*16*
of which mobile payments	*1,609*	*90.4*	*5.0*	*36*	*98.1*	*0.1*	*22*
Cheques	891	-11.6	2.8	467	-13.4	1.4	524
Credit transfers	5,658	9.7	17.6	30,589	-21.4	89.0	5,407
of which LVT [b]	*73*	*279.8*	*0.2*	*8,758*	*-44.9*	*25.5*	*119,689*
of which instant transfers (SCT Inst)	*364*	*83.9*	*1.1*	*174*	*46.3*	*0.5*	*478*
Direct debits	4,621	-6.0	14.3	2,139	4.8	6.2	463
Commercial papers	120	59.5	0.4	217	-2.0	0.6	1,812
Electronic money	97	29.7	0.3	1	144.5	0.0	13
Money remittances	8	120.5	0.0	1	33.8	0.0	146
Total	**31,080**	**5.4**	**96.5**	**34,222**	**-19.4**	**99.6**	**1,101**
Withdrawals by card[a]	1,127	-0.8	3.5	136	2.0	0.4	120
Total transactions	**32,207**	**5.2**	**100.0**	**34,357**	**-19.3**	**100.0**	**1,067**

a) Cards issued in France only.
b) LVT: large-value transfers issued via large-value payment systems (Target2, Euro1); professional payments only.
Source: Observatory for the Security of Payment Means.
Note: SCT Inst, SEPA Instant Credit Transfer.

T2 Historical development of cashless payments

a) In volume terms
(in millions of transactions)

	2016	2017	2018	2019	2020	2021	2022	2023
Cards	11,134	12,581	13,179	14,485	13,852	16,129	18,258	19,685
of which contactless	*635*	*1,300*	*2,374*	*3,779*	*5,159*	*7,369*	*9,103*	*10,792*
of which by mobile	*0*	*5*	*11*	*48*	*129*	*357*	*845*	*1,609*
Cheques	2,137	1,927	1,747	1,587	1,175	1,106	1,008	891
Credit transfers	3,753	3,870	4,038	4,269	4,483	4,843	5,158	5,658
of which instant transfers (SCT Inst)	*na*	*na*	*0*	*14*	*45*	*107*	*198*	*364*
Direct debits	3,963	4,091	4,211	4,370	4,622	5,020	4,914	4,621
Commercial papers	82	81	81	78	71	75	75	120
Electronic money	38	55	65	62	36	63	75	97
Money remittances	20	18	16	16	15	2	3	8
Total cashless payments	**21,107**	**22,605**	**23,320**	**24,851**	**24,238**	**27,238**	**29,491**	**31,080**
Withdrawals by card	1,491	1,481	1,439	1,392	1,064	1,086	1,136	1,127

b) In value terms
(EUR billions)

	2016	2017	2018	2019	2020	2021	2022	2023
Cards	499	530	568	600	578	660	746	806
of which contactless	*7*	*13*	*25*	*43*	*80*	*125*	*148*	*175*
of which by mobile	*0,005*	*0,1*	*0,2*	*1*	*3*	*8*	*18*	*36*
Cheques	1,077	1,002	891	814	614	589	540	467
Credit transfers	23,697	24,069	24,296	25,164	32,712	38,723	38,895	30,589
of which instant transfers (SCT Inst)	*na*	*na*	*0,086*	*7*	*27*	*50*	*119*	*174*
Direct debits	1,492	1,579	1,645	1,711	1,684	1,895	2,041	2,139
Commercial papers	266	260	252	232	197	212	222	217
Electronic money	1	1	1	1	1	1	1	1
Money remittances	0,8	1,6	2	2	2	1	1	1
Total cashless payments	**27,032**	**27,440**	**27,653**	**28,522**	**35,786**	**42,081**	**42,445**	**34,222**
Withdrawals by card	129	135	137	137	116	124	133	136

na, not available.

Source: Observatory for the Security of Payment Means.

Note: SCT Inst, SEPA Instant Credit Transfer.

T3 Breakdown of payment means fraud in 2023

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

	Volume			Value			Fraud rate	Average value
	2023	Change 2023/2022	Share	2023	Change 2023/2022	Share	2023	
Payments by card[a)]	6,635,955	-0.9	93.2	455,204,894	8.2	38.1	0.0564	69
of which contactless	*733,359*	*-7.9*	*10.3*	*18,786,086*	*-18.5*	*1.6*	*0.0108*	*26*
of which by mobile	*110,133*	*-32.4*	*1.5*	*7,294,895*	*-33.3*	*0.6*	*0.0205*	*66*
Cheques (new approach)[b)]	203,514	-6.7	2.9	363,549,771	-8.1	30.4	0.0778	1,786
Cheques (old approach)	253,338	-4.8	3.6	585,506,445	5.2	49.0	0.1253	2,311
Credit transfers	90,436	17.7	1.3	311,627,465	-0.5	26.1	0.0010	3,446
of which instant transfers (SCT Inst)	*48,630*	*46.5*	*0.7*	*69,003,730*	*30.8*	*5.8*	*0.0396*	*1,419*
Direct debits	77,876	57.5	1.1	22,320,813	12.4	1.9	0.0010	287
Commercial papers	34	3,300.0	0.0	1,296,652	10,634.8	0.1	0.0006	38,137
Electronic money	4,310	121.6	0.1	251,938	225.7	0.0	0.0201	58
Money remittances	102	-33.8	0.0	55,333	-28.3	0.0	0.0049	542
Total payments	**7,012,227**	**-0.4**	**98.5**	**1,154,306,867**	**0.4**	**96.6**	**0.0053**	**165**
Withdrawals by card[a)]	110,221	-10.8	1.5	40,608,913	-5.9	3.4	0.0300	368
Total transactions	**7,122,448**	**-0.6**	**100.0**	**1,194,915,780**	**0.2**	**100.0**	**0.0043**	**168**

a) Cards issued in France only.

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

Source: Observatory for the Security of Payment Means.

Notes: SCT Inst, SEPA Instant Credit Transfer.

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

T4 Historical development of fraud involving payment means

a) In volume terms
(in units)

	2016	2017	2018	2019	2020	2021	2022	2023
Cards	5,300,847	5,364,312	6,068,959	7,071,095	7,421,137	6,764,752	6,692,988	6,635,955
of which contactless	*125,860*	*248,991*	*445,919*	*603,509*	*537,061*	*604,278*	*796,027*	*733,359*
of which by mobile	*na*	*22*	*2,070*	*3,494*	*33,761*	*83,266*	*162,869*	*110,133*
Cheque (new approach)	na	na	na	na	190,001	232,277	218,122	203,514
Cheque (old approach)	120,295	114,906	166,421	183,488	220,685	272,970	266,216	253,338
Credit transfers	5,585	4,642	7,736	15,934	35,893	46,718	76,846	90,436
of which instant transfers (SCT Inst)	*na*	*na*	*5*	*729*	*7,131*	*12,913*	*33,193*	*48,630*
Direct debits	1,176	25,801	309,377	43,519	6,485	251,010	49,453	77,876
Commercial papers	4	3	5	1	62	1	1	34
Electronic money	na	na	na	na	na	2,001	1,945	4,310
Money remittances	na	na	na	na	na	962	154	102
Total cashless payment fraud	**5,427,907**	**5,509,664**	**6,552,498**	**7,314,037**	**7,684,262**	**7,297,721**	**7,039,509**	**7,012,227**
Withdrawals by card	202,158	177,562	158,908	165,505	113,067	129,083	123,574	110,221
Total fraudulent transactions	**5,630,065**	**5,687,226**	**6,711,406**	**7,479,542**	**7,797,329**	**7,426,804**	**7,163,083**	**7,122,448**

na, not available.

Source: Observatory for the Security of Payment Means.

Notes: SCT Inst, SEPA Instant Credit Transfer.

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

b) In value terms
(euro)

	2016	2017	2018	2019	2020	2021	2022	2023
Cards	378,455,912	344,962,084	401,604,986	428,249,931	439,489,315	421,410,285	420,585,823	455,204,894
of which contactless	*1,410,566*	*2,748,790*	*5,234,852*	*8,479,354*	*11,292,261*	*16,274,668*	*23,047,180*	*18,786,086*
of which by mobile	*na*	*1,227*	*73,682*	*216,236*	*2,792,574*	*5,610,270*	*10,942,984*	*7,294,895*
Cheque (new approach)	na	na	na	na	401,611,189	465,021,167	395,416,196	363,549,771
Cheque (old approach)	276,716,554	296,072,847	450,108,464	539,215,175	538,059,139	625,703,442	556,796,815	585,506,445
Credit transfers	86,284,101	78,286,492	97,327,128	161,642,174	266,969,099	287,264,068	313,163,442	311,627,465
of which instant transfers (SCT Inst)	*na*	*na*	*29,800*	*2,203,240*	*10,562,419*	*22,406,942*	*52,768,218*	*69,003,730*
Direct debits	39,935,882	8,726,403	58,346,253	10,990,025	1,891,051	25,318,677	19,853,012	22,320,813
Commercial papers	1,018,149	153,100	226,217	74,686	538,918	12,079	12,079	1,296,652
Electronic money	na	na	na	na	na	137,340	77,349	251,938
Money remittances	na	na	na	na	na	246,362	77,162	55,333
Total cashless payment fraud	**782,410,598**	**728,200,926**	**1,007,613,048**	**1,140,171,991**	**1,246,947,522**	**1,199,409,978**	**1,149,185,062**	**1,154,306,867**
Withdrawals by card	48,650,966	42,038,924	37,630,659	41,651,788	33,950,879	42,950,169	43,148,054	40,608,913
Total fraudulent transactions	**831,061,564**	**770,239,850**	**1,045,243,707**	**1,181,823,779**	**1,280,898,401**	**1,242,360,147**	**1,192,333,116**	**1,194,915,780**

na, not available.

Source: Observatory for the Security of Payment Means.

Notes: SCT Inst, SEPA Instant Credit Transfer.

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

T5 Payments by cards issued in France

(volume in thousands, value in EUR thousands)

	2018		2019		2020	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**11,222,954**	**443,193,792**	**12,171,755**	**459,066,750**	**11,193,795**	**424,105,649**
of which contactless payments (incl. mobile payments)	*2,374,029*	*25,219,537*	*3,778,756*	*42,903,452*	*5,159,657*	*79,664,370*
of which mobile payments	*11,399*	*200,876*	*47,885*	*850,983*	*129,105*	*2,734,667*
Remote payments (excl. internet)	**63,021**	**4,696,704**	**77,150**	**4,838,911**	**134,114**	**7,567,877**
Internet payments	**1,893,443**	**119,903,848**	**2,236,049**	**135,352,563**	**2,524,317**	**146,563,476**
Withdrawals	**1,439,414**	**136,638,334**	**1,391,930**	**136,507,651**	**1,064,095**	**115,958,207**
Total	**14,618,833**	**704,432,677**	**15,876,884**	**735,765,875**	**14,916,322**	**694,195,208**

Source: Observatory for the Security of Payment Means.
Note: UPT, Unattended Payment Terminal.

T5 Payments by cards issued in France (continued)

(volume in thousands, value in EUR thousands)

	2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**12,935,438**	**475,079,750**	**14,868,338**	**537,503,850**	**15,903,747**	**570,896,450**
of which contactless payments (incl. mobile payments)	*7,368,699*	*125,082,420*	*9,102,931*	*148,006,593*	*10,792,452*	*174,706,103*
of which mobile payments	*357,355*	*7,596,769*	*845,223*	*17,937,091*	*1,609,423*	*35,539,253*
Remote payments (excl. internet)	**76,931**	**7,995,010**	**105,781**	**16,994,865**	**96,368**	**15,880,261**
Internet payments	**3,116,285**	**177,056,237**	**3,283,604**	**191,418,128**	**3,685,180**	**219,662,525**
of which 3-D Secure payments with strong authentication	*787,664*	*85,221,641*	*1,034,950*	*112,713,734*	*1,282,644*	*136,151,668*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*135,611*	*4,119,307*
of which 3-D Secure payments without strong authentication	*444,723*	*19,267,910*	*781,313*	*27,091,534*	*800,728*	*27,212,160*
of which payments excl. 3-D Secure without strong authentication	*1,883,898*	*72,566,685*	*1,467,342*	*51,612,860*	*1,466,199*	*52,179,389*
of which MIT	*na*	*na*	*na*	*na*	*877,839*	*30,771,262*
of which "one-leg" payments	*na*	*na*	*na*	*na*	*31,151*	*1,997,096*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*250,843*	*9,039,674*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*306,366*	*10,371,359*
Withdrawals	**1,086,289**	**123,867,648**	**1,135,675**	**132,879,066**	**1,127,043**	**135,511,148**
Total	**17,214,942**	**783,998,644**	**19,393,398**	**878,795,909**	**20,812,338**	**941,950,384**

na, not available.
Source: Observatory for the Security of Payment Means.
Note: One-leg, a payment where the acquirer is located outside the European Union; MIT, Merchant Initiated Transaction; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

T5 *bis* Number of cards and instruments

T6 Fraudulent transactions using cards issued in France

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

	2018			2019			2020		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**1,142,861**	**64,546,992**	**0.015**	**1,203,233**	**64,992,145**	**0.014**	**972,228**	**47,994,762**	**0.011**
of which contactless payments (incl. mobile payments)	*445,919*	*5,234,852*	*0.021*	*603,509*	*8,479,354*	*0.020*	*537,061*	*11,292,261*	*0.014*
of which mobile payments	*2,070*	*73,682*	*0.037*	*3,494*	*216,236*	*0.025*	*33,761*	*2,792,574*	*0.102*
Remote payments (excl. internet)	**406,712**	**28,562,421**	**0.608**	**409,319**	**31,806,788**	**0.657**	**411,344**	**26,899,103**	**0.355**
Internet payments	**4,519,386**	**308,495,573**	**0.257**	**5,458,543**	**331,450,998**	**0.245**	**6,037,565**	**364,595,450**	**0.249**
Withdrawals	**158,908**	**37,630,659**	**0.028**	**165,505**	**41,651,788**	**0.031**	**113,067**	**33,950,879**	**0.029**
Total	**6,227,867**	**439,235,645**	**0.062**	**7,236,600**	**469,901,719**	**0.064**	**7,534,204**	**473,440,194**	**0.068**

Source: Observatory for the Security of Payment Means.

T6 Fraudulent transactions using cards issued in France (continued)

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

	2021			2022			2023		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**942,376**	**52,426,587**	**0.011**	**1,055,575**	**62,861,464**	**0.012**	**966,134**	**61,618,923**	**0.011**
of which contactless payments (incl. mobile payments)	*604,278*	*16,274,668*	*0.013*	*796,027*	*23,047,180*	*0.016*	*733,359*	*18,786,086*	*0.011*
of which mobile payments	*83,266*	*5,610,270*	*0.074*	*162,869*	*10,942,984*	*0.061*	*110,133*	*7,294,895*	*0.021*
Remote payments (excl. internet)	**124,596**	**22,193,382**	**0.278**	**174,364**	**42,028,102**	**0.247**	**186,499**	**42,177,372**	**0.266**
Internet payments	**5,697,780**	**346,790,316**	**0.196**	**5,463,049**	**315,696,257**	**0.165**	**5,483,322**	**351,408,599**	**0.160**
of which 3-D Secure payments with strong authentication	*496,017*	*103,029,680*	*0.121*	*624,473*	*124,258,815*	*0.110*	*722,396*	*132,754,198*	*0.098*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*159,680*	*8,966,661*	*0.218*
of which 3-D Secure payments without strong authentication	*364,223*	*26,046,078*	*0.135*	*625,296*	*25,695,176*	*0.095*	*593,808*	*22,929,848*	*0.084*
of which payments excl. 3-D Secure without strong authentication	*4,837,540*	*217,714,555*	*0.300*	*4,213,280*	*165,742,266*	*0.321*	*4,007,438*	*186,757,892*	*0.358*
of which MIT	*na*	*na*	*na*	*na*	*na*	*na*	*1,995,881*	*87,685,148*	*0.285*
of which "one-leg" payments	*na*	*na*	*na*	*na*	*na*	*na*	*416,116*	*30,632,806*	*1.534*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*553,018*	*16,515,229*	*0.183*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*1,042,423*	*51,924,709*	*0.501*
Withdrawals	**129,083**	**42,950,169**	**0.035**	**123,574**	**43,148,054**	**0.032**	**110,221**	**40,608,913**	**0.030**
Total	**6,893,835**	**464,360,454**	**0.059**	**6,816,562**	**463,733,877**	**0.053**	**6,746,176**	**495,813,807**	**0.053**

na, not available.

Source: Observatory for the Security of Payment Means.

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

T7 Types of fraud involving payments by cards issued in France in 2023

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

	Lost or stolen cards				Intercepted cards				Altered or counterfeit cards			
	Volume		Value		Volume		Value		Volume		Value	
	Number	Share	Number	Share	Number	Share	Number	Share	Number	Share	Number	Share
Face-to-face payments and UPT	**647,705**	**67.0**	**37,753,346**	**61.3**	**14,720**	**1.5**	**2,065,985**	**3.4**	**86,229**	**8.9**	**5,180,634**	**8.4**
of which contactless payments (incl. mobile payments)	*518,047*	*70.6*	*12,067,959*	*64.2*	*5,286*	*0.7*	*115,996*	*0.6*	*69,048*	*9.4*	*2,927,912*	*15.6*
of which mobile payments	*46,558*	*42.3*	*3,459,004*	*47.4*	*363*	*0.3*	*32,991*	*0.5*	*32,390*	*29.4*	*2,053,646*	*28.2*
Remote payments (excl. internet)	**16,273**	**8.7**	**3,188,540**	**7.6**	**111**	**0.1**	**8,899**	**0.0**	**472**	**0.3**	**147,974**	**0.4**
Internet payments	**324,358**	**5.9**	**23,817,989**	**6.8**	**2,992**	**0.1**	**192,755**	**0.1**	**238,292**	**4.3**	**10,280,753**	**2.9**
of which 3-D Secure payments with strong authentication	*52,736*	*7.3*	*9,924,112*	*7.5*	*532*	*0.1*	*61,051*	*0.0*	*6,645*	*0.9*	*1,117,341*	*0.8*
of which payments excl. 3-D Secure with strong authentication	*3,728*	*2.3*	*192,619*	*2.1*	*116*	*0.1*	*9,855*	*0.1*	*4,639*	*2.9*	*286,923*	*3.2*
of which 3-D Secure payments without strong authentication	*22,800*	*3.8*	*1,671,647*	*7.3*	*183*	*0.0*	*7,603*	*0.0*	*11,712*	*2.0*	*330,786*	*1.4*
of which payments excl. 3-D Secure without strong authentication	*245,094*	*6.1*	*12,029,611*	*6.4*	*2,161*	*0.1*	*114,246*	*0.1*	*215,296*	*5.4*	*8,545,703*	*4.6*
of which MIT	*202,601*	*10.2*	*8,584,383*	*9.8*	*1,089*	*0.1*	*35,474*	*0.0*	*37,263*	*1.9*	*1,503,421*	*1.7*
of which "one-leg" payments	*11,328*	*2.7*	*1,325,783*	*4.3*	*344*	*0.1*	*22,250*	*0.1*	*14,413*	*3.5*	*1,318,207*	*4.3*
of which PSD 2 compliant non-3-D Secure payments	*11,492*	*2.1*	*445,549*	*2.7*	*454*	*0.1*	*11,864*	*0.1*	*2,012*	*0.4*	*45,446*	*0.3*
of which non-PSD 2 compliant non-3-D Secure payments	*19,673*	*1.9*	*1,673,896*	*3.2*	*274*	*0.0*	*44,658*	*0.1*	*161,608*	*15.5*	*5,678,629*	*10.9*
Withdrawals	**83,317**	**75.6**	**32,189,560**	**79.3**	**4,657**	**4.2**	**1,593,329**	**3.9**	**3,354**	**3.0**	**843,585**	**2.1**
Total	**1,071,653**	**15.9**	**96,949,435**	**19.6**	**22,480**	**0.3**	**3,860,968**	**0.8**	**328,347**	**4.9**	**16,452,946**	**3.3**

Source: Observatory for the Security of Payment Means.

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

T7 Types of fraud involving payments by cards issued in France in 2023 (continued)

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

	Misappropriated card numbers				Other				All sources	
	Volume		Value		Volume		Value		Volume	Value
	Number	Share	Number	Share	Number	Share	Number	Share		
Face-to-face payments and UPT	**30,089**	**3.1**	**3,023,807**	**4.9**	**187,391**	**19.4**	**13,595,151**	**22.1**	**966,134**	**61,618,923**
of which contactless payments (incl. mobile payments)	*18,656*	*2.5*	*724,062*	*3.9*	*122,322*	*16.7*	*2,950,157*	*15.7*	*733,359*	*18,786,086*
of which mobile payments	*9,488*	*8.6*	*450,353*	*6.2*	*21,334*	*19.4*	*1,298,901*	*17.8*	*110,133*	*7,294,895*
Remote payments (excl. internet)	**169,058**	**90.6**	**38,780,374**	**91.9**	**585**	**0.3**	**51,585**	**0.1**	**186,499**	**42,177,372**
Internet payments	**4,897,807**	**89.3**	**313,568,198**	**89.2**	**19,873**	**0.4**	**3,548,904**	**1.0**	**5,483,322**	**351,408,599**
of which 3-D Secure payments with strong authentication	*660,474*	*91.4*	*120,457,312*	*90.7*	*2,009*	*0.3*	*1,194,382*	*0.9*	*722,396*	*132,754,198*
of which payments excl. 3-D Secure with strong authentication	*150,056*	*94.0*	*8,392,243*	*93.6*	*1,141*	*0.7*	*85,021*	*0.9*	*159,680*	*8,966,661*
of which 3-D Secure payments without strong authentication	*557,980*	*94.0*	*20,816,973*	*90.8*	*1,133*	*0.2*	*102,839*	*0.4*	*593,808*	*22,929,848*
of which payments excl. 3-D Secure without strong authentication	*3,529,297*	*88.1*	*163,901,670*	*87.8*	*15,590*	*0.4*	*2,166,662*	*1.2*	*4,007,438*	*186,757,892*
of which MIT	*1,751,336*	*87.7*	*77,429,884*	*88.3*	*3,592*	*0.2*	*131,986*	*0.2*	*1,995,881*	*87,685,148*
of which "one-leg" payments	*385,102*	*92.5*	*27,090,943*	*88.4*	*4,929*	*1.2*	*875,623*	*2.9*	*416,116*	*30,632,806*
of which PSD 2 compliant non-3-D Secure payments	*537,238*	*97.1*	*15,705,353*	*95.1*	*1,822*	*0.3*	*307,017*	*1.9*	*553,018*	*16,515,229*
of which non-PSD 2 compliant non-3-D Secure payments	*855,621*	*82.1*	*43,675,490*	*84.1*	*5,247*	*0.5*	*852,036*	*1.6*	*1,042,423*	*51,924,709*
Withdrawals	**550**	**0.5**	**102,577**	**0.3**	**18,343**	**16.6**	**5,879,862**	**14.5**	**110,221**	**40,608,913**
Total	**5,097,504**	**75.6**	**355,474,956**	**71.7**	**226,192**	**3.4**	**23,075,502**	**4.7**	**6,746,176**	**495,813,807**

Source: Observatory for the Security of Payment Means.

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

T8 Geographical breakdown of fraud involving cards issued in France in 2023

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

	Domestic transactions				European transactions			
	Volume		Value		Volume		Value	
	Number	Share	Value	Share	Number	Share	Value	Share
Face-to-face payments and UPT	**885,533**	**91.7**	**50,277,021**	**81.6**	**41,656**	**4.3**	**3,477,134**	**5.6**
of which contactless payments (incl. mobile payments)	*684,776*	*93.4*	*15,698,156*	*83.6*	*29,640*	*4.0*	*1,600,923*	*8.5*
of which mobile payments	*98,610*	*89.5*	*6,066,551*	*83.2*	*3,091*	*2.8*	*336,438*	*4.6*
Remote payments (excl. internet)	**118,903**	**63.8**	**22,602,626**	**53.6**	**28,029**	**15.0**	**8,936,220**	**21.2**
Internet payments	**1,913,224**	**34.9**	**152,815,486**	**43.5**	**2,349,387**	**42.8**	**120,406,288**	**34.3**
of which 3-D Secure payments with strong authentication	*314,857*	*43.6*	*72,017,359*	*54.2*	*299,991*	*41.5*	*45,596,872*	*34.3*
of which payments excl. 3-D Secure with strong authentication	*36,576*	*22.9*	*2,353,042*	*26.2*	*90,765*	*56.8*	*5,352,650*	*59.7*
of which 3-D Secure payments without strong authentication	*258,701*	*43.6*	*12,634,204*	*55.1*	*260,511*	*43.9*	*7,911,532*	*34.5*
of which payments excl. 3-D Secure without strong authentication	*1,303,090*	*32.5*	*65,810,881*	*35.2*	*1,698,120*	*42.4*	*61,545,234*	*33.0*
of which MIT	*1,044,582*	*52.3*	*49,260,633*	*56.2*	*634,013*	*31.8*	*27,045,718*	*30.8*
of which "one-leg" payments	*0*	*0.0*	*0*	*0.0*	*0*	*0.0*	*0*	*0.0*
of which PSD 2 compliant non-3-D Secure payments	*70,590*	*12.8*	*4,496,448*	*27.2*	*476,009*	*86.1*	*11,630,803*	*70.4*
of which non-PSD 2 compliant non-3-D Secure payments	*187,918*	*18.0*	*12,053,800*	*23.2*	*588,098*	*56.4*	*22,868,713*	*44.0*
Withdrawals	**102,357**	**92.9**	**38,832,083**	**95.6**	**2,882**	**2.6**	**845,142**	**2.1**
Total	**3,020,017**	**44.8**	**264,527,216**	**53.4**	**2,421,954**	**35.9**	**133,664,784**	**27.0**

Source: Observatory for the Security of Payment Means.

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

T8 Geographical breakdown of fraud involving cards issued in France in 2023 continued)

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

	International transactions				Total	
	Volume		Value		Volume	Value
	Number	Share	Value	Share		
Face-to-face payments and UPT	**38,945**	**4.0**	**7,864,768**	**12.8**	**966,134**	**61,618,923**
of which contactless payments (incl. mobile payments)	*18,943*	*2.6*	*1,487,007*	*7.9*	*733,359*	*18,786,086*
of which mobile payments	*8,432*	*7.7*	*891,906*	*12.2*	*110,133*	*7,294,895*
Remote payments (excl. internet)	**39,567**	**21.2**	**10,638,526**	**25.2**	**186,499**	**42,177,372**
Internet payments	**1,220,711**	**22.3**	**78,186,825**	**22.2**	**5,483,322**	**351,408,599**
of which 3-D Secure payments with strong authentication	*107,548*	*14.9*	*15,139,967*	*11.4*	*722,396*	*132,754,198*
of which payments excl. 3-D Secure with strong authentication	*32,339*	*20.3*	*1,260,969*	*14.1*	*159,680*	*8,966,661*
of which 3-D Secure payments without strong authentication	*74,596*	*12.6*	*2,384,112*	*10.4*	*593,808*	*22,929,848*
of which payments excl. 3-D Secure without strong authentication	*1,006,228*	*25.1*	*59,401,777*	*31.8*	*4,007,438*	*186,757,892*
of which MIT	*317,286*	*15.9*	*11,378,797*	*13.0*	*1,995,881*	*87,685,148*
of which "one-leg" payments	*416,116*	*100.0*	*30,632,806*	*100.0*	*416,116*	*30,632,806*
of which PSD 2 compliant non-3-D Secure payments	*6,419*	*1.2*	*387,978*	*2.3*	*553,018*	*16,515,229*
of which non-PSD 2 compliant non-3-D Secure payments	*266,407*	*25.6*	*17,002,196*	*32.7*	*1,042,423*	*51,924,709*
Withdrawals	**4,982**	**4.5**	**931,688**	**2.3**	**110,221**	**40,608,913**
Total	**1,304,205**	**19.3**	**97,621,807**	**19.7**	**6,746,176**	**495,813,807**

Source: Observatory for the Security of Payment Means.

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

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

(volume in thousands, value in EUR thousands)

	2018		2019		2020	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**10,864,788**	**421,977,639**	**11,774,183**	**437,193,670**	**10,978,602**	**413,760,411**
of which contactless payments (incl. mobile payments)	*2,320,822*	*24,439,724*	*3,690,364*	*41,558,002*	*5,081,519*	*78,386,853*
of which mobile payments	*10,949*	*190,953*	*45,249*	*794,288*	*126,945*	*2,687,300*
Remote payments (excl. internet)	**34,893**	**2,707,270**	**34,859**	**2,773,069**	**60,243**	**5,428,918**
Internet payments	**1,515,988**	**97,756,554**	**1,768,890**	**109,593,147**	**2,011,431**	**122,128,921**
Withdrawals	**1,385,723**	**129,786,224**	**1,339,625**	**130,198,441**	**1,038,647**	**112,337,533**
Total	**13,801,392**	**652,227,686**	**14,917,558**	**679,758,326**	**14,088,924**	**653,655,783**

Source : Observatoire de la sécurité des moyens de paiement.

Note: UPT, Unattended Payment Terminal.

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

(volume in thousands, value in EUR thousands)

	2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**12,611,966**	**460,274,895**	**14,340,211**	**514,159,801**	**15,252,122**	**543,567,354**
of which contactless payments (incl. mobile payments)	*7,202,992*	*121,694,861*	*8,781,813*	*141,160,469*	*10,357,439*	*164,920,568*
of which mobile payments	*348,251*	*7,390,633*	*808,622*	*17,132,553*	*1,533,084*	*33,773,794*
Remote payments (excl. internet)	**56,236**	**5,540,339**	**87,602**	**13,259,829**	**82,700**	**12,227,259**
Internet payments	**2,399,865**	**142,184,895**	**2,393,161**	**146,642,890**	**2,580,907**	**164,682,672**
of which 3-D Secure payments with strong authentication	*661,960*	*72,184,112*	*809,038*	*88,956,221*	*977,983*	*105,884,327*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*57,239*	*1,938,429*
of which 3-D Secure payments without strong authentication	*389,530*	*15,797,723*	*717,916*	*24,981,800*	*661,070*	*22,814,974*
of which payments excl. 3-D Secure without strong authentication	*1,348,375*	*54,203,060*	*866,207*	*32,704,868*	*884,617*	*34,044,942*
of which MIT	*na*	*na*	*na*	*na*	*704,832*	*25,137,618*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*92,513*	*4,489,918*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*87,272*	*4,417,407*
Withdrawals	**1,056,936**	**119,485,544**	**1,101,989**	**128,161,781**	**1,085,417**	**129,282,806**
Total	**16,125,003**	**727,485,673**	**17,922,963**	**802,224,301**	**19,001,146**	**849,760,091**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: MIT, Merchant Initiated Transaction; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

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

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

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

	2018			2019			2020		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**977,654**	**41,383,109**	**0.010**	**1,069,418**	**44,175,058**	**0.010**	**793,350**	**36,280,495**	**0.009**
of which contactless payments (incl. mobile payments)	*426,713*	*4,967,274*	*0.020*	*582,050*	*7,912,021*	*0.019*	*522,873*	*10,502,092*	*0.013*
of which mobile payments	*1,717*	*50,491*	*0.026*	*3,215*	*197,048*	*0.025*	*29,807*	*2,447,707*	*0.091*
Remote payments (excl. internet)	**159,916**	**9,512,197**	**0.351**	**64,113**	**7,498,207**	**0.270**	**74,832**	**8,964,315**	**0.165**
Internet payments	**2,180,379**	**163,824,893**	**0.168**	**2,630,697**	**183,067,879**	**0.167**	**2,847,769**	**212,962,645**	**0.174**
Withdrawals	**109,924**	**30,893,412**	**0.024**	**122,260**	**35,935,625**	**0.028**	**102,962**	**32,477,429**	**0.029**
Total	**3,427,873**	**245,613,611**	**0.038**	**3,886,488**	**270,676,769**	**0.040**	**3,818,913**	**290,684,884**	**0.044**

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

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

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

	2021			2022			2023		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**825,325**	**43,515,617**	**0.009**	**989,454**	**53,593,598**	**0.010**	**885,533**	**50,277,021**	**0.009**
of which contactless payments (incl. mobile payments)	*576,537*	*14,002,613*	*0.012*	*754,985*	*20,231,615*	*0.014*	*684,776*	*15,698,156*	*0.010*
of which mobile payments	*75,039*	*4,801,997*	*0.065*	*152,726*	*9,566,583*	*0.056*	*98,610*	*6,066,551*	*0.018*
Remote payments (excl. internet)	**77,941**	**10,604,251**	**0.191**	**120,708**	**24,857,056**	**0.187**	**118,903**	**22,602,626**	**0.185**
Internet payments	**2,577,337**	**191,873,234**	**0.135**	**1,874,565**	**145,299,292**	**0.099**	**1,913,224**	**152,815,486**	**0.093**
of which 3-D Secure payments with strong authentication	267,556	69,544,332	0.096	314,967	72,922,674	0.082	314,857	72,017,359	0.068
of which payments excl. 3-D Secure with strong authentication	na	na	na	na	na	na	36,576	2,353,042	0.121
of which 3-D Secure payments without strong authentication	159,344	11,208,886	0.071	342,714	17,460,124	0.070	258,701	12,634,204	0.055
of which payments excl. 3-D Secure without strong authentication	2,150,437	111,120,015	0.205	1,216,884	54,916,494	0.168	1,303,090	65,810,881	0.193
of which MIT	*na*	*na*	*na*	*na*	*na*	*na*	*1,044,582*	*49,260,633*	*0.196*
of which "one-leg" payments	*na*	*na*	*na*	*na*	*na*	*na*	*0*	*0*	*0.000*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*70,590*	*4,496,448*	*0.100*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*187,918*	*12,053,800*	*0.273*
Withdrawals	**121,642**	**41,437,842**	**0.035**	**115,643**	**41,344,934**	**0.032**	**102,357**	**38,832,083**	**0.030**
Total	**3,602,245**	**287,430,944**	**0.040**	**3,100,370**	**265,094,880**	**0.033**	**3,020,017**	**264,527,216**	**0.031**

na, not available.

Source: Observatory for the Security of Payment Means.

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

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

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

T11 Breakdown of remote fraud by sector of activity involving domestic transactions in 2023

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

	Transactions		Fraud		Fraud rate	
	Volume	Value	Volume	Value	Volume (‰)	Value (%)
General and semi-general trade	743,394,922	43,609,426,035	345,222	27,987,056	0.464	0.064
Technical and cultural products (books, dvds, computers, audio, photo, video, household appliances)	142,806,627	6,598,626,354	296,264	17,591,684	2.075	0.267
Travel and transportation	282,064,146	26,693,359,943	204,572	18,623,728	0.725	0.070
Telephony and communication	410,678,797	15,141,508,530	273,643	21,255,918	0.666	0.140
Food	32,190,669	2,500,508,834	15,102	1,373,571	0.469	0.055
Household goods, furnishings and DIY	70,571,937	12,134,281,628	39,672	14,390,135	0.562	0.119
Insurance	13,105,332	2,579,914,202	4,396	592,659	0.335	0.023
Health, beauty and personal care	44,992,745	2,911,493,933	22,083	1,943,418	0.491	0.067
Personal and professional services	514,891,901	38,017,635,080	646,729	43,168,306	1.256	0.114
Account loading and person-to-person sales	122,260,388	11,661,875,830	112,888	20,409,951	0.923	0.175
Online gaming	134,297,474	4,189,186,895	41,239	2,956,047	0.307	0.071
Miscellaneous	152,352,304	10,872,113,907	30,317	5,125,639	0.199	0.047
Total	**2,663,607,242**	**176,909,931,171**	**2,032,127**	**175,418,112**	**0.763**	**0.099**

Source: Observatory for the Security of Payment Means.

T12 Payments by cards accepted in France

(volume in thousands, value in EUR thousands)

	2018		2019		2020	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**11,286,513**	**453,608,003**	**12,277,149**	**468,895,511**	**11,284,433**	**428,180,387**
of which contactless payments (incl. mobile payments)	*2,370,247*	*25,007,584*	*3,802,953*	*42,931,374*	*5,187,488*	*79,877,184*
of which mobile payments	*11,911*	*209,710*	*56,169*	*1,014,657*	*145,527*	*2,979,437*
Remote payments (excl. internet)	**50,543**	**5,757,108**	**48,998**	**5,586,755**	**69,950**	**7,087,913**
Internet payments	**1,652,894**	**112,607,104**	**1,906,065**	**121,920,272**	**2,158,226**	**132,554,575**
Withdrawals	**1,418,919**	**136,201,131**	**1,375,145**	**136,636,741**	**1,062,376**	**116,986,747**
Total	**14,408,869**	**708,173,346**	**15,607,358**	**733,039,279**	**14,574,985**	**684,809,622**

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

T12 Payments by cards accepted in France (continued)

(volume in thousands, value in EUR thousands)

	2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value
Face-to-face payments and UPT	**13,031,098**	**480,804,099**	**15,093,611**	**551,753,133**	**16,159,605**	**588,228,633**
of which contactless payments (incl. mobile payments)	*7,437,197*	*125,344,168*	*9,248,429*	*149,971,446*	*10,982,717*	*178,132,864*
of which mobile payments	*388,175*	*8,403,747*	*897,307*	*19,846,999*	*1,716,563*	*39,282,385*
Remote payments (excl. internet)	**64,620**	**7,272,724**	**107,228**	**18,523,094**	**105,756**	**18,799,343**
Internet payments	**2,565,276**	**155,816,405**	**2,589,260**	**166,197,062**	**2,821,038**	**190,607,365**
of which 3-D Secure payments with strong authentication	*708,194*	*78,650,830*	*871,961*	*99,937,461*	*1,049,797*	*120,158,448*
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*86,343*	*3,228,632*
of which 3-D Secure payments without strong authentication	*409,008*	*18,152,505*	*748,083*	*27,403,752*	*707,064*	*26,605,058*
of which payments excl. 3-D Secure without strong authentication	*1,448,074*	*59,013,071*	*969,216*	*38,855,848*	*977,834*	*40,615,228*
of which MIT	*na*	*na*	*na*	*na*	*730,327*	*26,600,426*
of which "one-leg" payments	*na*	*na*	*na*	*na*	*13,616*	*1,740,365*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*101,735*	*5,110,587*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*132,156*	*7,163,850*
Withdrawals	**1,083,643**	**125,105,264**	**1,134,543**	**134,637,455**	**1,117,986**	**135,559,666**
Total	**16,744,636**	**768,998,491**	**18,924,643**	**871,110,743**	**20,204,386**	**933,195,008**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, the card issuer is located outside the European Union; MIT, Merchant Initiated Transaction; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

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

T13 Fraudulent transactions using cards accepted in France

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

	2018			2019			2020		
	Volume	Value	Fraude rate by value	Volume	Value	Fraude rate by value	Volume	Value	Fraude rate by value
Face-to-face payments and UPT	**1,064,889**	**58,485,280**	**0.0129**	**1,170,399**	**64,448,538**	**0.0137**	**841,280**	**42,883,367**	**0.0100**
of which contactless payments (incl. mobile payments)	*438,088*	*5,174,314*	*0.0207*	*602,309*	*8,534,090*	*0.0199*	*538,313*	*12,238,895*	*0.0153*
of which mobile payments	*1,915*	*64,599*	*0.0308*	*3,890*	*307,230*	*0.0303*	*35,968*	*3,640,684*	*0.1222*
Remote payments (excl. internet)	**206,957**	**27,274,865**	**0.4738**	**108,259**	**23,167,505**	**0.4147**	**105,972**	**17,644,315**	**0.2489**
Internet payments	**2,537,264**	**225,819,184**	**0.2005**	**2,989,333**	**232,763,441**	**0.1909**	**3,176,400**	**248,966,265**	**0.1878**
Withdrawals	**114,727**	**32,353,075**	**0.0238**	**127,005**	**37,354,814**	**0.0273**	**104,960**	**33,084,175**	**0.0283**
Total	**3,923,837**	**343,932,404**	**0.0486**	**4,394,996**	**357,734,298**	**0.0488**	**4,228,612**	**342,578,122**	**0.0500**

Source: Observatory for the Security of Payment Means.

Note: UPT, Unattended Payment Terminal.

T13 Fraudulent transactions using cards accepted in France (continued)

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

	2021			2022			2023		
	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value	Volume	Value	Fraud rate by value
Face-to-face payments and UPT	**874,166**	**49,441,754**	**0.0103**	**1,084,701**	**67,409,965**	**0.0122**	**999,344**	**67,688,751**	**0.0115**
of which contactless payments (incl. mobile payments)	601,803	15,600,613	0.0124	819,535	24,406,015	0.0163	769,976	21,898,465	0.0123
of which mobile payments	*84,421*	*5,793,427*	*0.0689*	*170,752*	*12,007,511*	*0.0605*	*127,622*	*10,042,616*	*0.0256*
Remote payments (excl. internet)	**96,257**	**15,211,163**	**0.2092**	**144,965**	**35,446,137**	**0.1914**	**142,763**	**32,984,939**	**0.1755**
Internet payments	**2,885,920**	**227,162,875**	**0.1458**	**2,252,283**	**190,461,573**	**0.1146**	**2,337,170**	**201,724,304**	**0.1058**
of which 3-D Secure payments with strong authentication	306,265	76,891,633	0.0978	346,366	80,959,973	0.0810	354,651	83,805,192	0.0697
of which payments excl. 3-D Secure with strong authentication	*na*	*na*	*na*	*na*	*na*	*na*	*71,563*	*5,522,986*	*0.1711*
of which 3-D Secure payments without strong authentication	*213,403*	*20,406,481*	*0.1124*	*405,445*	*26,105,266*	*0.0953*	*342,878*	*20,687,862*	*0.0778*
of which payments excl. 3-D Secure without strong authentication	*2,366,252*	*129,864,761*	*0.2201*	*1,500,472*	*83,396,334*	*0.2146*	*1,568,078*	*91,708,264*	*0.2258*
of which MIT	*na*	*na*	*na*	*na*	*na*	*na*	*1,098,829*	*52,343,346*	*0.1968*
of which "one-leg" payments	*na*	*na*	*na*	*na*	*na*	*na*	*92,524*	*12,994,451*	*0.7467*
of which PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*80,195*	*5,068,095*	*0.0992*
of which non-PSD 2 compliant non-3-D Secure payments	*na*	*na*	*na*	*na*	*na*	*na*	*296,530*	*21,302,372*	*0.2974*
Withdrawals	**124,077**	**42,256,276**	**0.0338**	**120,217**	**42,811,637**	**0.0318**	**106,749**	**40,292,502**	**0.0297**
Total	**3,980,420**	**334,072,068**	**0.0434**	**3,602,166**	**336,129,312**	**0.0386**	**3,586,026**	**342,690,496**	**0.0367**

na, not available.

Source: Observatory for the Security of Payment Means.

Note: One-leg, the card issuer is located outside the European Union; MIT, Merchant Initiated Transaction; PSD 2, second Payment Services Directive; UPT, Unattended Payment Terminal.

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

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

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

T13 *quater* Breakdown of fraud involving payments by cards accepted in France in 2023

T13 *quinquies* Geographical breakdown of fraud involving cards accepted in France in 2023

CHEQUES

T14 Cheques exchanged

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

	2018	2019	2020	2021	2022	2023
Volume	1,746.9	1,586.5	1,175.5	1,105.8	1,008.0	891.5
Value	891.1	814.5	614.2	588.6	539.8	467.2
Average value	**510.1**	**513.4**	**522.5**	**532.3**	**535.5**	**524.1**

Source: Observatory for the Security of Payment Means.

T14 *bis* Detailed volume of cheques exchanged

T15 Cheque fraud

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

a) Old approach

	2018	2019	2020	2021	2022	2023
Volume	**166,421**	**183,488**	**220,685**	**272,970**	**266,216**	**253,338**
Fraud rate (‰)	0.095	0.116	0.188	0.247	0.264	0.284
Value	**450,108,464**	**539,215,175**	**538,059,139**	**625,703,442**	**556,796,815**	**585,506,445**
Fraud rate (%)	0.051	0.066	0.088	0.106	0.103	0.125
Average value	**2,705**	**2,939**	**2,438**	**2,292**	**2,092**	**2,311**

b) New approach

	2018	2019	2020	2021	2022	2023
Volume	**na**	**na**	**190,001**	**232,277**	**218,122**	**203,514**
Fraud rate (‰)			0.162	0.210	0.216	0.228
Value	**na**	**na**	**401,611,189**	**465,021,167**	**395,416,196**	**363,549,771**
Fraud rate (%)			0.065	0.079	0.073	0.078
Average value	**na**	**na**	**2,114**	**2,002**	**1,813**	**1,786**

na, not available.

Source: Observatory for the Security of Payment Means.

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

T16 Types of cheque fraud

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

	2018		2019		2020		2021		2022		2023	
	Volume/ value	Share	Volume/ value	Share	Volume/ value	Share	Volume/ value	Share	Volume/ value	Share	Volume/ value	Share
Volume												
Theft, loss	138,358	83.1	154,211	84.0	196,754	89.2	244,750	89.7	237,854	89.3	225,786	89.1
Forgery	17,178	10.3	16,459	9.0	13,894	6.3	18,074	6.6	18,885	7.1	18,009	7.1
Counterfeiting	8,092	4.9	9,574	5.2	7,207	3.3	5,119	1.9	5,969	2.2	5,700	2.2
Misappropriation, replay	2,793	1.7	3,244	1.8	2,830	1.3	5,026	1.8	3,508	1.3	3,843	1.5
Value												
Theft, loss	252,890,727	56.2	296,367,562	55.0	365,813,764	68.0	398,739,224	63.7	375,576,575	67.5	384,036,365	65.6
Forgery	145,737,424	32.4	145,881,745	27.1	102,801,337	19.1	100,395,756	16.0	93,152,894	16.7	100,520,775	17.2
Counterfeiting	36,739,051	8.2	76,511,582	14.2	32,340,420	6.0	33,725,041	5.4	32,648,566	5.9	29,819,343	5.1
Misappropriation, replay	14,741,262	3.3	20,454,286	3.8	37,103,618	6.9	92,823,421	14.8	55,418,781	10.0	71,129,963	12.1

Source: Observatory for the Security of Payment Means.

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

T17 Credit transfers issued by type

(volume in millions, value in EUR millions)

	2018		2019		2020		2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Total	**4,038**	**24,211,142**	**4,251**	**25,879,217**	**4,483**	**32,713,128**	**4,843**	**38,722,734**	**5,158**	**38,894,879**	**5,658**	**30,588,908**
of which SEPA Credit Transfers	*3,974*	*10,846,914*	*4,174*	*9,602,866*	*4,384*	*10,029,108*	*4,668*	*12,980,883*	*4,689*	*9,655,892*	*4,869*	*9,921,539*
of which SEPA Instant Transfers – SCT Inst	*0*	*86*	*14*	*7,074*	*45*	*26,243*	*107*	*50,053*	*198*	*118,972*	*364*	*174,049*
of which LVT[a)]	*10*	*10,130,586*	*9*	*12,266,316*	*9*	*19,042,030*	*9*	*19,661,685*	*19*	*15,907,892*	*73*	*8,757,890*
of which other transfers	*53*	*3,233,556*	*54*	*4,002,960*	*45*	*3,615,748*	*59*	*6,030,114*	*252*	*13,212,124*	*351*	*11,735,430*
Total – excluding LVT	**4,028**	**14,080,556**	**4,242**	**13,612,900**	**4,474**	**13,671,098**	**4,834**	**19,061,050**	**5,138**	**22,986,988**	**5,585**	**21,831,018**

a) Large-value transfers issued via Target2 or Euro1.

Source: Observatory for the Security of Payment Means.

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

T17 *bis* Credit transfers issued by initiation channel

T17 *ter* Credit transfers issued by geographical destination

T18 Fraudulent transactions by type of credit transfer

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

	2018			2019			2020		
	Volume	Value		Volume	Value		Volume	Value	
		Value	Fraude rate		Value	Fraude rate		Value	Fraude rate
Total	**7,736**	**97,327,128**	**0.0004**	**15,934**	**161,642,174**	**0.0006**	**35,893**	**266,969,099**	**0.0008**
of which SEPA Credit Transfers	*6,521*	*78,314,614*	*0.0007*	*13,302*	*127,572,549*	*0.0013*	25,254	191,474,396	0.0019
of which SEPA Instant Transfers – SCT Inst	*5*	*29,800*	*0.0345*	*729*	*2,203,240*	*0.0311*	7,131	10,562,419	0.0402
of which LVT[a)]	*14*	*4,622,598*	*0.0000*	*15*	*15,476,053*	*0.0001*	51	2,439,224	0.0000
of which other transfers	*1,196*	*14,360,116*	*0.0004*	*1,888*	*16,390,332*	*0.0004*	3,457	62,493,060	0.0017
Total – excluding LVT	**7,722**	**92,704,530**	**0.0007**	**15,919**	**146,166,121**	**0.0011**	**35,842**	**264,529,875**	**0.0019**

a) Large-value transfers issued via Target2 or Euro1.

Source: Observatory for the Security of Payment Means.

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

T18 Fraudulent transactions by type of credit transfer (continued)

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

	2021			2022			2023		
	Volume	Value		Volume	Value		Volume	Value	
		Value	Fraud rate		Value	Fraud rate		Value	Fraud rate
Total	**46,718**	**287,264,068**	**0.0007**	**76,846**	**313,163,442**	**0.0008**	**90,436**	**311,627,465**	**0.0010**
of which SEPA Credit Transfers	*33,199*	*246,527,533*	*0.0019*	*40,874*	*205,737,587*	*0.0021*	*38,625*	*202,099,216*	*0.0020*
of which SEPA Instant Transfers – SCT Inst	*12,913*	*22,406,942*	*0.0448*	*33,193*	*52,768,218*	*0.0444*	*48,630*	*69,003,730*	*0.0396*
of which LVT[a)]	*5*	*1,539,120*	*0.0000*	*49*	*1,934,774*	*0.0000*	*32*	*9,828,077*	*0.0001*
of which other transfers	*601*	*16,790,473*	*0.0003*	*2,730*	*52,722,863*	*0.0004*	*3,149*	*30,696,443*	*0.0003*
Total – excluding LVT	**46,713**	**285,724,948**	**0.0015**	**76,797**	**311,228,668**	**0.0014**	**90,404**	**301,799,388**	**0.0014**

a) Large-value transfers issued via Target2 or Euro1.

Source: Observatory for the Security of Payment Means.

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

T18 *bis* Fraudulent transactions by transfer initiation channel

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

T19 Total fraud on credit transfers

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

	2018	2019	2020	2021	2022	2023
Volume	**7,736**	**15,934**	**35,893**	**46,718**	**76,846**	**90,436**
Rate (%)	0.0019	0.0037	0.0080	0.0096	0.0149	0.0160
Value	**97,327,128**	**161,642,174**	**266,969,099**	**287,264,068**	**313,163,442**	**311,627,465**
Rate (%)	0.0004	0.0006	0.0008	0.0007	0.0008	0.0010
Average value	**12,581**	**10,144**	**7,438**	**6,149**	**4,075**	**3,446**

Source: Observatory for the Security of Payment Means.

T20 Fraud on credit transfers by type

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

	2018		2019		2020		2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Deceit	**5,525**	**51,069,661**	**13,769**	**98,525,485**	**28,211**	**87,061,255**	**35,865**	**87,370,131**	**57,443**	**120,006,990**	**63,528**	**135,231,281**
Share	71.4	52.5	86.4	61.0	78.6	32.6	76.8	30.4	74.8	38.3	70.2	43.4
Forgery	**151**	**485,131**	**125**	**3,438,923**	**203**	**3,377,807**	**875**	**5,387,862**	**179**	**2,838,371**	**269**	**2,293,923**
Share	2.0	0.5	1.6	2.1	0.6	1.3	1.9	1.9	0.2	0.9	0.3	0.7
Misappropriation	**1,037**	**40,250,639**	**1,534**	**56,514,755**	**5,731**	**157,318,883**	**8,523**	**168,094,274**	**16,991**	**148,732,203**	**24,997**	**150,088,618**
Share	13.4	41.4	19.8	35.0	16.0	58.9	18.2	58.5	22.1	47.5	27.6	48.2
Other	**1,023**	**5,521,697**	**506**	**3,163,011**	**1,748**	**19,211,154**	**1,455**	**26,411,801**	**2,233**	**41,585,878**	**1,642**	**24,013,643**
Share	13.2	5.7	3.2	2.0	4.9	7.2	3.1	9.2	2.9	13.3	1.8	7.7

Source: Observatory for the Security of Payment Means.

T21 Direct debits issued by type of mandate

(volume in millions, value in EUR millions)

	2018		2019		2020		2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Total	**4,211**	**1,644,553**	**4,370**	**1,710,931**	**4,622**	**1,684,258**	**5,020**	**1,895,098**	**4,914**	**2,040,963**	**4,621**	**2,139,398**
Breakdown of direct debits by type of mandate												
Direct debit by electronic mandate	na	na	na	na	na	na	1,106	430,781	1,357	1,045,754	1,254	1,021,908
Direct debit by paper-based mandate	na	na	na	na	na	na	3,914	1,464,317	3,558	995,210	3,366	1,117,490
Breakdown of direct debits by initiation method												
Direct debits initiated in a file/batch	4,151	1,609,405	4,312	1,672,338	4,560	1,647,504	4,936	1,819,420	4,645	1,929,438	4,247	2,010,766
Direct debits initiated on the basis of a single payment	60	35,148	58	38,593	61	36,754	84	75,678	269	111,525	374	128,632

na, not available.

Source: Observatory for the Security of Payment Means.

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

T22 Direct debit fraud

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

	2018	2019	2020	2021	2022	2023
Volume	**309,377**	**43,519**	**6,485**	**251,010**	**49,453**	**77,876**
Fraud rate (%)	0.0735	0.0100	0.0014	0.0500	0.0101	0.0169
Value	**58,346,253**	**10,990,025**	**1,891,051**	**25,318,677**	**19,853,012**	**22,320,813**
Fraud rate (%)	0.0035	0.0006	0.0001	0.0013	0.0010	0.0010
Average value	**189**	**253**	**292**	**101**	**401**	**287**

Source: Observatory for the Security of Payment Means.

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

T22 *ter* Fraudulent direct debits by type of mandate

T23 Types of direct debit fraud

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

	2018		2019		2020		2021		2022		2023	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Deceit	**309,302**	**58,329,283**	**14,601**	**3,961,260**	**6,011**	**1,388,326**	**250,493**	**25,201,709**	**43,788**	**14,206,533**	**70,212**	**22,003,546**
Share	100.0	100.0	33.6	36.0	92.7	73.4	99.8	99.5	88.5	71.6	90.2	98.6
Misappropriation	**72**	**16,703**	**26,223**	**6,677,467**	**62**	**10,720**	**517**	**116,968**	**5,665**	**5,646,479**	**7,664**	**317,267**
Share	0.0	0.0	60.3	60.8	1.0	0.6	0.2	0.5	11.5	28.4	9.8	1.4

Source: Observatory for the Security of Payment Means.

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

Electronic money

T24 Number of instruments from providers authorised or established in France

T25 Use of electronic money by type of transaction

T26 Fraudulent electronic money transactions

Commercial papers: bills of exchange and promissory notes

T27 Payments by commercial papers

T28 Types of commercial paper fraud

Money remittances

T29 Transactions by remittances

T30 Fraudulent transactions on remittances

Payment initiation services

T31 Transactions initiated by an institution acting as payment initiation service provider (paragraph 7 of Article L. 314-1 of the French Monetary and Financial Code)

T32 Fraudulent transactions initiated by an institution acting as payment initiation service provider (paragraph 7 of Article L. 314-1 of the French Monetary and Financial Code)

Published by
Banque de France

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

Editor-in-Chief
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, Yolaine Fischer, Anne-Marie Fourel, Trân Huynh, Marc-Antoine Jambu, Isabelle Maranghi, Adrien Mocek, Cyril Ronfort, Marine Soubielle

Technical production
Studio Création
Press and Communication Directorate

Contact
Observatory for the Security of Payment Means
Internal mail code: S2B-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Legal deposit
September 2024
ISSN 2557-1230 (online version)
ISSN 2556-4536 (printed)

Internet
www.observatoire-paiements.fr

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

www.banque-france.fr