OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2021

www.observatoire-paiements.fr

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2021

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

JULY 2022

CHAPTERS

APPENDICES

Chapter 3 and Appendices 1 and 2 are available in French only in the original version of the report, which can be found here: *https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021*

Appendices 3, 4 and 5 are available in English in this report.

All tables in Annex 6 can be downloaded in English at the following address: *https://www.banque-france.fr/en/2021-statistics-appendix-6-annual-report*

SUMMARY

Following a year marked by the measures related to the health crisis in 2020, 2021 saw an economic recovery and an associated rebound in payment flows, with consumers confirming their new, more digital and dematerialised practices, which have now become firmly established. In this 2021 Annual Report, the Observatoire de la sécurité des moyens de paiement *(OSMP – the Observatory for the Security of Payment Means) notes that this digitisation was accompanied by new threats to payment means, with a marked rise in scams and manipulative schemes. Against this backdrop, thanks to the actions undertaken by the Observatory and professionals in the payment industry, combined with the vigilance of users, it was possible to maintain a high level of security and confidence in cashless payment means in 2021.*

Chapter 1 of the report presents changes in payment flows and fraud in 2021. *The easing of health measures and the resulting economic recovery led to very strong growth in cashless transactions (up 12.4% in volume and 17.5% in value), which exceeded economic growth, thus confirming the rapid and sustained digitisation of payment practices.*

Bank card payments continued to account for the largest share of cashless transactions, at nearly 61%. With the pandemic, contactless payments have become the preferred method of point-of-sale payments, accounting for more than half of all face-to-face card payments (57%). Even though mobile contactless payments still account for only 3% of point-of-sale transactions, they also tripled in 2021, suggesting a strong increase in their use in coming years. Lastly, online payments continued to grow strongly (up 21% in 2021), still driven by the growth of e-commerce and new consumption habits (collection from stores of purchases made remotely, such as drive or click & collect, home deliveries of quick commerce[1] purchases, online subscriptions, etc.).

- *Alongside bank cards, instant transfers are also becoming an integral part of the cashless payment landscape. Their use more than doubled in 2021, and now accounts for more than 2% of total transfers. Although still lagging behind other European countries, their use in France is expected to rise in the coming years, reflecting national and European payment means strategies.*

- *At the same time, despite the economic recovery, traditional payment methods are still declining. Cheque use is continuing to fall, albeit at a slower pace than before the pandemic, with a 6% drop in volume and a 4% drop in value. With the easing of health measures, card cash withdrawals held up better (up 2.1% in volume), although their growth was lower than that of total transactions.*

Against this background of a very strong increase in cashless transactions, partly linked to a catch-up effect after an atypical year in 2020, the Observatory's statistical monitoring shows that fraud observed for payments made in France increased in value twice as slowly as that of flows, to reach EUR 1.2 billion (up 8.5%), and decreased in volume to 7.5 million fraudulent transactions (down 3.8%). This encouraging result reflects differing trends across payment means.

1 Quick commerce is online shopping – usually using a mobile phone – combined with the promise of very fast home delivery, from a few minutes to a few hours. Quick commerce has developed particularly in the food sector.

- *For the fourth year in a row, cheques continue to suffer from the highest fraud rate of 0.079%. They accounted for 37% of total fraud in 2021, or EUR 465 million. These figures reflect a new approach to cheque fraud, more in line with losses actually sustained, insofar as the Observatory now excludes fraud attempts that were prevented by banks after the cheque was deposited (EUR 161 million of frauds prevented in 2021 to be deducted from EUR 626 million of fraudulent cheque transactions).*

- *Bank cards are very similar to cheques in terms of fraud amounts: 37% of total fraud in 2021, or EUR 464 million. Despite an increase in the use of this payment instrument, 2021 nevertheless saw a significant 1.9% drop in fraud in value and in the fraud rate (0.059%, against 0.068% in 2020). The Observatory estimates that 1.3 million cards were subject to fraud and reported lost or stolen in 2021, down 10% on 2020. These results confirm the effectiveness of the use of strong customer authentication for remote payments, provided for in the Second European Payment Services Directive (PSD2), which was gradually implemented in France in 2021 as part of the migration plan managed by the Observatory. Accordingly, the fraud rate on remote payments fell from 0.249% in 2020 to 0.196% in 2021 (down 21%), its lowest level ever. With the risk of phishing still high, misappropriated card numbers remain the main source of card fraud (78% of fraud, compared to 18% for lost or stolen cards), such that online payments still account for almost three-quarters of fraud in terms of value, even though they represent less than a quarter of card payments. At the same time, contactless payments continue to offer a very high level of security, with the fraud rate reaching an all-time low of 0.013%, almost equivalent to the 0.010% rate recorded for traditional point-of-sale payments with PIN code.*

- *Credit transfers continue to have the third highest incidence of fraud of all payment means (23% of total fraud, or EUR 287 million). However, in a context of increasing flows and the predominant use of transfers for retail payments (wages, social security benefits, etc.), the fraud rate by transfer remains particularly low and contained at 0.0007% (0.0015% excluding large-value transfers), down slightly from 2020. Fraud rates were limited for both online banking transfers, mainly used by individuals (0.0012%), as well as for transfers via telematic channels, used by businesses and government (0.0006%). Furthermore, with the sharp increase in flows, the security of instant transfers was ensured with only a slight rise in the fraud rate to 0.045%, which is very similar to card payments in France. The Observatory notes that misappropriation of transfers, i.e. situations where the initiator of the transaction is legitimate but is manipulated or deceived by the fraudster, is the most common type of fraud (59% of total fraud in value terms). These cases of fraud affect businesses, government and individuals alike, as fraudsters manage to bypass authentication mechanisms. The steady rise in remote interactions and identity or bank detail theft are conducive to the direct manipulation of users, who must continue to be made aware of these risks. Given these risks, the Observatory will actively participate in discussions aimed at identifying new ways of combating credit transfer fraud that would benefit banking institutions and their users.*

- *After these three payment instruments, fraud amounts for direct debits, trade bills, e-money and remittances are relatively insignificant. The Observatory nevertheless notes an increase in direct debit fraud, which amounted to EUR 25 million in 2021, compared to less than EUR 2 million in 2020, and whose fraud rate (0.0013%) has been particularly volatile year-on-year over the past four years. The reason for this increase, attributable to a very small number of creditors, was identified. Corrective measures are being implemented to remedy this.*

Chapter 2 gives a positive assessment of the work carried out by the Observatory in 2021 to improve the security of payment means.

- *The first is the implementation of strong authentication measures for online card payments, which has been managed by the Observatory since the publication of its migration plan for the French financial sector in autumn 2019 (see 2018 Annual Report). The Observatory is pleased to note that the French financial sector has achieved a very high level of compliance with the requirements of PSD2, both in terms of cardholders' equipment and transaction processing by merchants and the payment chain. The Observatory welcomes the fact that these strong authentication measures have already led to a significant reduction in online payment fraud, while at the same time supporting the growth of e-commerce and related new consumption patterns. In 2022, the Observatory will focus on consolidating the performance of these new authentication infrastructures, while continuing to combat fraud aimed at circumventing strong authentication by manipulating the payer.*

- *One year after the publication of ten new recommendations on cheque security (see 2020 Annual Report), the*

Observatory has issued an encouraging progress report on several concrete actions taken by both public authorities and industry professionals, such as the revision of the Banque de France's cheque security framework, which was completed in April 2022. However, given the persistently high levels of fraud, the Observatory calls on the industry to continue and intensify its efforts to strengthen the security of this declining payment instrument, in particular by focusing on monitoring cheque transactions, simplifying the procedures for reporting lost or stolen cheques and securing the delivery of chequebooks. Taking into account the controls already carried out and the risk policy of each institution, the Banque de France will ensure that the Observatory's recommendations are duly implemented by the banking institutions as part of its oversight activities.

- *Lastly, the Observatory would like to remind both payment industry professionals and users of the relevance of its recommendations regarding certain rapidly growing practices, which the Observatory had covered in its monitoring work in previous years. This includes pursuing efforts and investments to strengthen the security of instant credit transfers in order to ensure the rapid and secure development of this payment instrument, which is expected to grow strongly, raising users' awareness of the need to protect their own payment data given the ongoing high risk of phishing, and strengthening the security of enrolments for mobile payment solutions.*

Chapter 3 presents the Observatory's monitoring of the digital identity of natural persons. *The Observatory notes that the strong growth in digital practices has not been accompanied by an attendant strengthening of remote identification processes. This has led to an increase in identity theft, often associated with document fraud techniques, which also undermine the security of payment means by deceiving one of the parties to the transaction. While the French government is developing and testing an administrative digital identity, associated with the new electronic national identity card, the Observatory is already calling on the players in the payment chain, as well as users, to make greater use of digital identity solutions and trust services, such as the electronic signature or seal, which offer more robust levels of security for remote exchanges.*

In a context of rapidly evolving payment means and constant new threats, the Observatory remains committed to ensuring the security of all payment means, whether they are in decline, such as cheques, or expected to develop in coming years, such as instant transfers or mobile payments. The security of all payment means is a prerequisite for offering all users, from individuals to businesses, genuine freedom of choice in their daily use.

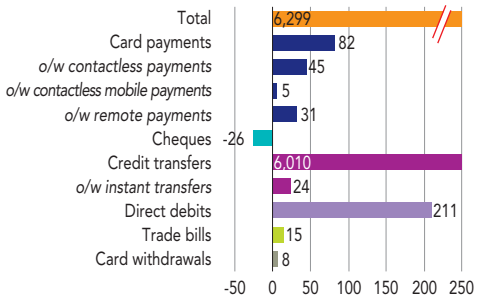
1

FRAUD IN 2021

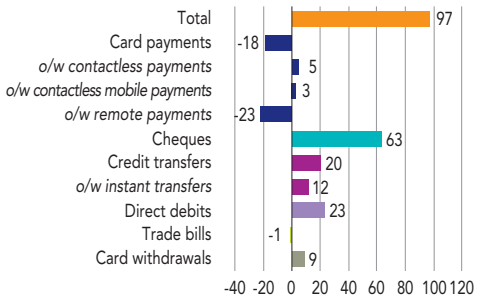
Key data

C1 Change in payment means between 2020 and 2021

a) Payment flows (EUR billions)



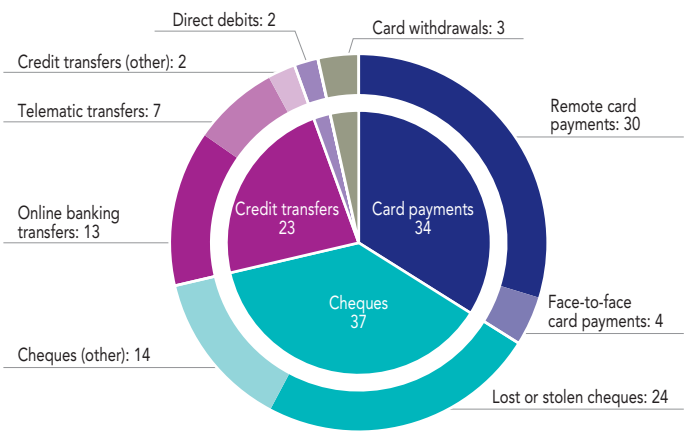
b) Fraud (EUR millions)



Source: Observatory for the Security of Payment Means.

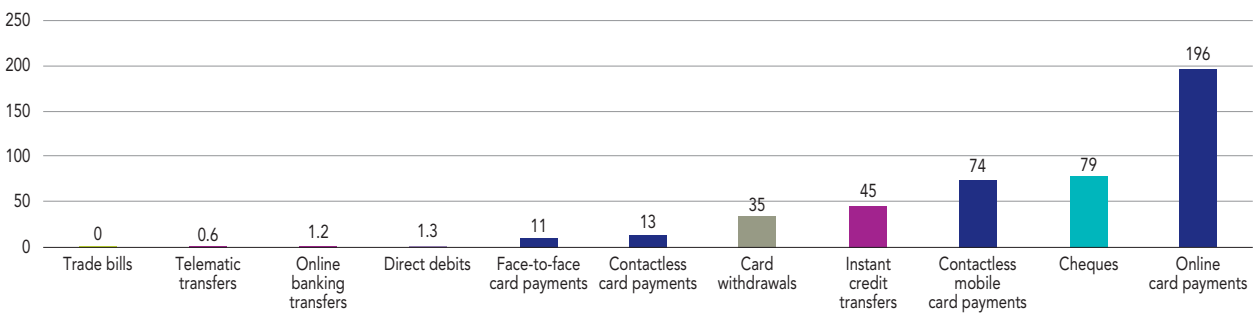
Note: The change in fraud between 2020 and 2021 (Chart b) is presented here at constant methodology and scope, by applying the new approach to measuring cheque fraud over the two years.

C2 Main sources of fraud in value terms (%)



Source: Observatory for the Security of Payment Means.

C3 Vulnerability to fraud of the main payment means (in euro of fraud per EUR 100,000 of payment)



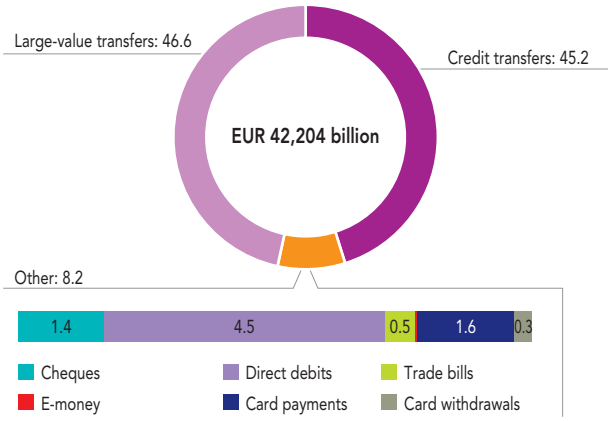
Source: Observatory for the Security of Payment Means.

1.1 Overview

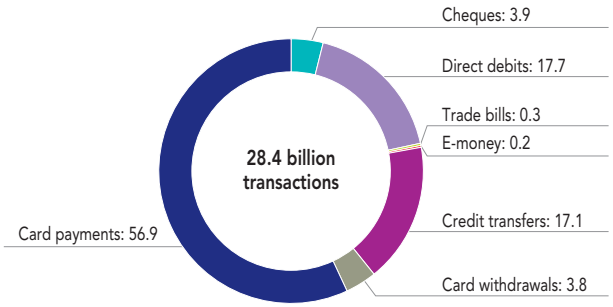
1.1.1 Means of payment

C4 Use of cashless payment means in France in 2021 (%)

a) In value terms



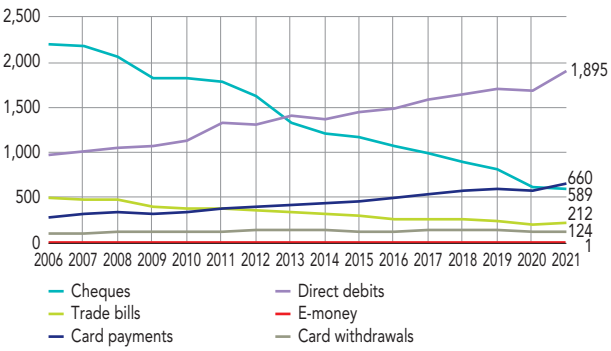
b) In volume terms



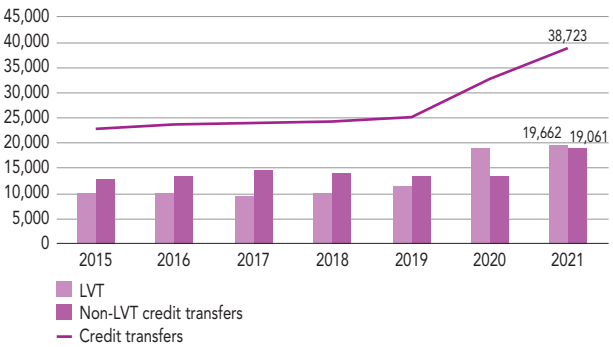
Source: Observatory for the Security of Payment Means.

C5 Payment flows in value terms (EUR billions)

a) By instrument (excl. credit transfers)



b) By credit transfer



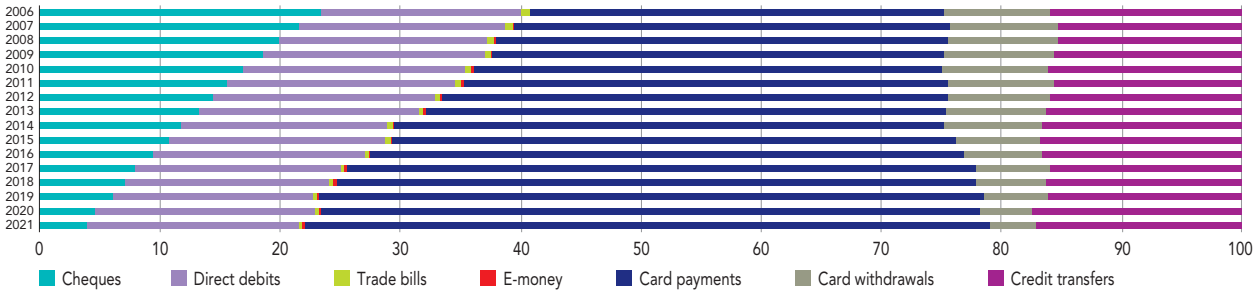
Source: Observatory for the Security of Payment Means.
Note: LVT – large-value transfer.

Against a backdrop of an easing of health measures and the resulting economic recovery, cashless transactions by individuals, businesses and public administrations reached 28.4 billion in 2021 (up 12% compared with 2020), with a total value of EUR 42,204 billion (up 17.5%).

Credit transfers took the lion's share of total flows, at 92%. This is mainly due to the weight of large-value transfers (LVTs), i.e. flows issued through large-value payment systems (Target 2 and Euro1) reserved for professional payments. These accounted for 51% of transfer values, for only 0.2% of the volume of these transactions.

Bank cards continued to be the most widely used cashless payment method in terms of the number of transactions, and their share in the volume of transaction, excluding card withdrawals, rose from 54.7% in 2020 to 56.9% in 2021. Conversely, cheques continued to decline, in terms of both volume and value. For the first time in 2021, card payments exceeded cheque transactions in value terms (EUR 660 billion compared with EUR 58 billion).

C6 Change in payment flows in volume terms (%)

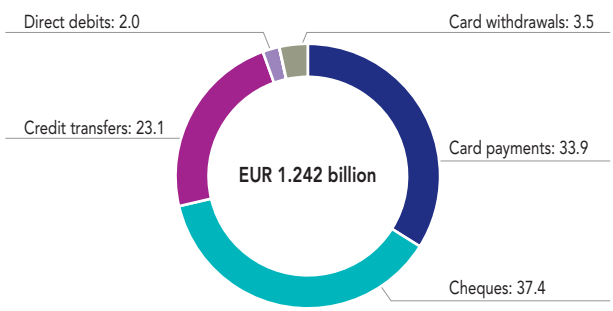


Source: Observatory for the Security of Payment Means.

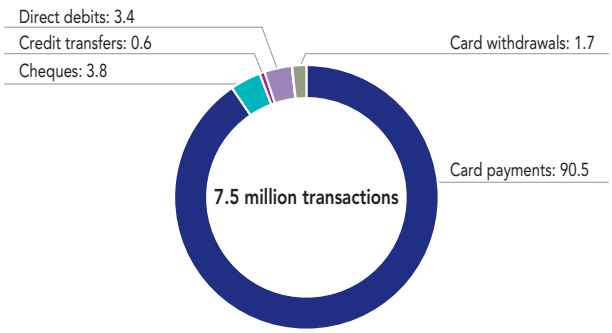
1.1.2 Fraud targeting means of payment

C7 Breakdown of fraud (%)

a) In value terms

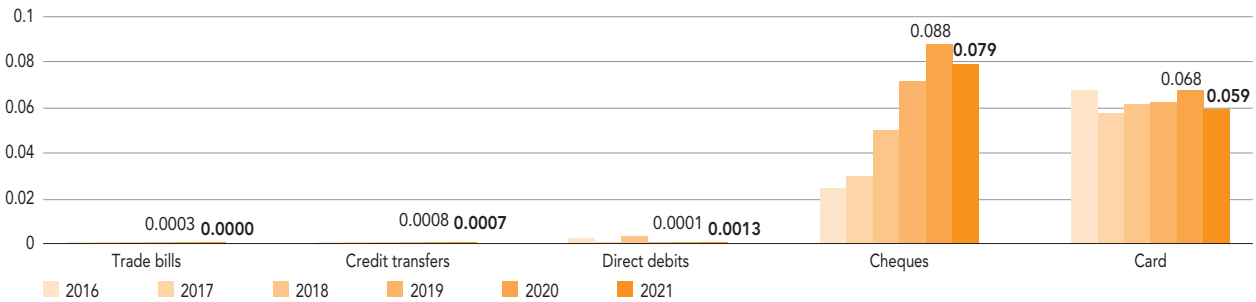


b) In volume terms



Source: Observatory for the Security of Payment Means.

C8 Change in fraud rate for each payment means (%)



Source: Observatory for the Security of Payment Means.

In 2021, 7.5 million fraudulent cashless transactions were perpetrated (down 3.8% compared with 2020), for a total fraud amount of EUR 1.242 billion (up 8.5% at constant methodology and scope).

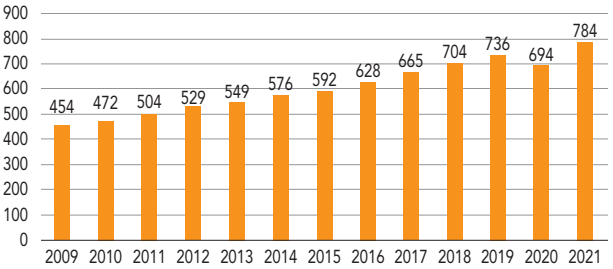
Cheques remained the most widely used means of payment for fraudulent purposes, but their share in fraud values fell from 42% in 2020 to 37% in 2021, due to a new approach to reporting fraud that is closer to the reality of the losses incurred. The share of fraud on cards – including withdrawals – remained stable at 37%, on a par with cheques, despite a shift towards higher risk internet sales channels. Cards – including withdrawals – still accounted for the bulk of the volume of fraudulent transactions, although their share decreased from 97% in 2020 to 92% in 2021.

1.2 Card payment fraud

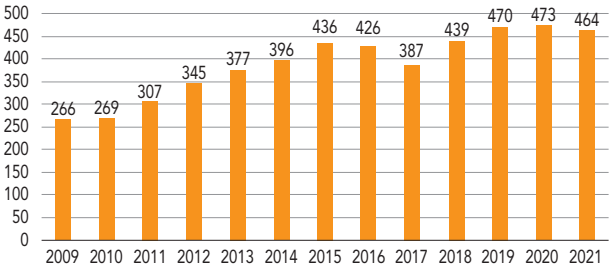
1.2.1 Overview of cards issued in France

C9 Cards issued in France in 2021

a) Total transaction value (EUR billions)



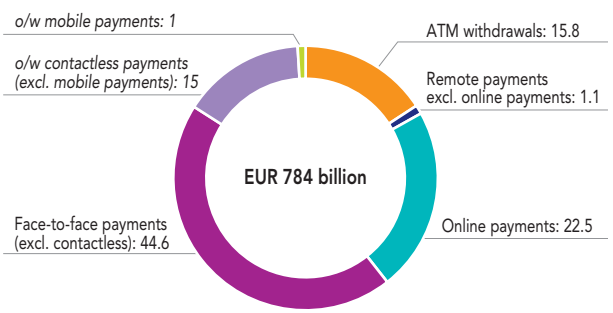
b) Total fraud value (EUR millions)



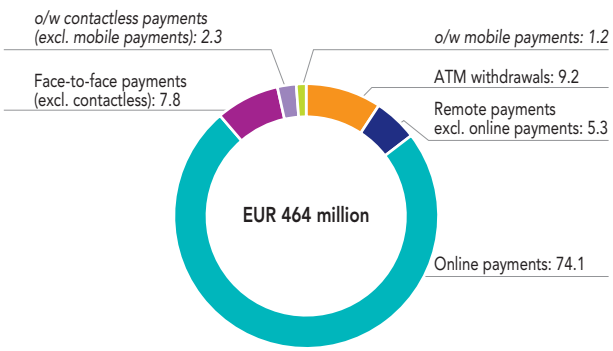
Source: Observatory for the Security of Payment Means.

C10 Use of cards issued in France in 2021 (%)

a) Breakdown of transaction value



b) Breakdown of fraud value

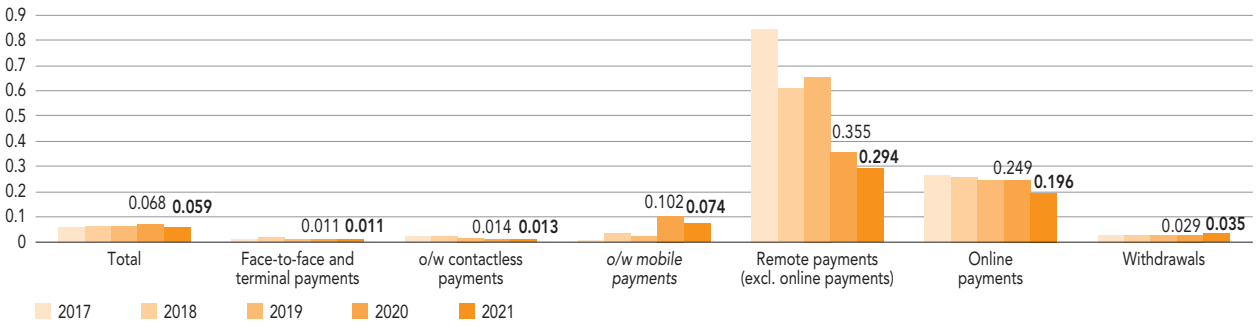


Source: Observatory for the Security of Payment Means.
Note: ATM – Automated Teller Machine.

After a marked slowdown in 2020 due to the health crisis, the easing of restrictions together with the strong growth in the use of contactless payments boosted card transactions. The number of flows thus posted a sharp rise of 15.4% in 2021.

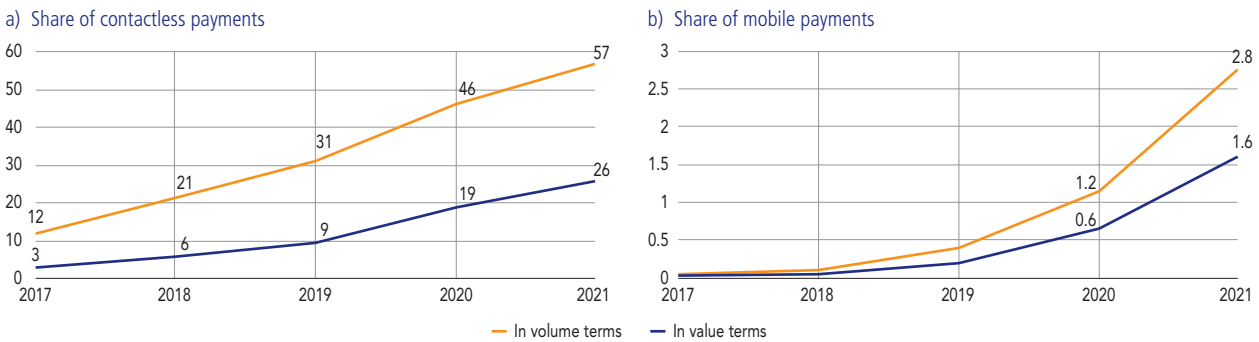
At the same time, the strengthening of security, in particular through the gradual generalisation of strong authentication rules for remote transactions, led to a 1.9% decrease in the total value of fraud on French cards.

C11 Change in fraud rate on French cards by initiation channel (in value, in %)



Source: Observatory for the Security of Payment Means.

C12 Face-to-face card payments (%)



Source: Observatory for the Security of Payment Means.

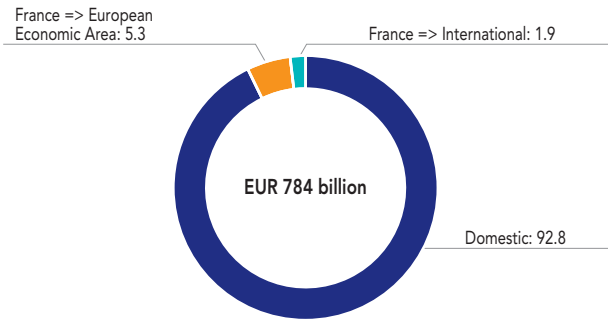
The fraud rate on card transactions issued in France dropped significantly from 0.068% in 2020 to 0.059% in 2021, i.e. a substantial decrease of 13%. The main highlights are as follows.

- The significant decline in the fraud rate on remote payments: from 0.249% in 2020 to 0.196% in 2021 for online payments (down 22%), but also from 0.355% to 0.294% for remote payments excluding online payments (down 17%), i.e. their lowest level ever.
- Fraud on contactless payments reached an all-time low of 0.013%, against a backdrop of strong growth in their use. Among contactless payments, the fraud rate on mobile phone payments remained significantly higher but decreased from 0.102% in 2020 to 0.074% in 2021, also in a context of rapid development. The Covid-19 pandemic boosted the use of face-to-face contactless payments, which accounted for 57% of transactions and 26% in terms of value. As part of this trend, the share of contactless mobile payments was still small but increased threefold in 2021, rising from 1.2% of face-to-face payments in 2020 to 2.8% in terms of the volume of transactions, and from 0.6% to 1.6% in terms of value.

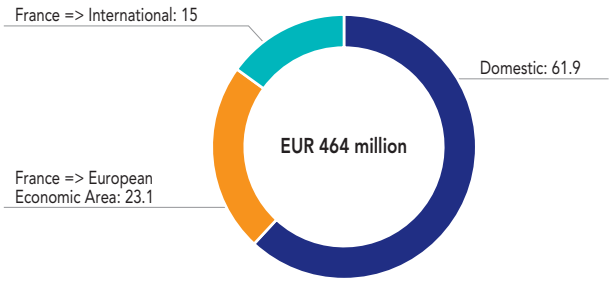
1.2.2 Geographical breakdown of fraud on cards issued in France

C13 Cards issued in France by geographical area (%)

a) Breakdown of transaction value

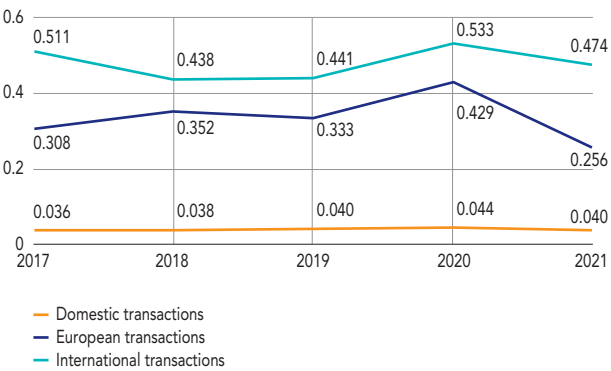


b) Breakdown of fraud value



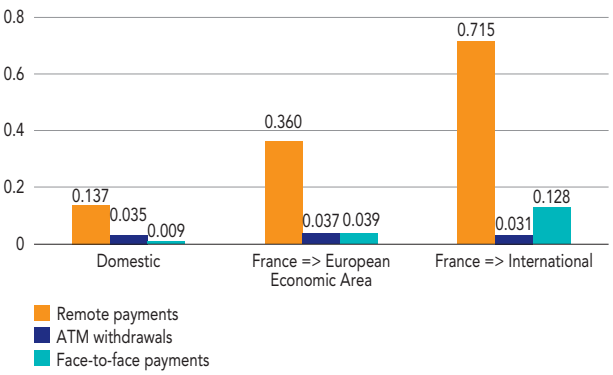
Source: Observatory for the Security of Payment Means.

C14 Change in fraud rate on cards issued in France by geographical area (%)



Source: Observatory for the Security of Payment Means.

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



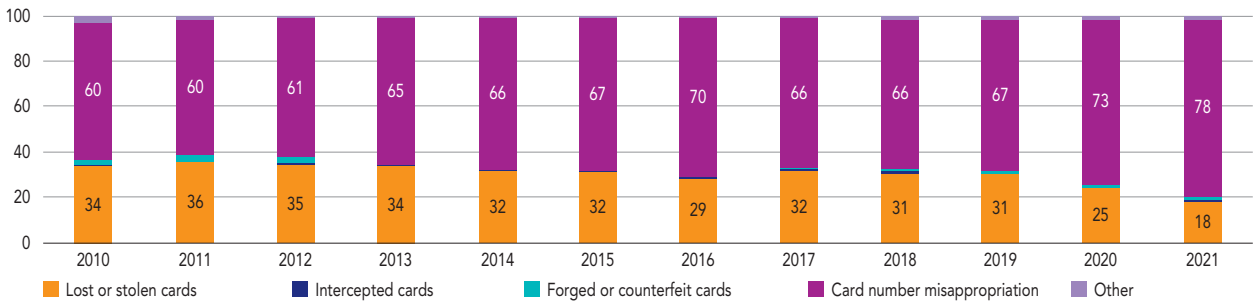
Source: Observatory for the Security of Payment Means.
Note: ATM – Automated Teller Machine.

In 2021, international transactions represented only 7% of transactions using cards issued in France, but they accounted for 38% of fraud, i.e. EUR 177 million. If only transactions outside the European Economic Area are taken into account, the imbalance is even more marked. Indeed, these transactions represented only 2% of flows, but accounted for 15% of fraud, i.e. EUR 70 million. However, although transactions with EU countries and international transactions are structurally more prone to fraud, their respective fraud rates decreased significantly in 2021.

Finally, irrespective of the geographical area, fraud rates were higher on remote payments, mainly online payments. Fraud is carried out by reusing stolen or lost cards or usurped card numbers on less secure sites abroad. In addition, the fraud rate on international face-to-face payments is higher than that on European transactions, due to the use of less robust technologies, which are therefore more vulnerable to counterfeiting, such as reading a card's magnetic stripe or taking a manual imprint of the card.

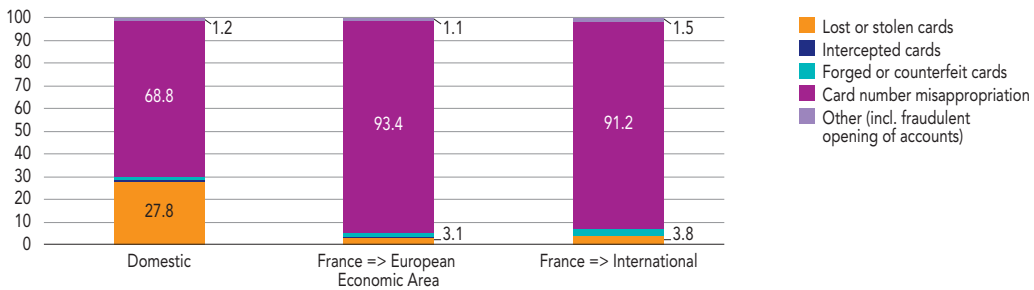
1.2.3 Breakdown by type of fraud on cards issued in France

C16 Change in card payment fraud value by type since 2010 (%)



Source: Observatory for the Security of Payment Means.

C17 Card payment fraud value by type and by geographical area in 2021 (%)



Source: Observatory for the Security of Payment Means.

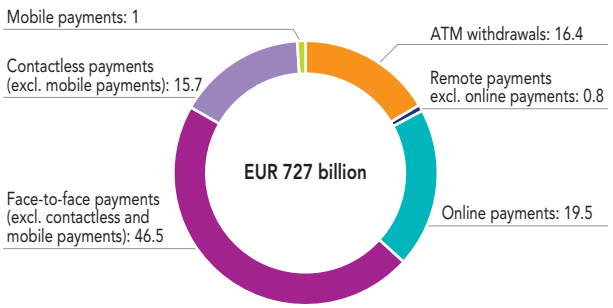
The share of fraud linked to misappropriated card numbers has steadily increased since 2010, in parallel with the development of e-commerce. This phenomenon is related to the development of increasingly sophisticated attack techniques, ranging from phishing to fraud by manipulation of cardholders. On the other hand, the share of fraud linked to the loss or theft of cards has decreased and represented less than one-fifth of fraud in 2021. Other types of fraud, such as undelivered or counterfeit cards, remain marginal.

Fraud linked to misappropriated card numbers, which can be carried out remotely, accounts for a structurally larger share of fraud on European (93%) and international (91%) transactions than on domestic transactions (69%). On the other hand, fraud linked to the theft or loss of a card is higher for domestic transactions (28%).

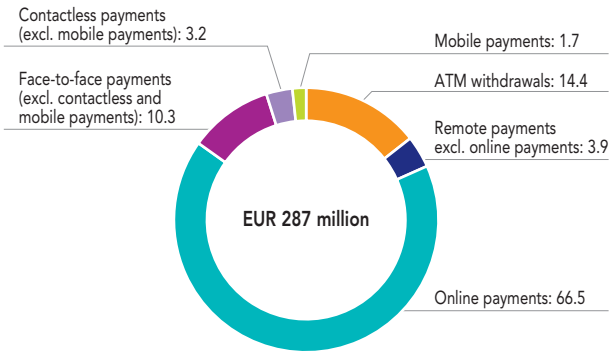
1.2.4 Breakdown of fraud on domestic transactions

C18 Value of domestic card transactions (%)

a) Breakdown of transactions

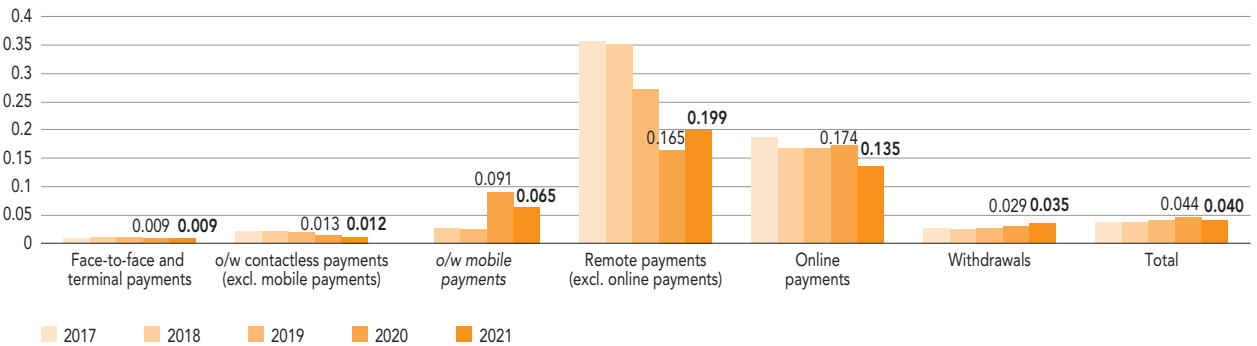


b) Breakdown of fraud



Source: Observatory for the Security of Payment Means.
Note: ATM – Automated Teller Machine.

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



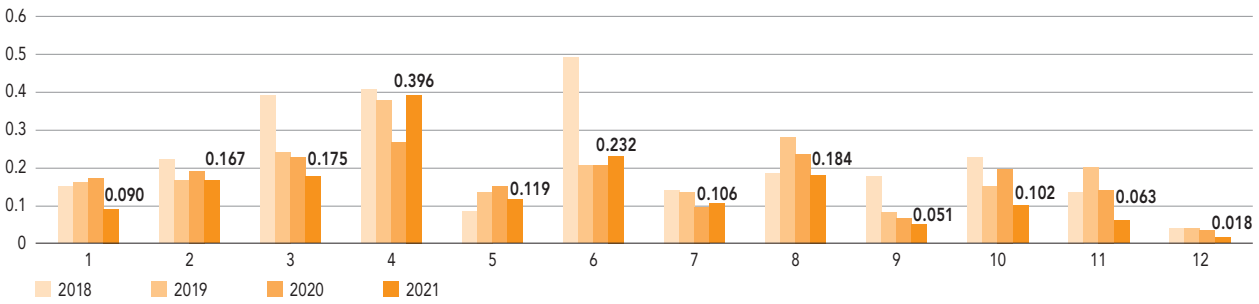
Source: Observatory for the Security of Payment Means.

While remote payments accounted for only 20% of domestic transactions, and essentially online payments (96%), they alone accounted for 70% of fraud (67% for online payments). However, thanks to the gradual roll-out of strong authentication throughout the year, the fraud rate on online payments dropped significantly, from 0.174% in 2020 to a historical low of 0.135% in 2021 (down 22%). At the same time, the fraud rate on contactless payments reached 0.012%, against a backdrop of strong growth in flows (up 55%).

Overall, the fraud rate on domestic card transactions fell from 0.044% in 2020 to 0.040% in 2021, after three consecutive years of slight increases.

1.2.5 Focus on domestic online card payments

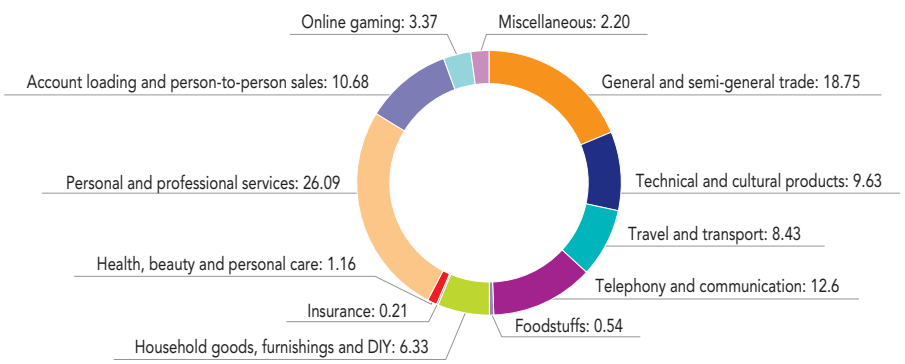
C20 Change in the fraud rate for domestic online card payments, by sector (%)



1 General and semi-general trade
2 Personal and professional services
3 Telephony and communication
4 Technical and cultural products
5 Travel and transport
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

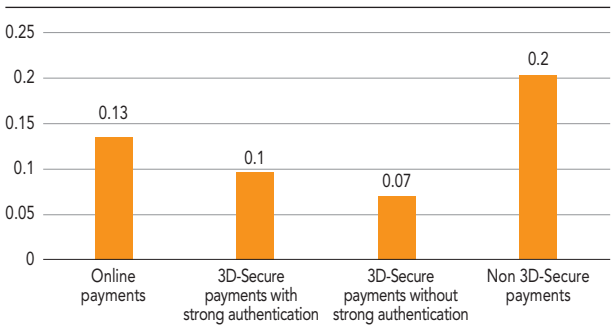
Source: Observatory for the Security of Payment Means.

C21 Breakdown of fraud on domestic online card payments, by sector in 2021 (%)



Source: Observatory for the Security of Payment Means.

C22 Fraud rate on domestic online payments, by channel (%)

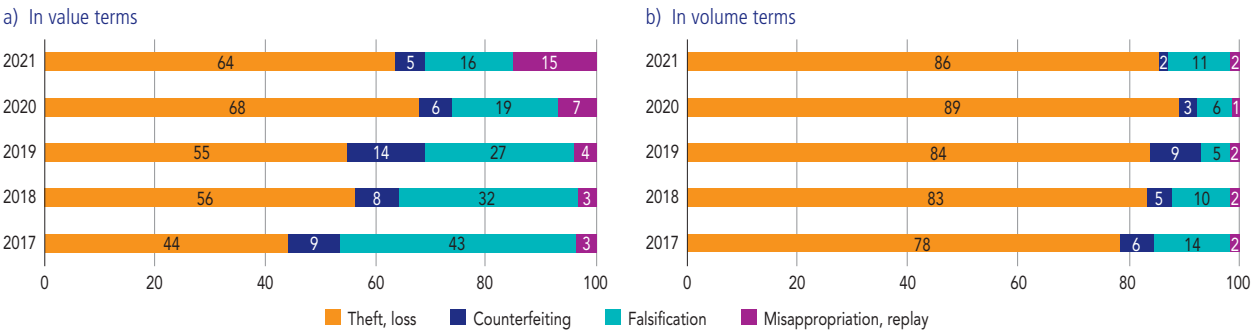


Source: Observatory for the Security of Payment Means.

Thanks to the roll-out of strong authentication, the security of online payments has been significantly reinforced. At the national level, unsecured transactions are twice as likely to be defrauded as those within the 3D-Secure protocol (0.20%, compared with 0.10%). In addition, the exemptions, by their nature, target lower risk transactions (0.07%).

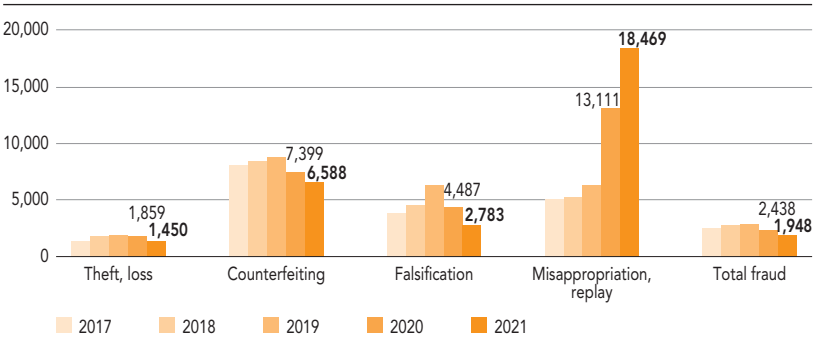
1.3 Cheque fraud

C23 Breakdown of cheque fraud by type (%)



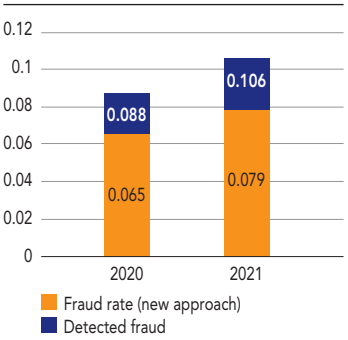
Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

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



Source: Observatory for the Security of Payment Means.

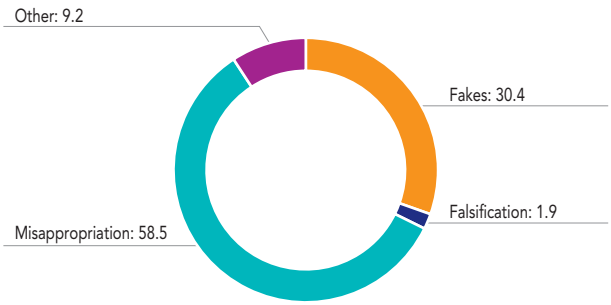
In 2021, the total value of fraudulent cheque transactions increased to EUR 625 million (up 16.3% compared with 2020). Nevertheless, thanks to the fraud prevention mechanisms set up by banks in accordance with the Observatory's roadmap *(see Chapter 2)*, EUR 161 million worth of fraudulent cheque deposits were prevented. Thus, gross fraud, under the new approach, amounted to EUR 465 million. According to this new approach, the fraud rate posted an increase, rising from 0.065% in 2020 to 0.079% in 2021, whereas it would have reached 0.106% without these prevention mechanisms, against 0.088% in 2020.

In this context, the types of cheque fraud are changing. The share of lost and stolen cheques in fraud value has increased substantially, climbing from 44% in 2017 to 64% in 2021, while its share in fraud volume has recorded a smaller rise (78% in 2017, compared with 86% in 2021). Similarly, the share of misappropriation or replay has increased significantly from 3% in 2017 to 15% of the amounts defrauded in 2021. On the other hand, the share of cheque counterfeiting in fraud value has dropped from 43% in 2017 to 16% in 2021.

The average amount of a fraudulent cheque has declined overall since 2019 to EUR 1,948 in 2021. However, the average amount of fraud by misappropriation or replay has continued to rise, reaching EUR 18,469 in 2021.

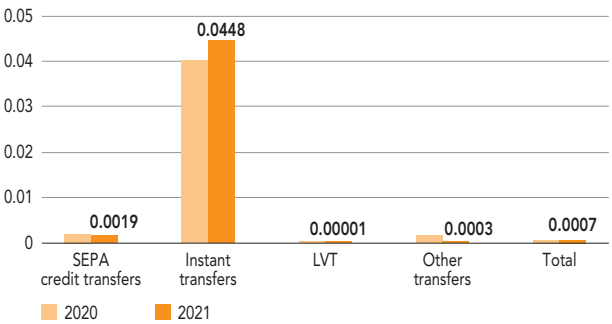
1.4 Credit transfer fraud

C26 Breakdown of credit transfer fraud value by fraud type in 2021 (%)



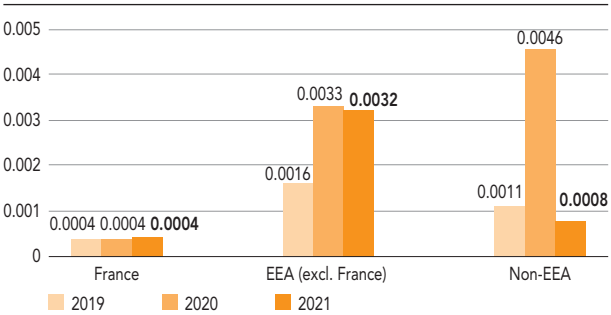
Source: Observatory for the Security of Payment Means.

C27 Credit transfer fraud rate by transfer type (%)



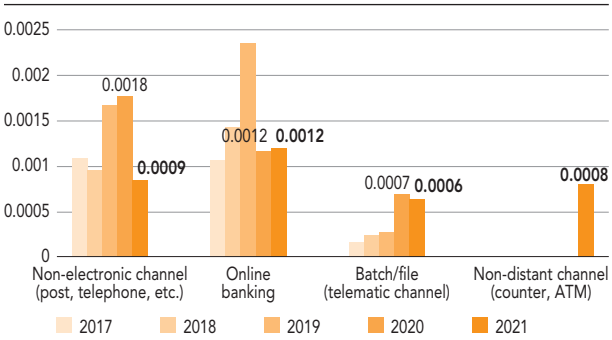
Source: Observatory for the Security of Payment Means.
Note: SEPA – *Single Euro Payment Area*, LVT – large-value transfer.

C28 Change in credit transfer fraud rate by geographical area (%)



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

C29 Change in credit transfer fraud by initiation channel (%)



Source: Observatory for the Security of Payment Means.
Note: ATM – Automated Teller Machine.

Overall, fraud involving credit transfers rose slightly to EUR 287 million in 2021, compared with EUR 267 million in 2020. However, the fraud rate for credit transfers fell slightly by 0.0007% as a result of increasing flows. Excluding large-value transfers, this fraud rate also improved and stood at 0.0015% in 2021, compared with 0.0019% in 2020. The average amount of fraudulent credit transfers stood at EUR 6,149 in 2021, down by more than 50% in three years. With volumes having more than doubled in one year, the fraud rate for instant transfers inched up to 0.0448%.

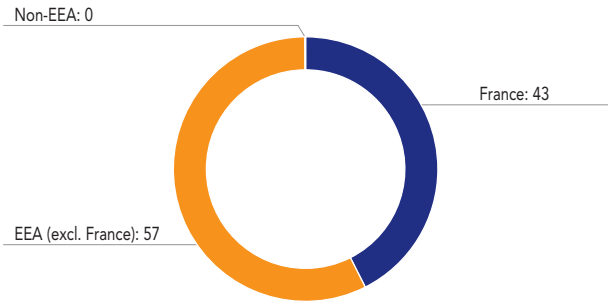
The fraud rate declined or was constant on all initiation channels. In particular, it dropped by half for non-electronic transfers, which were previously the most vulnerable to fraud. It remained stable for online banking transfers, mainly used by private individuals (0.0012%) and slightly down for telematics transfers, mainly used by businesses and administrations (0.0006%).

The fraud rate for cross-border credit transfers was down for transactions outside the European Economic Area (EEA) and stabilised for those within the EEA. Cross-border transfers accounted for 52% of the value of credit transfer fraud.

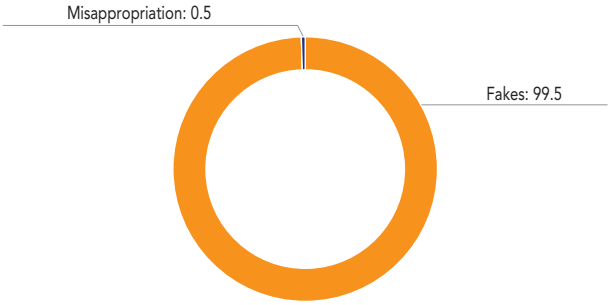
1.5 Direct debit fraud

C30 Breakdown of direct debit fraud value (%)

a) By geographical area



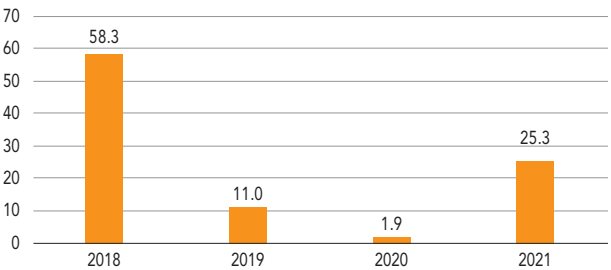
b) By type of fraud



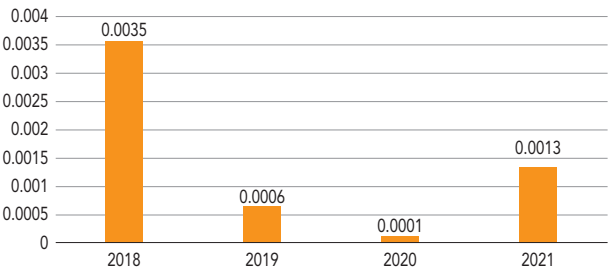
Source: Observatory for the Security of Payment Means.
Note: EEA – European Economic Area.

C31 Direct debit fraud

a) In value terms (EUR millions)



b) Rate (%)



Source: Observatory for the Security of Payment Means.

Direct debit fraud is extremely volatile, amounting to EUR 25 million in 2021, compared with EUR 11 million in 2019 and EUR 2 million in 2020. The fraud rate thus increased significantly, climbing from 0.0001% in 2020 to 0.0013% in 2021.

However, this increase should be put into perspective, as direct debit is the means of payment with the lowest annual fraud rate among the payment instruments available to individuals.

In 2021, the average amount of direct debit fraud was EUR 101, an amount almost three times lower than in 2020 (EUR 292).

The types of direct debit fraud are changing: direct debit fraud now mostly affects accounts held in the European Economic Area (57%, compared with 25% in 2020); it is based almost exclusively on the issuance of fake direct debit instructions by a fraudulent creditor, i.e. without a direct debit mandate or an underlying economic relationship with the victim.

BOXES

❶ Payment fraud indicators, conclusions and recommendations by law enforcement agencies in France in 2021

The Ministry of the Interior is represented in the Observatory by the *Service central de renseignement criminel* (SCRC – the central criminal investigation service) of the French *Gendarmerie* and the *Direction centrale de la police judiciaire* (DCPJ – the central judicial police service) of the French *Police*. As they do every year, these two departments have provided the Observatory with their main observations on payment fraud in 2021.

1. Bank card fraud

The police and *gendarmerie* record offences relating to the fraudulent use of bank cards, whether the data are captured in France or abroad. Falsification and counterfeiting of payment or withdrawal cards are also included in the aggregates taken into account. For this purpose, three sources are mainly monitored by law enforcement agencies:

- data from the *Service statistique ministériel de la sécurité intérieure* (SSMSI), which gathers all the figures reported by the police and *gendarmerie*;
- the number of opened legal proceedings recorded in the TAJ database (*Traitement des antécédents judiciaires*), a shared database for the police and *gendarmerie*;
- figures obtained from searches by type of offence (NATINF – *nature d'infraction*), which is an indicator of the criminal classification of offences by the Ministry of Justice.

According to the three indicators, bank card fraud offences increased by between 20% and 25% from 2020 to 2021. This rise could be explained by the gradual easing of measures relating to the Covid-19 health crisis, which may have had an impact on the scale of card theft.

According to Perceval, which is a national platform for reporting bank card fraud targeting individual victims on the internet, 324,594 cases were reported in 2021 (compared with 318,804 in 2020, up 1.8%) for a total loss of EUR 140 million (compared with EUR 137 million in 2020, up 2.6%). This represents an average loss per case of EUR 432 (compared with EUR 428 in 2020). It should be noted that a report on the Perceval platform may cover several transactions initiated fraudulently using the same usurped card data.

As regards bank card fraud by contactless payment, the TAJ details 2,779 legal proceedings initiated nationwide in 2021, reflecting a slightly upward trend compared with previous years (2,530 in 2020 and 2,484 proceedings in 2019 respectively), but which must be put into perspective given the increase in the volume of these transactions. In these proceedings, law enforcement agencies mainly note the use of cards' contactless functionality after a theft. **The use of advanced fraud technologies based on the remote capture of data by the Near-Field Communication (NFC) system has not been observed.**

Number of bank card fraud incidents recorded by law enforcement agencies in France

	2018	2019	2020	2021 (change 2020-2021)
Source SSMSI	57,708	67,037	60,824	73,757 (+21%)
Source TAJ	53,703	58,537	53,221	66,497 (+25%)
Source NATINF	53,276	64,168	58,414	70,425 (+21%)

Source: Service statistique ministériel de la Sécurité intérieure *(SSMSI).*

2. Hacking of payment and card withdrawal terminals

Considered one of the European priorities in terms of cybercrime, the capture of bank data remains a criminal act that is well established in France. The modus operandi now extends to all types of payment and cash withdrawal machines (ATMs – Automated Teller Machines, card-operated fuel pumps, motorway payment terminals, car park payment terminals, etc.), on which skimmers[1] and shimmers[2] continue to be installed, as well as to portable payment terminals, i.e. any type of wireless terminal that is not attached to the shop's cash register, which are also compromised or diverted from their purpose.

Skimmer fraud consists in retrieving, through tampered or usurped payment terminals, the banking data stored on the card's magnetic strip. Shimmer fraud is based on similar procedures, but consists in retrieving the data contained in the card's chip. In both cases, the card data obtained by the criminal networks is then re-encoded onto magnetic stripe cards. These counterfeit cards are then used for face-to-face payments or withdrawals, where reading the chip is optional, such as for payments at motorway payment terminals or in countries where smart cards are not yet widely used (in the Americas and South-East Asia). These stolen data can also be used for remote payments, mainly on non-European e-commerce sites that have not implemented strong cardholder authentication.

In 2021, the number of ATMs and terminals compromised by skimmers or shimmers remained stable, with 28 cases. The law enforcement authorities recorded 30 cases in 2020, 26 in 2019, 19 in 2018, 35 in 2017 and 82 in 2016. Of the 28 cases recorded in 2021, 13 concerned automatic fuel pumps (AFPs) and 15 concerned automated teller machines (ATMs). Both petrol station managers and ATM managers must therefore remain vigilant to prevent attempts to replace a legitimate payment terminal with a tampered terminal or any installation by a third party of a fraudulent external device (reader, camera, keyboard, etc.).

In particular, law enforcement agencies have noted a significant but as yet unquantified number of complaints from trucking companies following the fraudulent use of their fuel cards. The fuel cards pirated in France are then used on motorway tolls in France and Eastern Europe, particularly in Poland, the Czech Republic and Slovenia. The *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* (OCLCTIC), attached to the DCPJ, cooperates through Europol with the Fuel Industry Card Fraud Bureau (FICFIB).[3]

3. Jackpotting attacks on automated teller machines (ATMs)

Law enforcement agencies continue to investigate ATM jackpotting attacks. Jackpotting consists in physically or logically attacking an ATM in order to hack into the embedded computer, take control of it and thus activate the cash dispensing mechanisms. These very sophisticated techniques can only be implemented by organised crime networks or specialised criminals.

In 2021, damage caused by jackpotting fell significantly compared with 2020: 32 incidents were recorded in 2021 for a total amount of EUR 335,370, compared with 95 in 2020 for a total amount of EUR 681,170. Of these 32 incidents, 22 involved a new modus operandi targeting a specific model of ATM. This significant decrease can be explained by the identification and arrest by OCLCTIC officers of twelve offenders specialised in jackpotting and the dismantling of five criminal networks responsible for over half of the attacks recorded in 2020.

In view of the findings on jackpotting occurrences, the OCLCTIC notes that obsolete hardware and software still too often contribute to successful attacks. It therefore recommends that ATM operators take minimum security measures, such as systematically updating operating systems, encrypting the hard

1 A device that slides into the slot of an ATM while leaving space for a bank card to be slid in naturally. The magnetic stripe data is then copied by the device without affecting the correct functioning of the bank card.

2 A device that is inserted into an ATM in a similar manner to a skimmer, but which intercepts the data on the bank card's chip, including its confidential code.

3 FICFIB was set up in 2003 to establish and maintain a network for exchanging information on the reduction and prevention of fuel card fraud and to develop common strategies to prevent and reduce fuel card fraud on a European scale. It is a similar organisation to the European Association for Secure Transactions (EAST), which is involved in combating ATM fraud. Membership of FICFIB is open to companies that issue fuel cards or operate a distribution network and have a clear interest in preventing and combating fuel card fraud.

disk to prevent attacks from passing through the operating system, installing anti-intrusion sensors capable of putting the ATM out of service in the event of an attack, and reinforcing the security of the communication between the ATM and the devices dedicated to maintenance.

Thus, in addition to the physical and logical ATM protection measures implemented by payment professionals, the repressive actions conducted by law enforcement agencies (infiltration, use of video surveillance images, bugging, etc.) make it possible to dismantle these networks and contain this type of fraud.[4]

4. False transfer orders affecting the private and public sectors

According to law enforcement agencies, false transfer orders are financial scams that consists in obtaining from the victim a credit transfer to a bank account managed by the fraudster. In the statistical methodology of the Observatory, false transfer orders are classified as bank transfer fraud. Generally operating by telephone or e-mail and using social engineering techniques, fraudsters exploit the technical, human and organisational vulnerabilities of companies (SMEs, VSEs, tradespeople) or public administrations in order to make unauthorised transfers of funds for fraudulent purposes.

The Covid-19 health crisis and the generalisation of teleworking led to an exponential increase in false transfer orders in 2020, with the rapid roll-out of new operating and organisational methods, which enabled malevolent parties to exploit new or pre-existing vulnerabilities. **In 2021, law enforcement agencies identified 517 cases of false transfer orders for a total value of EUR 101.2 million, including one exceptional case amounting to a loss of EUR 33 million.**

Law enforcement agencies have identified several methods used by the fraudsters:

- change of bank details (68.5% of cases);
- CEO fraud (19.5% of cases);
- remote control (8.5% of cases);[5]
- unknown modus operandi (3.5% of cases).

In addition, a new phenomenon was observed in 2021. Until then, in over half of the cases of false transfer orders, the accounts credited were held in French banks in the Paris financial centre. In 2021, three quarters of initial destination accounts were linked to a French IBAN by payment service providers offering online banking or mobile banking type services.

The French Banking Federation, the *Club des directeurs de sécurité et de sûreté des entreprises* (CDSE – a group of directors working for business security) and the DCPJ have joined forces to combat fraudulent transfer orders carried out by changing bank details and to offer an e-learning module to companies and administrations.[6]

4 Jackpotting attacks that target banking equipment and not withdrawal operations are not categorised as card payment fraud by the Observatory.

5 Remote control is generally achieved by hacking and using an email, enabling fraudsters to give instructions and make bank transfers using the stolen identity of a natural or legal person. By installing spyware, fraudsters are able to retrieve access codes from online banking interfaces, but also to assist and accompany the victim on the banking application by encouraging him/her to make bank transfers to an account that he/she has set up.

6 The e-learning module is available on the following website: *https://www.lesclesdelabanque.com/entreprise/prevenir-escroquerie-aux-coordonnees-bancaires/*

2

THE OBSERVATORY'S ACTIONS IN 2021

2.1 Positive results from the implementation of strong authentication for internet payments

The use of strong customer authentication when initiating an electronic payment was introduced by the second European Payment Services Directive (PSD 2) and is a key payment security feature. Its implementation on the French market was backed by a migration plan adopted by the Observatory in autumn 2019 and rolled out over a period of around two years.

2.1.1 The migration plan for the French financial sector

The plan for the migration towards strong payment authentication had two aspects:

- an aspect aimed at consumers that involved enrolling cardholders in authentication systems that meet the PSD 2 definition of strong authentication, replacing the use of the OTP (One Time Password) SMS code as a sole authentication factor;
- an aspect aimed at professionals in the payments chain, including e-merchants, that focuses on developing authentication infrastructures to ensure the application of the directive's strong authentication liability and exemption rules.

For both, monitoring indicators with targets and deadlines, and also action plans, have been developed to assist the French financial sector in becoming compliant. At its plenary session on 17 December 2021, the Observatory noted that given the French financial sector's high degree of compliance, the migration plan could be considered completed.

2.1.2 The deployment of strong authentication solutions among cardholders

Strong authentication is based on the use of two or more elements from at least two of three different categories of authentication factors:

- "knowledge": something only the user knows, such as a confidential code, a password, or a personal detail;
- "possession": something only the user possesses and that can be recognised without risk of error by the payment service provider (PSP), such as a card, a smartphone, or connected objects like a watch, bracelet or key chain, etc.;
- "inherence": something the user is, i.e. a biometric characteristic.

PSD 2 stipulates that these elements must be independent: should one be compromised, that must not undermine the reliability of the others so as to preserve the confidentiality of authentication data. Furthermore, for remote payments, PSD 2 provides for an additional requirement: the authentication data must be linked to the payment transaction, and cannot be reused for a subsequent payment transaction:

- the authentication code generated for the transaction is specific to the value of the transaction and the identified beneficiary;
- any change in amount or beneficiary invalidates the authentication code.

Where a biometric factor is used, the validation key for the payment operation generated after the print is read must also be single-use.

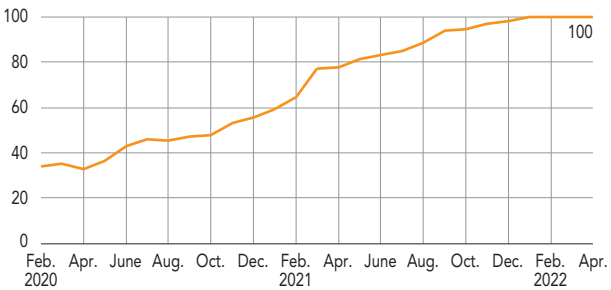
As at June 2022, the Observatory estimated that 100% of cardholders who are active on the internet (i.e. who have

made at least one online payment in the last three months) are equipped with, and now use, this authentication mode in place of the OTP SMS. That represents more than 90% of all cardholders.

French cardholders use the following strong authentication solutions.

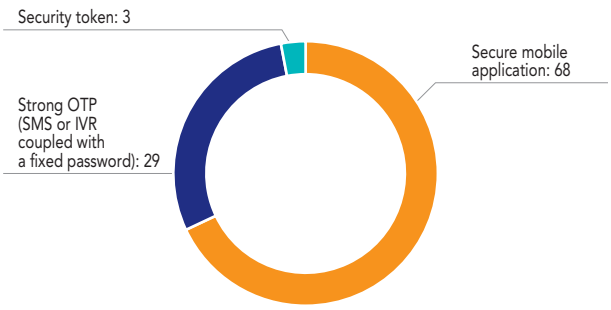
- Two-thirds use a secure mobile application with validation when making an internet card payment via an online banking application on a smartphone (securely pre-registered and thus recognised as a possession factor), either with a personal code (a knowledge factor) or a biometric characteristic (an inherence factor).
- 28% use a "strong OTP" approach with authentication by means of a one time password received by SMS or interactive voice response (the telephone line is recognised as a possession factor) and a fixed password (an online bank access code or dedicated password is recognised as a knowledge factor).

C1 Monitoring trends in cardholder enrolment: proportion of cardholders active on the internet that are equipped with an SCA solution (%)



Source: Observatory for the Security of Payment Means.
Note: Active cardholder: a cardholder that has carried out at least one online transaction during the last three months.

C2 Breakdown of cardholder equipment with an SCA solution (%)



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

- The remaining 3% use a solution such as an electronic unit provided by the bank (recognised as a possession factor), and an additional means of authentication (generally a knowledge factor).

2.1.3 The compliance of e-merchant practices

PSD 2 established precise rules for the authentication of transactions for merchants and their service providers:

- merchants must use strong authentication with every payment accepted over the internet, unless an exemption applies;
- the merchant may request activation of one of the five exemption mechanisms provided for in PSD 2 to facilitate the payment process and take account of different levels of risk, but such activation remains subject to the agreement of the card-issuing bank.

The **five grounds for exemption from strong authentication** provided by the regulatory technical standards (RTS)[1] for transactions where the user is actively present are:

- **low value payments** (Article 16) of less than EUR 30, limited to five consecutive individual transactions or a cumulative amount that does not exceed EUR 100;
- **low risk payments** (Article 18) on the grounds that the transaction corresponds to the cardholder's payment habits (purchase from its usual terminal, known delivery address, nature of purchase, amount, etc.) and does not exceed EUR 500;
- **recurring payments** (Article 14) of a fixed amount and frequency, starting from the second transaction;
- **payments to a trusted beneficiary** (Article 13), designated as such by the cardholder through a process that required strong cardholder authentication;
- **payments initiated electronically via secure payment processes or protocols reserved for use between professionals** (Article 17), requiring a prior assessment of the processes and protocols by the competent national authority (in France, the Banque de France) to ensure that the level of security offered is at least equivalent to that of strong authentication.

The use strong authentication by merchants has been very gradual, owing to the need to improve the reliability of the new authentication infrastructures based on the 3D-Secure v2 protocol. However, it accelerated due to the ramp-up plan for the soft decline mechanism.[2] As a result, at the end of April 2022, all payment flows subject to PSD 2 complied with its provisions. Either they were transited through the

3D-Secure protocols (allowing for strong authentication or the activation of an exemption) or they were granted an exemption outside of 3D-Secure (particularly for low value payments). During the first quarter of 2022, the process of compliance was completed with the travel and events sector flows. These sectors were particularly affected by the health crisis and had been temporarily exempted by the Observatory.

The Observatory has also strived to strengthen the payment issuance framework for merchant-initiated transactions (MITs). These are initiated by the merchant without the active involvement of the user, and correspond in particular to payments in several instalments or deferred payments (e.g. payment at the time of dispatch or receipt of an order), subscriptions (print media, video-on-demand, etc.) and pay-per-use payments (e.g. urban transport).

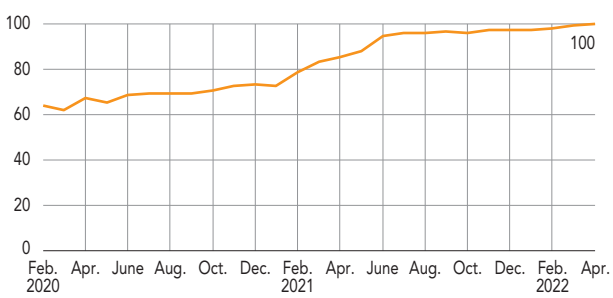
- MITs from new subscriptions must include the technical trace (transaction "chaining") of a strong authentication carried out when the subscriber's card number is taken, formalised by a mandate specifying the commitment to pay and payment conditions (amount, ceilings, frequency, etc.).
- MITs from subscriptions made before chaining was implemented qualify for a grandfathering clause and must feature a standard chaining reference predefined by the cad payment system.

At the end of the first quarter of 2022, all merchants and their acceptance service providers were able to issue MITs that complied with the chaining requirement. According to card-issuing banks, 93% of the total volume of transactions in April were chained MITs.

French cardholder online payment flows in the post-PSD 2 environment break down as follows:

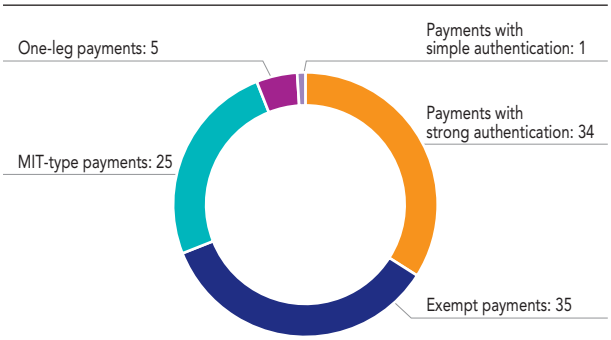
- one-third of transactions are subject to strong authentication;

C3 Monitoring trends in merchants' flow compliance: proportion of value-compliant CIT flows (%)



Source: Observatory for the Security of Payment Means.
Note: CIT – customer-initiated transaction.

C4 Breakdown of flows by security method (%)



Source: Observatory for the Security of Payment Means.
Note: One-leg payments: transactions for which strong authentication is not mandatory as they are carried out with a merchant or cardholder located outside the European Economic Area; MIT – merchant-initiated transaction.

- 35% of transactions are exempted;
- one-quarter are MIT-type transactions;
- the remaining 5% of transactions without strong authentication are "one-leg" transactions, i.e. with a merchant that is not located in the European Economic Area and not subject to the requirement for strong authentication.

2.1.4 Outlook for the period ahead

Looking beyond the fact that the French market has been properly brought into compliance, the Observatory will continue to monitor the proper application of the rules provided for in PSD 2 while ensuring that e-commerce operates as smoothly as possible. It will also continue to play its role as coordinator for the market as a whole across a range of subjects:

- continuing to educate consumers to ensure that they fully understand the new authentication solutions, and that they adopt good security habits when using the internet;
- combating new methods of fraud aimed at circumventing strong authentication, particularly by manipulating the payer, and, in partnership with telephone operators, seeking the means to prevent the technological flaws that are exploited (usurping telephone numbers by spoofing, pirating mobile lines by SIM-swapping, etc.);

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

2 These messages are card issuers' rejections of authorisation of transactions that do not comply with PSD 2. Merchants or their technical acceptance provider then have the option to resubmit the transaction via the 3D-Secure protocol (the retry feature).

- monitoring the performance level of authentication solutions and infrastructures, as well as the associated continuity mechanisms, in order to ensure that e-commerce maintains a high level of fluidity and resilience;
- developing 3D-Secure protocol functionalities to facilitate the integration of all the exemptions provided for by the regulations, in particular Article 13 of the RTS on trusted beneficiaries, under the same conditions of security applied to the other exemptions;
- combating the inappropriate use of authentication means and infrastructures, for example by certain flash sales professionals (use of strong authentication to access online sales spaces), or even by certain individuals (social network influencers who share their card details with followers).

Consolidation work will continue on these various topics in the second half of 2021, under the leadership of the multi-stakeholder working group that successfully oversaw the migration process.

2.2 Monitoring the Observatory's actions and recommendations on cheque fraud

Given the context of rapidly declining cheque payment use and the risks of fraud that continue to be high, the Observatory has carried out a specific study on the security of cheque payments. The study's findings were published in July 2021 in the Observatory's 2020 Annual Report.[3] The Observatory issued ten recommendations for all industry players, particularly banks, cheque processing companies, public authorities, and cheque users.

One year after the publication of its recommendations, the progress report drawn up by the Observatory is encouraging. Several concrete actions have been put in place by both public authorities and industry professionals. However, given that fraud levels remain high, the Observatory exhorts the players in the industry to continue and step up their efforts to improve the security of this declining payment method. Taking into account the controls already carried out and the risk policy of each institution, the Banque de France will ensure that its recommendations are duly implemented by the banking institutions as part of its supervisory activities.

2.2.1 Revision of the Banque de France's cheque security framework

Within the framework of its mission to oversee the security of payment means,[4] the Banque de France ensures that the standards applicable to cheques remain relevant. While most payment instruments are European in nature and are thus subject to European regulations (in particular PSD 2), and governance by authorities supervised by the Eurosystem,[5] the cheque is essentially a national payment instrument. Its use internationally is covered by the Geneva Convention of 1935.

In addition to the legislative and regulatory provisions set out in the *Code monétaire et financier* (the French Monetary and Financial Code),[6] the functioning of the French cheque payment system is determined by the 2001 regulation on

T1 Summary of the implementation of the Observatory's ten recommendations on cheque fraud

Recommendations	Level of implementation
Recommendation No. 1: Revise the Banque de France's statistical data collection to improve understanding of cheque fraud incidents	Done
Recommendation No. 2: Improve the controls of collecting banks against the remittance of fraudulent cheques	Implemented under the responsibility of each institution and under the supervision of the Banque de France
Recommendation No. 3: Support the development of controls on the part of the issuing institution	Implemented under the responsibility of each institution and under the supervision of the Banque de France
Recommendation No. 4: Protect cheques from theft while in transit to or at the customer's address	Implemented under the responsibility of each institution and under the supervision of the Banque de France
Recommendation No. 5: Simplify the reporting procedures for loss or theft	Implemented under the responsibility of each institution and under the supervision of the Banque de France
Recommendation No. 6: Give greater access to more cheque beneficiaries to consult the *Fichier national des chèques irréguliers* (FNCI – National Register of Irregular Cheques)	Implementation ongoing by the Vérifiance FNCI Banque de France service
Recommendation No. 7: Enhance Banque de France oversight of the physical solutions used on cheques to counter falsification and counterfeiting	Done
Recommendation No. 8: Ensure the effectiveness of the Vérifiance FNCI Banque de France service against cheque counterfeiting	Done
Recommendation No. 9: Structure long-term cooperation between the parties involved in combating fraud and support the efforts of law enforcement agencies	Done
Recommendation No. 10: Promote cheque user watchfulness through a communication plan	Done

cheque clearing and by professional standards published by the *Comité français d'organisation et de normalisation bancaires* (CFONB – the French Banking Organisation and Standardisation Committee), which counts the Banque de France among its members. The Banque de France also imposes its security requirements through the cheque security framework (CSF). The first version of the CSF came into force in July 2005 when the cheque payment system was radically reformed with the dematerialisation of interbank exchanges and clearing (the image clearing system – ICS).[7] It aimed to ensure that banks correctly applied cheque processing procedures following the clearing reform. Since its introduction in 2005, the CSF has covered different aspects of cheque security (reliability of transactions, business continuity and combating fraud). The Banque de France checks that the CSF is properly observed by sending a self-assessment questionnaire to institutions every year.

The CSF was subject to its first major revision in 2016, resulting in a simpler framework based on key principles of security. Later, in April 2022, the Banque de France again revised the CSF in order to take into account the Observatory's new cheque recommendations issued in 2021 and to more explicitly cover the risks of fraud. This revision rendered the Observatory's recommendations in practical operational terms for the banking institutions. Through this new framework, the Banque de France notably called upon banks to:

- enhance monitoring of the remittance of fraudulent cheques, particularly with regard to cheque cashing scams;
- improve efforts to counter lost and stolen cheques, by improving the security of chequebook deliveries (for example, by alerting customers by SMS that the chequebook is on its way and requesting rapid notification if it has not been received within a certain period of time), the quality of procedures once a chequebook has been reported lost or stolen and the circulation of tools that verify cheque validity;
- remain watchful with regard to the physical integrity of cheques, by incorporating security features that should counter the risks of falsification and counterfeiting.

The new CSF will be used as a benchmark for the 2023 assessment of 2022 results. From 2023 onwards, the Banque de France also plans to enhance its oversight of cheque templates by requiring banks to provide specimens of the cheques made available to their customers and to alert it to any serious incident affecting the cheque payment system. These procedures are noted in the appendices to the new CSF and will come into force in January 2023.

2.2.2 Revision of the Banque de France's statistical framework for cheque fraud declaration

In order to enhance its oversight and to improve its understanding of the different types of fraud, the Banque de France has also revised the statistical data collection for its *Report on means of payment fraud* by expanding its indicators to better identify cheque fraud. Until 2021, cheque fraud was only declared by the collecting institutions, i.e. the bank of the beneficiary who cashes the cheque. From 2022 data onwards, the drawee institutions, i.e. the bank of the customer who issued the cheque, will also have to declare cheque fraud. Declarations will be made in a similar manner by both types of institutions, in number and value for each of the four types identified by the Observatory. In addition to cheques rejected for loss or theft or for counterfeiting, banks will also have to report the proportion of cheques rejected automatically due to their inclusion in the *Fichier national des chèques irréguliers* (FNCI – the French National Register of Irregular Cheques). This should enable the Observatory to assess in the medium term the FNCI's capacity to play a preventive role in combating cheque fraud.

Collecting institutions have also developed mechanisms to delay or block cheque remittances, in some cases preventing the fraud from taking place. Therefore, the Banque de France has incorporated a new statistical indicator to measure the proportion of fraud that is prevented despite

3 See Chapter 4 "Cheque fraud: lessons learned and recommendations".

4 Article L. 141-4, paragraph 4 of the French Monetary and Financial Code (*Code monétaire et financier*): "The Banque de France shall ensure that the means of payment as defined in Article L. 311-3, other than currency, are secure and that the regulations applicable thereto are appropriate. It deems that if a means of payment does not offer sufficient safeguards, it may recommend that the issuer take all appropriate remedial action. If such recommendations are not followed, it may, having obtained the issuer's observations, decide to issue a negative opinion for publication in the Official Journal."

5 The Eurosystem's new oversight framework for electronic payment instruments, schemes and arrangements (PISA) was published in December 2021. It merges the previous frameworks for card payment networks, credit transfers, direct debits and e-money and extends the Eurosystem's oversight to payment solutions used to initiate transactions based on another payment instrument (e.g. mobile payment solutions).

6 Legislation with regard to cheques has remained relatively unchanged for many years, with the exception of certain changes in the regulations on cheques written despite having inadequate funds. The cheque remains the only means of payment for which the issuer can be subject to sanctions.

7 The dematerialisation of interbank cheque clearing was enabled through (i) CRBF Regulation No. 2001-04 of 29 October 2001 on cheque clearing, approved by an order of 17 December 2001, (ii) the professional agreement on the image clearing system (ICS) of 9 July 2003 and (iii) the image clearing system rules of July 2000, supplemented in 2005, which are under the responsibility of the CFONB. The ICS regulations may be subject to additional amendment, as was the case in 2021.

the cheque's submission for exchange within the system. The prevented fraud included within the indicator must fulfil the following two criteria.

1) The cheque was rejected for fraudulent reasons **before** the funds were made available to the collecting party thanks to the transfer of funds to the customer's account being **delayed** or **blocked** (for example, by using a suspense account or technical account). In the latter case, this includes rejections posted to the collecting customer's account at the same time as credits.

2) The bank has **reasonable assurance**, supported by **substantiated indicators**, that the cheque could be linked to fraudulent remittances, i.e. a cheque remitted in order to recover proceeds from cheque fraud, including when the remittance is made through an intermediary account.

The Banque de France has already asked the main banking groups of the French financial sector to communicate this indicator on an ad-hoc basis, without waiting for it to be incorporated into the data collection for the 2022 financial year. Initial findings from their declarations show that delaying or blocking measures are effective, with **EUR 161 million of fraud prevented** from 40,693 deposited cheques: **26% of cheque fraud was thus thwarted**.

2.2.3 The promotion of the National Register of Irregular Cheques (FNCI) and of its consultation via the Vérifiance service

In addition to revising the oversight frameworks, the Observatory insisted upon the need to promote the use of the *Fichier national des chèques irréguliers* (FNCI – the French National Register of Irregular Cheques) maintained by the Banque de France and accessible via the Vérifiance service. Indeed, its contribution to the prevention of fraud has declined over the years as its consultation has diminished more rapidly than payments by cheque.

In addition to cheques associated with accounts that have bank-imposed or court-ordered cheque-writing bans or have been closed, the FNCI records all stopped cheques reported by the bearer for loss, theft or fraud (Articles L. 131-35 and L. 131-84 of the French Monetary and Financial Code) and all counterfeit cheques reported by banking institutions (order of 24 July 1992 related to the automatic processing of information on the validity of cheques implemented by the Banque de France).

In order to maintain an effective service against cheque counterfeiting, in May 2022 the Banque de France disseminated a new procedure via the *Comité français d'organisation et de normalisation bancaires* (CFONB – the French Banking Organisation and Standardisation Committee) for declaring counterfeit cheques in the FNCI. This new procedure is intended to ensure the reactivity of banks that detect counterfeit cheques. In order to achieve the same objective of combating counterfeiting, the *Association du Paiement* (the French Payment Association) has revised the *Chèque – Protocole normalisé* (CHPN – standardised cheque protocol) in order to enable merchants to identify certain counterfeit cheques by communicating additional information on the cash terminals of cheque accepting merchants and users of the Vérifiance service. Finally, in conjunction with the service provider in charge of the Vérifiance service, the Banque de France is continuing its efforts to make consultation of the FNCI available to a broad range of cheque receivers (individuals, self-employed, professionals, etc.).

2.2.4 Constant communication efforts directed towards users

The Observatory regularly reminds users of the need for watchfulness in cheque payment security. As part of the 2020 Annual Report published in July 2021, the Observatory drew up five precautions for the safe use of cheques, intended for both cheque issuers and acceptors. For example, the Observatory recommends that users collect their chequebooks from a bank branch or (for those who cannot or do not wish to go to a branch) be particularly watchful if receiving chequebooks by post. Equally, users are advised to keep their chequebooks in a safe place.

In addition to the awareness campaigns directed at their clientele by banking institutions and associations, the Observatory and the Banque de France, as the national steering body for France's financial education strategy, have communicated on several specific issues.

- In July 2021, the Banque de France, in partnership with the *Institut national de la consommation* (INC – the French national institute for consumption), released a video[8] focusing on cheque cashing scams (at the publication date of this report, it had received 23,000 views).
- In December 2021, in the context of the coming New Year festivities, the Observatory alerted the general public to the risks of cheque fraud and reminded them of the best practices[9] to follow, and invited several press organisations to a dedicated event.

Furthermore, the pages related to cheque use on the official websites of the Banque de France[10] (February 2022) and *Assurance Banque Épargne – Info Service* (March 2022) have been updated and improved to better raise awareness of specific cheque issues, which is not a guaranteed means of payment, and the risks of cheque fraud.

Events organised as part of the Banque de France's EDUCFI financial education forums and programmes have provided opportunities to hear individuals' personal accounts. They confirm that fraudsters and scam artists are active on social media and forums and that they target and solicit people to cash fraudulent cheques, often with the promise of payment. Those people run the risk of owing large sums of money to their banks and of being accomplices to fraud. Thanks to the proliferation of financial education initiatives, bank cheque fraud and scams are now better understood by the general public.

In order to pursue and step up these educational efforts, the Banque de France has suggested that a specific section on bank cheque swindles be included in the next guide on scam prevention, which is the result of an unprecedented degree of public authority cooperation and has been widely circulated within central government, social and local authorities. The Banque de France, in conjunction with other public bodies, will look into the possibility of taking action with regard to social media platforms to ensure their cooperation in combating all types of scams.

Box 3 in this chapter provides practical information to help fraud victims identify the steps they need to take.

2.2.5 Enhanced cooperation between cheque industry players thanks to the continuation of the cheque working group

The initiatives to combat fraud highlighted the need to structure cooperation between the actors involved and to support the activities of law enforcement agencies.

To this end, the cheque fraud working group has been kept on by the Observatory as a permanent group with the objectives of (i) monitoring over time the correct implementation of the recommendations made in the Observatory's 2020 Annual Report and their outcome, (ii) structuring cooperation between industry players, and (iii) organising communication initiatives targeting cheque users. The working group's mandate is presented in Box 2.

In particular, the working group will identify main points of contact to ensure that a structured partnership between cheque processing professionals and law enforcement agencies is in place, with the aim of supporting the latter in their policing efforts.

2.3 A summary of the Observatory's main recommendations on technology watch issues

As part of its annual overview activities, the Observatory makes recommendations to market players and users. The main recommendations issued over recent years are summarised in this section.

2.3.1 Recommendations for real-time payment security

Recommendations related to real-time payment security were published in the *Observatory for the Security of Payment Means Annual Report* 2020.

In a context where the use of instant transfers is rising rapidly and could replace traditional transfers and even other means of payments, the Observatory remains particularly watchful as to the security of real-time payments. In 2021, instant transfers accounted for 2.5% of the total volume of transfers and 0.9% of the values exchanged (excluding large-value transfers processed through large-value payment systems). The volume of instant transfers has thus tripled since 2020 and this growth is expected to continue over the coming years, encouraged by national and European payment means strategies. In terms of security, the Observatory has taken note that real-time payment fraud has risen more slowly than flows, such that the fraud rate for instant transfers is similar to that of contactless payments (0.014% compared with 0.013%). Fraud on instant transfers amounted to EUR 22 million in 2021, accounting for almost 8% of total transfer fraud. The Observatory thus urges the payment industry to pursue its efforts and investments to strengthen the security of instant transfers. Furthermore, the Observatory repeats its recommendations aimed at ensuring the rapid development of this new means of payment.

2.3.2 Recommendations for payment data security

Recommendations related to payment data security were published in the *Observatory for the Security of Payment Means Annual Report* 2019.

8 See *https://www.youtube.com/*

9 See *https://www.banque-france.fr/*

10 See *https://particuliers.banque-france.fr/*

T2 The Observatory's recommendations on the security of real-time payments

Recommendations	Target audience
Implement, under the conditions set out in PSD 2, strong user authentication for real-time payment authorisation and for all sensitive peripheral transactions (adding a beneficiary, changing details, etc.)	Payment service providers (issuers)
Continuously improve real-time fraud prevention tools, particularly through machine learning technologies, to enhance the performance of the risk analysis systems used	Payment service providers (issuers and recipients)
Make use when necessary of rights management measures, such as ceilings and limits, to restrict the impact of the uncontrolled development of fraud	Payment service providers (issuers)
Identify unusual transactions at reception, particularly when they precede other outgoing transactions	Payment service providers (recipients)
Pay particular attention, before validating a payment order, to the source of the request and the identity of the contact, and to checking the bank details of the beneficiary	Users
Enter bank data on reputable, reliable and trustworthy websites or mobile applications only in this respect, users are encouraged to favour recommended sites and applications and to only connect directly, treating links received through unsecured communication tools such as SMS and email with the utmost caution	Users
Notify the banking institution of any suspicious, unauthorised or fraudulent transactions as soon as possible after the funds have been released	Users
Help to support user watchfulness by providing confirmation tools for beneficiaries and active, real-time information on transactions carried out on their account	Payment service providers

T3 The Observatory's recommendations on the security of payment data

Recommendations	Target audience
Use strong authentication to access services and any sensitive data (under the conditions set by PSD 2, particularly the stipulated 90 day period for account consultation)	Payment service providers
Put in place devices to detect suspicious connections	Payment service providers
Keeping secret all elements used to make payments for payment cards, this watchfulness does not only apply to PIN codes (which should never be communicated to a third party or stored digitally), but to all data present on the card and that facilitate online payments, i.e. the card number, name of the cardholder, expiry date and validation code	Users
Enter bank data on reputable, reliable and trustworthy websites or mobile applications only in this respect, users are encouraged to favour recommended sites and applications and to only connect directly, treating links received through unsecured communication tools such as SMS and email with the utmost caution	Users
Specifically when accessing payment services, use only trusted applications, particularly those published by their payment service providers or whose supplier is duly authorised in France as a payment service provider (i.e. listed in the Regafi or European Banking Authority registers)	Users
Keep regularly up to date on digital risks and their developments via, for example, the government's website *www.cybermalveillance.gouv.fr*	Users

The development of digital uses that incorporate payment information – be they mobile applications, connected objects or access to personalised budget advisory services – has led to payment data being widely circulated and shared with a wide range of players (banks, merchants, Fintechs, etc.) in different environments.

In this context, the implementation of PSD 2 has facilitated the strengthening of open banking security. Supervised third parties can thus access users' payment accounts in order to provide information aggregation or payment initiation services, through dedicated secure interfaces without the need to communicate personal login details. The levels of security and performance offered by these interfaces and their capacity to maintain data confidentiality will be decisive in developing open banking services in the best conditions of trust and fluidity for the user.

The Observatory reminds users of the key role they play in protecting their own payment data and urges them to develop appropriate habits to ensure their data is protected and only shared in trusted environments.

2.3. 3 Recommendations for mobile payment security

Recommendations related to mobile payment security were published in the *Observatory for the Security of Payment Means Annual Report* 2019.

The use of mobile solutions to make point-of-sale card payments has increased sharply over the past two years, encouraged by the health crisis and the possibility of contactless payment above the EUR 50 limit. The volume of this type of payment thus grew 7.5-fold between 2019 and 2021 to account for 3% of face-to-face card payments

and 5% of contactless payments by volume, compared with 0.5% and 1%, respectively, before the health crisis.

At the same time, the fraud rate for contactless mobile payments, which had risen sharply in 2020 to 0.102%, fell back in 2021 to a level closer to the average for card payments, at 0.074%. This decrease reflects the enhanced tools available to manage the risk of fraud, particularly at the time the user is enrolled in the solution. The Observatory calls for this strengthening to continue. To avoid the risks of fraudsters enrolling stolen card numbers in this type of solution, the implementation of strong cardholder authentication, as set out in PSD 2 for sensitive transactions, is imperative.

T4 The Observatory's recommendations on the security of mobile payments

Recommendations	Target audience
Put in place reliable mechanisms for the secure storage of confidential data in mobile applications (sensitive payment data, information on identity, authentication or biometric data)	Payment service providers and their technical service providers
Put in place a mechanism for strong user identification at the time of enrolling the means of payment in the payment application	Payment service providers
Provide users with corrective updates to mobile solutions whenever a security vulnerability is identified that could affect the integrity, confidentiality or availability of the system or data	Suppliers of operating systems or applications, manufacturers of smartphones
Provide users with the level of visibility required on the security measures integrated into their applications while stressing the need to deploy effective countermeasures to combat the unauthorised use of these applications	Payment service providers
Regularly assess the level of security of mobile payment solutions	Payment service providers
Regularly update their mobile operating system	Users
Choose secret codes, passwords and any other personal data used for mobile authentication processes, or at least their payment applications, with care and change them regularly	Users
Activate, if allowed by the operating system, the remote data deletion option in case of loss or theft of mobiles	Users
Use only trusted applications, particularly those recommended by payment service providers	Users
Avoid as much as possible carrying out payment transactions on mobile devices when the communication channel is not dependable (unsecured public Wi-Fi connections, for example)	Users

BOXES

❷ The mandate of the Observatory's cheque working group

Given the context of rapidly declining cheque payment use and the risks of fraud that continue to be high, the Observatory has carried out a specific study on the security of cheque payments. Its findings were published in July 2021 in the Observatory's 2020 Annual Report. They include ten recommendations for industry professionals, public authorities and cheque users.

The Observatory recommended the "[structuring of] long-term cooperation between the parties involved in combating fraud and support[ing] the efforts of law enforcement agencies" (recommendation No. 9) and thus decided to make the cheque fraud working group permanent. It also recommended the "[promotion of] cheque user watchfulness through a communication plan" (recommendation No. 10). The current mandate is intended to set down the objectives and resources of this permanent Observatory working group.

The cheque fraud working group, attached to the Observatory, has the following objectives:

- monitor over time the correct implementation of the Observatory's recommendations made in its 2020 Annual Report;
- structuring cooperation between industry players, particularly with law enforcement agencies and social media platforms, to combat cheque cashing scams;
- organising communication and awareness-raising initiatives that target cheque users to improve fraud prevention.

The Observatory has mandated the Banque de France, which acts as the Secretary to the Observatory, to maintain and update membership of the working group. Like the ad-hoc working group responsible for conducting the initial study, it must include appointments by the Observatory's members, as well as representatives of key industry institutions and service providers, such as cheque manufacturing and processing service providers, the French postal service, Vérifiance, etc.

The "Cheque" working group meets at least once every six months and reports on its activities at the Observatory's plenary meetings.

❸

Victim of cheque fraud? What to do?

1. Contact your bank

Whether a private individual, merchant or tradesperson, you must first inform your bank as quickly as possible in order to consider your options to limit the loss (blocking cheques and transactions, recovering funds, changing authentication data, etc.).

2. File a pre-complaint online

Make a declaration on the Ministry of the Interior's "pre-complaint online"[1] website to later be seen at a police station or by a unit of the police.

3. Get help

- By contacting the fraud line (*Info Escroqueries*) on (+33) 08 05 80 58 17 (freephone) on Monday to Friday from 9 a.m. to 6.30 p.m.
- By contacting the victim helpline for support, information and advice for victims of crime on 116 006 (freephone) or (+33) 01 80 52 33 76 (standard rate), available 7 days a week from 9 a.m. to 7 p.m. or by email to "*victimes@france victimes.fr*" and/or associations available to assist you (*UFC-Que Choisir*, AFOC – *Association Force ouvrière consommateurs*, ALLDC – *Association Léo Lagrange pour la défense des consommateurs*, UNAF – *Union nationale des associations familiales*, ADEIC – *Association de défense, d'éducation et d'information du consommateur*, *Prévention Océane*, etc.).

The Observatory urges all victims of cheque fraud to always file a complaint against persons who have solicited them to cash fraudulent cheques.

1 See *https://www.pre-plainte-en-ligne.gouv.fr/*

3

DIGITAL IDENTITY AND PAYMENT SECURITY

Chapter 3 is available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021

APPENDICES

Appendices 1 and 2 are available in French only in the original version of the report, which can be found here:
https://www.banque-france.fr/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021

Appendices 3, 4 and 5 are available in English in this report.

All tables in Appendix 6 can be downloaded in English at the following address:
https://www.banque-france.fr/en/2021-statistics-appendix-6-annual-report

A3 MISSIONS AND ORGANISATIONAL STRUCTURE OF THE OBSERVATORY

Articles R. 141-1, R. 141-2 and R. 142-22 to R. 142-27 of the *Code monétaire et financier* (French Monetary and Financial Code) set out the responsibilities, composition and operating procedures of the Observatory for the Security of Payment Means.

SCOPE

Pursuant to Article 65 of Law No. 2016-1691 of 9 December 2016 and in accordance with the national strategy for payment means, Article L. 141-4 of the French Monetary and Financial Code has been amended to extend the missions of the Observatory for Payment Card Security to all cashless payment means. Henceforth, in addition to cards issued by payment service providers or equivalent institutions, all other cashless payment means now fall within the scope of the missions of the Observatory for the Security of Payment Means.

In accordance with Article L. 311-3 of the French Monetary and Financial Code, a means of payment is understood as any instrument that allows any person to transfer funds, regardless of the form that such an instrument takes or the technical process used. The means of payment listed below fall within the remit of the Observatory.

- **Credit transfers**, carried out by the payment service provider that holds the payer's payment account, consist in crediting a beneficiary's payment account with a payment transaction or a series of payment transactions from a payer's payment account, pursuant to instructions from the payer.

- **Direct debits** are used to debit a payer's payment account, where a payment transaction is initiated by the beneficiary on the basis of the payer's consent given to the beneficiary, to the beneficiary'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 transmit funds. There are different types of cards.
  - Debit cards draw on a payment account and enable their holders to make withdrawals or payments that are debited in accordance with a timeframe set out in the card issuance contract.
  - Credit cards are backed by a credit line that carries an interest rate and a maximum limit negotiated with the customer. These cards serve to make payments and/or cash withdrawals and enable their holders to pay the issuer at the end of a certain period. The payment acceptor is paid directly by the issuer without any particular credit-related delay.
  - Commercial cards are issued to businesses, public bodies or natural persons engaged in an independent activity. Their use is restricted to expenses incurred in a professional capacity, and any payments made with them are directly billed to the account of the business, public body or natural person engaged in an independent activity.
  - Prepaid cards can store electronic money.

- **Electronic money** is a monetary value that is stored in electronic form, including magnetically, representing a claim on the issuer. It is issued (by credit institutions or electronic money institutions) against the remittance of funds for the purpose of performing payment transactions. It can be accepted by a natural person or legal entity other than the electronic money issuer.

- **Cheques** are documents whereby a person, the drawer, instructs a credit institution, the drawee, to pay on demand (at sight) a certain sum to the drawer or to a third party, the beneficiary.

- **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.

RESPONSIBILITIES

Pursuant 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 a threefold responsibility.

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

- It compiles statistics on fraud. These statistics are compiled from the information reported by the issuers of payment means to the Observatory's secretariat. The Observatory issues recommendations aimed at harmonising procedures for establishing fraud statistics for the various cashless payment means.

- It maintains a technology watch on cashless payment means, with a view to proposing ways to tackle threats to the security of payment instruments. To this end, it collects all the available information that is liable to reinforce the security of payment means and puts

it at the disposal of its members. It organises the exchange of information between its members while respecting confidentiality where necessary.

In accordance with Article R. 141-2 of the French Monetary and Financial Code, the Minister of the Economy and Finance may request the Observatory's opinion on various issues, setting a time limit for its responses. These opinions may be made public by the Minister.

COMPOSITION

The composition of the Observatory is set out in Article R. 142-22 of the French Monetary and Financial Code. Accordingly, the Observatory is made up of:

- a Deputy and a Senator;
- eight general government representatives;
- the Governor of the Banque de France or his representative;
- the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French prudential supervision and resolution authority) or his representative;
- a representative of the *Commission nationale de l'informatique et des libertés* (CNIL – the French data protection body);
- fourteen representatives of issuers of payment means and operators of payment systems;
- five representatives of the Consumer Board of the French National Consumers' Council;
- eight representatives of merchants' professional organisations and corporations, notably from the retail sector, the supermarket sector and remote sales and e-commerce channels;
- two qualified prominent persons chosen for their expertise.

The names of the members of the Observatory are listed in Appendix 4 of this report.

The members of the Observatory, other than the members of Parliament, those representing the state, the Governor of the Banque de France and the Secretary General of the ACPR, are appointed for a three-year term. Their appointments shall be renewable.

The President is chosen from the Observatory members by the Minister of the Economy and Finance. She or he has a three-year term of office, which may be renewed. François Villeroy de Galhau, the Governor of the Banque de France, is the current President of the Observatory.

OPERATING PROCEDURES

In accordance with Article R. 142-23 *et seq.* of the French Monetary and Financial Code, the Observatory meets at least twice a year at the invitation of its President. The meetings are held in camera. Measures proposed within the Observatory are adopted by absolute majority. Each member has one vote and the President has the casting vote in the event of a tie. The Observatory has adopted internal rules of procedure setting out its operating conditions.

The secretariat of the Observatory, which is provided by the Banque de France, is responsible for organising and following up on meetings, centralising the information required for the establishment of payment means fraud statistics, and collecting and making available to members the information required to monitor the security measures adopted and maintain the technology watch in the field of payment means. The secretariat also drafts the *Annual Report of the Observatory for the Security of Payment* means that is submitted every year to the Minister of the Economy and Finance and transmitted to Parliament.

The Observatory may set up working or study groups, notably when the Minister of the Economy and Finance requests its opinion. The Observatory defines the mandate and composition of these groups by absolute majority. The groups report on their work at each meeting of the Observatory. They may hear all persons who could provide them with information that is useful to their mandates.

Given the sensitivity of the data reported to them, 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 maintain the confidentiality of the information that is transmitted to them in the course of their work. To this end, the Observatory's rules of procedure stipulate the members' obligation to make a commitment to the President to ensure the complete confidentiality of working documents.

A4 MEMBERS OF THE OBSERVATORY

Pursuant to Article R. 142-22 of the *Code monétaire et financier* (the French Monetary and Financial Code), the members of the Observatory, other than the members of Parliament, those representing the state, the Governor of the Banque de France and the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French prudential supervision and resolution authority), are appointed for a three-year term by order of the Minister of the Economy. The most recent appointment order was issued on 28 April 2022.

PRESIDENT

François VILLEROY DE GALHAU
Governor of the Banque de France

MEMBERS OF PARLIAMENT

Éric BOCQUET
Senator

Rémi REBEYROTTE
Deputy

REPRESENTATIVES OF THE GENERAL SECRETARIAT OF THE ACPR

- The Secretary General or her/his representative:
  Dominique LABOUREIX
  Olivier FLICHE

REPRESENTATIVES OF GENERAL GOVERNMENT

Nominated on the recommendation of the General Secretariat for Defence and National Security:

- The Director General of the French National Cybersecurity Agency or her/his representative:
  Grégoire LUNDI

Nominated on the recommendation of the Minister of the Economy, Industry and Digital Affairs:

- The Senior Official for Defence and Security or her/his representative:
  Christian DUFOUR
- The Head of the Treasury or her/his representative:
  Pierre-Olivier CHOTARD
  Clara PAOLONI
- The Chair of the *Institut d'émission des départements d'outre-mer* (IEDOM – the note-issuing bank for the French overseas departments) and Director General of the *Institut d'émission d'outre-mer* (IEOM – the French overseas note-issuing bank):
  Marie-Anne POUSSIN-DELMAS
- The Director General for Competition, Consumer Affairs and the Punishment of Fraud Offences or her/his representative:
  Aurélien HAUSER

Nominated on the recommendation of the Minister of Justice:

- The Director for Criminal Affairs and Pardons or her/his representative:
  Louise NEYTON
  Marion LE LORRAIN

Nominated on the recommendation of the Minister of the Interior:

- The Deputy Director for the fight against financial crime at the *Direction centrale de la police judiciaire* (DCPJ – the central directorate of the judicial police) or her/his representative:
  Thomas DE RICOLFIS
  Anne-Sophie COULBOIS
- The Director General of the *Gendarmerie nationale* or her/his representative:
  Étienne LESTRELIN

Nominated on the recommendation of the *Commission nationale de l'informatique et des libertés* (CNIL – the French data protection body):

- The Head of Economic Affairs or her/his representative:
  Nacéra BEKHAT
  Aymeric PONTVIANNE

REPRESENTATIVES OF ISSUERS OF PAYMENT MEANS AND OPERATORS OF PAYMENT SYSTEMS

Thomas GOUSSEAU
Member of the Board of Directors
Association française des établissements de paiement et de monnaie électronique (Afepame)

Amelia NEWSOM-DAVIS
Director Pay Services Orange
Association française du multimédia mobile (AF2M)

Corinne DENAEYER
Head of Market Research
Association française des sociétés financières (ASF)

Sébastien MARINOT
Head of Strategy and External Relations, Cash Management
BNP Paribas (BNPP)

Carole DELORME D'ARMAILLE
Director General
Office de coordination bancaire et financière (OCBF)

Caroline GAYE
Director General
American Express France (Amex)

Violette BOUVERET
Vice-chair Cyber & Intelligence
MasterCard France

Philippe LAULANIE
Executive Director
Groupement des cartes bancaires (GCB)

Philippe MARQUETTY
Global Head of Payments and Cash Management Products
Société Générale

Évelyne BOTTOLLIER-CURTET
Card scheme relationships manager
Groupe BPCE

Romain BOISSON
Executive Director
Visa Europe France

Jérôme RAGUÉNÈS
Director of the Digital, Payments
and Operational Resilience Department
Fédération bancaire française (FBF)

Jean-Marie VALLÉE
Director General
STET

Marie-Anne LIVI
Head of Strategy and Market Relations
Crédit Agricole

CORPORATE REPRESENTATIVES

Bernard COHEN-HADAD
President of the Business Financing Commission
Confédération des petites et moyennes entreprises (CPME)

Émilie TISON
Confederation of Wholesale and International Trade
Mouvement des entreprises de France (MEDEF)

Isabelle CHARLIER
President of the electronic banking and payment means commission
Association française des trésoriers d'entreprise (AFTE)

REPRESENTATIVES OF THE CONSUMER BOARD OF THE FRENCH NATIONAL CONSUMERS' COUNCIL

Mélissa HOWARD
Lawyer
Association Léo Lagrange pour la défense des consommateurs (ALLDC)

Morgane LENAIN
Lawyer
Union nationale des associations familiales (Unaf)

Mathieu ROBIN
Project leader Banking/Insurance
UFC – *Que choisir*

Hervé MONDANGE
Lawyer
Association Force ouvrière consommateurs (Afoc)

Bernard FILLIAT
Association pour l'information et la défense des consommateurs salariés CGT (INDECOSA-CGT)

REPRESENTATIVES OF MERCHANTS' PROFESSIONAL ORGANISATIONS

Jean-Michel CHANAVAS
General delegate
Mercatel

Isabelle CLAIRAC
Director General of Market Pay
Fédération du commerce et de la distribution (FCD)

Philippe JOGUET
Correspondent on financial issues
Conseil du commerce de France (CdCF)

Marc LOLIVIER
General delegate
Fédération du e-commerce et de la vente à distance (Fevad)

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

PERSONS CHOSEN FOR THEIR EXPERTISE

Claude FRANCE
Chief Operations Officer, France
Worldline

David NACCACHE
Professor
École normale supérieure (ENS)

A5 METHODOLOGICAL APPROACH USED TO MEASURE FRAUD ON CASHLESS PAYMENT MEANS

GENERAL FRAMEWORK

Definition of payment means fraud

The Observatory's definition of cashless payment fraud is now aligned with that of the European Banking Authority (EBA) as set out in its 2018 Guidelines on reporting requirements for fraud data (EBA/GL/2018/05).[1] Fraud is thus defined in this report as the **illegitimate use of a payment instrument 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 lawful beneficiary of the funds (the acceptor and/or creditor), an insurer, a trusted third party or any party involved in the chain of design, manufacture, transport or distribution of physical or logical data that could incur civil, commercial or criminal liability;
- **by whatever means**:
  - the methods used to obtain, without lawful reason, the means of payment or related data (theft, taking possession of the payment means or data, hacking of acceptance devices, etc.),
  - the procedures for using the means of payment or related data (payments/withdrawals, face-to-face or remote payments, via physical use of the means of payment or the related data, etc.),
  - the geographical area of issuance or use of the means of payment and related data;
- **regardless of the identity of the fraudster**: a third party, the account-holding institution and/or issuer of the means of payment, the lawful holder of the means of payment, the lawful beneficiary of the funds, a trusted third party, etc.

In accordance with this definition, the Observatory measures fraud by recording all payment transactions that have given rise to an entry on the account of at least one of the counterparties of the transaction and which have subsequently been rejected on fraud-related grounds. Thus, fraud does not include attempted fraud, whereby the fraud is prevented before the transaction is executed.

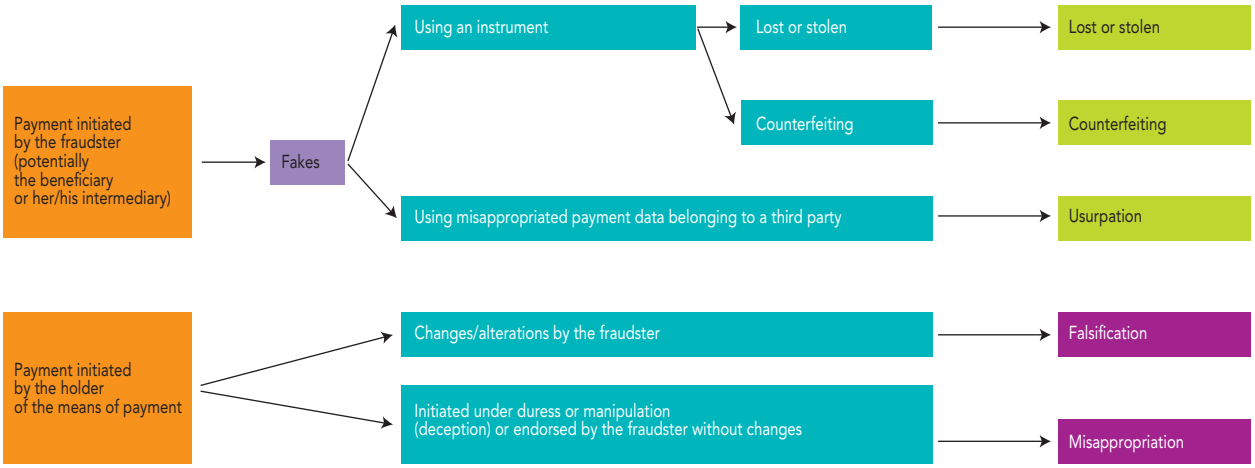
The following are also excluded from fraud:

- improper use of a means of payment due solely to insufficient funds and resulting notably in a non-payment;
- the use of a false or stolen identity to open an account and/or obtain a means of payment for the purposes of making payments;
- situations where the legitimate holder of the means of payment authorises but stops a payment by circumventing the procedures provided for by law by contesting said payment in bad faith, including in the case of commercial disputes (for example, the case of a bankrupt site which does not deliver the ordered products or when the object purchased does not comply with the order);
- cases of fraud where the payer makes a payment to a beneficiary who is a fraudster or an accomplice of a fraudster where the product or service purchased does not exist and is therefore not delivered (e.g. illegal sale of financial products such as investment products or loan offers).

The Observatory applies a "gross approach" when measuring fraud, which consists in identifying the initial payment transaction amounts without taking into account any measures that may subsequently be taken by the counterparties to mitigate the related losses (for instance, the interruption of product delivery or service provision, out-of-court agreement to reschedule payment in the event of wrongful repudiation of the payment, damages and interest subsequent to legal proceedings, etc.). In its 2015 Annual Report,[2] the Observatory for Payment Card Security considered that such measures reduced gross estimated card payment fraud by 5%.

The Observatory's secretariat collects the fraud data from all relevant institutions, using different approaches depending on the means of payment (see below). Due to the confidential nature of the personal data gathered, only national consolidated statistics are made available to the members of the Observatory and presented in its annual report.

Overview of the different types of fraud



Note: This overview should be considered alongside the Banque de France's official guides on statistical data collection on payment fraud.

Types of payment means fraud

In order to analyse payment means fraud, the Observatory has defined three main fraud types, bearing in mind that they do not all apply in the same manner to the various payment instruments:

- **fakes** (theft, loss, counterfeit): fraud involving the issuance of false payment orders either through a physical payment instrument (card, chequebook, etc.) that has been stolen (when sent by the payment service provider or after receipt by the legitimate beneficiary), lost or counterfeited, either through the misappropriation of bank details or credentials;
- **falsification**: modification of a regular payment order by making one or more alterations (amount, currency, name of the beneficiary, account details of the beneficiary, etc.);
- **misappropriation**: a transaction initiated by the payer under duress or manipulation (deception), without the fraudster altering or modifying the status.

Geographical breakdown of payment means fraud

Fraud is broken down into domestic, European and international transactions. Until 2020, European transactions were based on the Single Euro Payment Area (SEPA). Since 2021, the European transactions are based on the European Economic Area (EEA) in order to align the Observatory's methodology with that of the European Banking Authority (EBA). The United Kingdom is for instance part of the SEPA, but since Brexit in 2020, is now outside the EEA.

1. These guidelines were drawn up pursuant to Article 96(6) of the Second European Payment Services Directive (EU Directive 2015/2366, the so-called "PSD 2").

2. See *Annual Report of the Observatory for the Security of Payment Cards* 2015 (page 12).

A6 STATISTICS

All tables in Appendix 6 can be downloaded in English at the following addresse :
https://www.banque-france.fr/en/2021-statistics-appendix-6-annual-report

www.banque-france.fr