OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2020

BANQUE DE FRANCE
EUROSYSTÈME

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

ANNUAL REPORT 2020

addressed to
The Minister of the Economy, Finance and Recovery
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 2021

CHAPTERS

SUMMARY 6

CHAPTER 1
INITIAL ASSESSMENT OF THE ROLL-OUT OF STRONG CUSTOMER AUTHENTICATION FOR ONLINE CARD PAYMENTS 9

1.1 Plan for the roll-out of strong customer authentication for online card payments 9

1.2 Actions to assist the migration process 10

1.3 Assessment of migration 13

CHAPTER 2
FRAUD IN 2020 21

2.1 Overview 21

2.2 Card payment and withdrawal fraud 25

2.3 Cheque fraud 30

2.4 Credit transfer fraud 32

2.5 Direct debit fraud 34

Chapters 3 and 4 and the appendices 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-2020*

CHAPTER 3
TECHNOLOGY WATCH ON REAL-TIME PAYMENT SECURITY

3.1 Introduction

3.2 The development of real-time in payments

3.3 The fight against fraud

3.4 Conclusion and recommendations

CHAPTER 4
CHEQUE FRAUD: LESSONS LEARNED AND RECOMMENDATIONS

4.1 A means of payment in rapid decline, but still used by certain persons and businesses

4.2 A vulnerable means of payment given its decline and changes in its use

4.3 Cheque fraud: initial lessons learned from the Observatory's statistics

4.4 Amongst the different types of fraud, the remittance of fraudulent cheques is growing significantly

4.5 Recommendations of the Observatory

4.6 Security recommendations for the use of cheques

APPENDICES

A1 Security recommendations for the use of payment means

A2 Payer protection in the event of unauthorised payments

A3 Missions and organisational structure of the Observatory

A4 Members of the Observatory

A5 Methodological approach used to measure fraud on cashless payment means

A6 Statistics

BOXES

1 Mechanisms for handling e-commerce payment flows in the event of authentication infrastructure or device failures 17

2 Fraud statistics for payment cards: respondents 39

3 Domestic remote payment fraud, by sector of activity 40

4 Indicators provided by law enforcement agencies regarding ATM and payment terminal attacks 41

5 Occasional beneficiaries and trusted beneficiaries of credit transfers

6 Instant credit transfers: use cases

7 Confirmation of Payee (CoP) tools

8 Real-time payment security: machine learning use cases

SUMMARY

Against the backdrop of the health crisis which had such a profound effect on the year 2020, the Observatory for the Security of Payment Means *was able to closely monitor its impact on the payment habits of French households and professionals as well as on the pattern of changes in the modus operandi of fraudsters. This* 2020 Annual Report *describes the trends observed as a result of the crisis, together with the steps taken by the Observatory to maintain a high level of security and confidence in cashless payments.*

Chapter 2 *of the* Report *presents* ***the trends in payment flows and payment fraud in 2020****. In particular, it highlights the acceleration of the trend towards the digitisation of payments resulting from the crisis, as illustrated by the following:*

- *on the one hand, by a very sharp decline, from the time of the March 2020 lockdown, in transactions involving physical contact: cheques (–25% in value), cash withdrawals (–15% in value) and card payments requiring the entry of a PIN code thus recorded an unprecedented drop in flows compared with historical trends;*

- *on the other hand, unprecedented growth in two types of usage: contactless payment (+86% in value), which became the preferred method of payment at the point of sale and was greatly boosted by the increase in the payment limit from EUR 30 to EUR 50, effective 11 May 2020; and online payment (+8% in value), which was stimulated, in particular, by the movement of traditional neighbourhood shops towards new modes of consumption (home delivery, click and collect, etc.).*

This chapter also shows that, despite the impact of the health crisis on payment practices, the level of fraud observed on payments issued in France remains under control, with the notable exception of cheques, where the fraud rate is rising markedly.

- *For the third consecutive year, cheques remained the means of payment most subject to fraud in terms of both value and proportion. Indeed, despite the decline in use of cheques in 2020, the associated share in fraud amounts for all means of payment remained the highest at 42%, for a value of EUR 538 million, and the rate of cheque fraud rose to 0.088%, representing the equivalent of one euro of fraud for every EUR 1,100 of payment. Theft of cheques and chequebooks is still the main modus operandi, accounting for the largest share of fraud amounts at 68%, a clear increase year-on-year (55% in 2019).*

- *The rate of fraud associated with French payment cards remained at an essentially manageable level of 0.068%, i.e. the equivalent of one euro of fraud for every EUR 1,500 of transactions, despite the massive shift in flows towards types of transactions that are more vulnerable to the risk of fraud. These include contactless payments (where the fraud rate has fallen to 0.013% despite the increase in the payment ceiling and is close to the fraud rate for payments involving the entry of a PIN code) and remote payments (where the fraud rate is virtually stable at 0.174%).*

- *Although the rate of fraud on credit transfers remained particularly low at 0.0008% (equivalent to one euro of fraud for every EUR 120,000 of payment), the Observatory nevertheless highlights the resurgence of fraud by means of social engineering primarily targeting companies. Indeed, the strengthening of digital exchanges and the*

widespread practice of working from home, leading to a loss of the usual reference points for accounting and financial services, have been conducive to the perpetration of this type of fraud. Moreover, government agencies have also been confronted with the development of a type of fraud targeting companies' short-time working arrangements, based on the theft of the identities of beneficiary companies in order to misappropriate the financial aid made available in the context of the Covid-19 crisis.

- *Direct debit fraud fell sharply in 2020, to EUR 1.9 million (–83% year-on-year). This rate of fraud is thus the lowest among all means of payment, at 0.0001%, i.e. the equivalent of one euro of fraud for one million euros of payment.*

***Chapter 1** presents **the first assessment of the migration of the French financial sector towards strong customer authentication for online card payments**. This development seems all the more necessary as it is taking place against a background of increasing use of this method of payment, which accounts for more than two-thirds of fraud even though it represents only 22% of transactions.*

Although the implementation of the migration plan drawn up by the Observatory had to be adjusted to take account of public health constraints, in particular with the granting of a three-month period of flexibility in mid-2020, the situation at the end of June 2021 reflected a high level of compliance by the French financial sector:

- *More than 80% of cardholders making online purchases have been enrolled in a strong authentication system that they use to validate their transactions. The initiatives undertaken by the Banque de France and the* Autorité de contrôle prudentiel et de résolution *(French prudential supervision and resolution authority) with the institutions that have made the least progress should make it possible to achieve full compliance by autumn 2021.*

- *Some 95% of the flows of French e-merchants comply with the regulations, i.e. they use an authentication request from their customer or are covered by an exemption recognised as valid by the card issuer.*

These results are the fruit of the coordination work carried out within the framework of the Observatory, which has endeavoured to ensure an ambitious migration while maintaining e-commerce activity in an environment that has been severely constrained by the public health crisis. They constitute a validation of the end of the migration plan, it being understood that the Observatory will continue to closely oversee its further implementation with a view to ensuring full compliance of the French financial sector in the short term, while at the same time bolstering the smooth operation of online payments.

***Chapter 4** reports on the work carried out by the Observatory to **improve the security of cheque payments**. This work has made it possible to better identify the main vulnerabilities of this means of payment that are exploited by fraudsters, and to develop a set of security objectives designed to counter them. These objectives are mainly based on the enhancement by banking institutions of their analysis capabilities and fraud prevention measures, the promotion of cooperation between sector players and, lastly, raising user awareness.*

The Observatory will monitor the implementation of these objectives by market players and evaluate their effectiveness over time in the light of changes in annual fraud involving this means of payment.

*Finally, **Chapter 3** reports on the **technology watch on real-time payment security**, in a context where the use of instant transfers, although still limited (1% of transfers issued in 2020 in volume terms), was on the rise, with flows tripling in one year. While these payments offer greater convenience to users through the immediate availability of funds, they require security measures that are geared to the challenges of real-time transactions.*

The Observatory thus recommends that a set of fraud prevention measures be put in place at the time of payment initiation, combining the requirement for strong authentication of the payer provided for by the Regulations with the introduction of payment limits tailored to the customer's usage, as well as real-time identification tools for transactions that pose a high level of risk. The Observatory also draws attention to the important role played by users' behaviour in ensuring the security of their payment means, and urges market players to conduct appropriate awareness-raising activities when instant payment solutions are being made available.

1

INITIAL ASSESSMENT OF THE ROLL-OUT OF STRONG CUSTOMER AUTHENTICATION FOR ONLINE CARD PAYMENTS

1.1 Plan for the roll-out of strong customer authentication for online card payments

The use of strong customer authentication to initiate an electronic payment is a key payment security provision introduced in the second European Payment Services Directive (PSD 2). Although this directive has been in force since 13 January 2018, various second-level texts issued by the European Banking Authority (EBA) have clarified the rules applicable to online card transactions:

- regulatory technical standards on strong customer authentication (RTS SCA), which specified the conditions for implementing strong authentication, were to come into effect on 14 September 2019;
- Opinion EBA-OP-2019-11 of 16 October 2019 endorsed the need to allow market players, under the responsibility of national authorities, an additional period of time until 31 December 2020 to comply with the provisions governed by the above-mentioned standards; this additional period was supplemented by an assessment phase in the first quarter of 2021.

This prompted the Observatory to develop a migration plan for the French financial sector, the final version of which was published on its website on 30 October 2019.[1] However, the outbreak of the public health crisis linked to the Covid-19 pandemic in the spring of 2020 led the Observatory to incorporate more flexible measures and, in particular, to provide a margin of flexibility of three additional months.

1.1.1 The migration plan for the French financial sector

The plan approved by the Observatory for the migration to strong customer authentication comprises two components:

- the first is directed at consumers: enrolling cardholders in authentication arrangements that comply with the PSD 2 definition of strong authentication, which will replace one-time passwords (OTP) sent by SMS as the only acceptable authentication factor;
- the second is directed at professional participants in the payment chain, including e-merchants: upgrading the authentication infrastructure in order to ensure that the rules of responsibility and exemptions to strong authentication provided in PSD 2 are properly managed.

The plan includes performance indicators setting out targets and deadlines for both components, together with action plans designed to provide support to the French financial sector in meeting its compliance obligations.

1 See *https://www.banque-france.fr/sites/default/files/medias/documents/2019-10-30_-_osmp_-_plan_de_migration_dsp2.pdf*

1.1.2 Strong customer authentication solutions

Strong authentication is based on the use of two or more elements belonging to at least two different categories of authentication factor, from the following three categories:

- a "knowledge" factor: information known only to the user, such as a confidential code, a password or a piece of personal information;
- a "possession" factor: an object that only the user owns, and which can be recognised without risk of error by the payment service provider (PSP): a card, a smartphone, a watch or smartwatch, a key ring, etc.;
- an "inherence" factor: a user-specific authentication factor, i.e., a biometric characteristic.

PSD 2 provides 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 amount 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.

T1 Main strong authentication solutions for online card payments

Combination of authentication factors	Knowledge	Inherence
Possession	Entering a confidential code in the cardholder's secure banking application or Entering a single-use code sent by SMS or voice server + entering a confidential code or Entering a confidential code on an electronic unit supplied by the bank	Reading a biometric print in the cardholder's secure banking application

Source: Observatory for the Security of Payment Means.

1.1.3 The role of merchants in the migration

Prior to the introduction of DSP 2, merchants who accepted online card payments had the option of using a secure payment by activating the 3D-Secure protocol. However, they were not required to justify their choice when they did not request authentication of their customer. This method of activation "by the hand of the merchant" is no longer allowed, as the new regulations change the authentication decision rules:

- merchants must now 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 the Directive 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.

Merchants who accept online card payments were thus invited to contact their bank and, where appropriate, their technical acceptance provider, in order to prepare for these changes. In particular, they were requested to:

- check that their online payment acceptance contract includes the possibility of using the 3D-Secure protocol;
- verify their technical ability to issue payments via 3D-Secure;
- ensure that the use of this protocol increases so as to safeguard the continuity of their business, particularly in view of the planned lowering of the thresholds for rejecting non-compliant transactions (or soft declines), and to facilitate the ability to make use of exemptions, with version 2 of the 3D-Secure protocol, for merchants who so wish.

In parallel, the Observatory encouraged payment market professionals to work with their merchant customers, in order to make them aware of these new requirements and to support them in these changes.

1.2 Actions to assist the migration process

In order to stimulate and provide guidance for the migration of all players in the French financial sector, the Observatory had included several support actions in its roadmap, either in the initial plan or in the additional measures introduced in September 2020.

1.2.1 Clarification of the rules applying to the various transaction categories

With regard to remote card payments, the regulations provide for different qualifications. These determine whether or not strong authentication must be applied:

- **Customer-initiated online transactions** (CIT) are payments performed online by the cardholder, using either a browser or an application. These transactions are subject to the requirement for strong cardholder authentication, but may be exempted by the RTS if the conditions for such exemption are met (*see below*).
- **Merchant-initiated online transactions** (MIT) are transactions initiated by the merchant without the active presence of the cardholder, in situations where the issuing of the payment is dissociated from the commitment to pay, for example: in the case of a subscription, a payment in several instalments, a consumption-based service (flexible subscription, transport reservation, etc.), payments made in several amounts at the time of delivery of the various items in the shopping cart, or a booking guarantee fee payable in the event of a no-show. These transactions, usually issued without the customer being actively present on the merchant's site, are not subject to the requirement for strong cardholder authentication, but must contain evidence of strong authentication provided at the time of the customer's commitment to pay (in line with a process known as transaction "chaining"). This commitment, known as an "MIT mandate", must specify the settlement conditions to which the client has committed (amount, number of transactions, frequency, period of validity).
- **Remote transactions issued via a non-electronic channel (MOTO** – mail order/telephone order) are transactions for which the card data has been transmitted by the cardholder via a channel that does not allow it to be processed automatically (e.g. by mail, fax, e-mail, telephone call or voice server), and which is entered, for payment purposes, by the merchant. These transactions are excluded from the scope of DSP 2 and are not subject to the requirement for strong cardholder authentication.
- **Transactions carried out using anonymous payment instruments**, including anonymous prepaid cards, are not subject to the requirement for strong cardholder authentication.
- **So-called "one-leg" transactions for which the card issuer or the payment acquirer is not located in the European Economic Area**, which cannot always be authenticated and for which strong authentication is only required on a best-effort basis.

In the case of online CIT-type transactions initiated by card, the RTS provide for **five grounds for exemption from strong authentication:**

- **Low-value payments** (Article 16): this exemption covers payments of up to EUR 30 each and is applicable where the cumulative amount of the most recent consecutive transactions exempted under this provision and performed with a given card does not exceed EUR 100 or if the number of transactions does not exceed five. Operation of this exemption is similar to that applying to contactless payments at the point of sale (provided for in Article 11, with higher caps).
- **Low risk payments** (Article 18): this exemption relates to transactions recognised by the merchant and/or by the cardholder's bank and/or by the merchant's bank as having a reduced level of risk, on the grounds that the parameters of the transaction correspond to the cardholder's payment habits (purchase from its usual terminal, known delivery address, nature of purchase, amount, etc.).
- **Recurring payments** (Article 14): this exemption covers payments of a fixed amount and frequency, starting from the second transaction. However, this exemption is of limited interest for card payments, where transactions beyond subscription are initiated by the merchant (MIT-type).
- **Payments to a trusted beneficiary** (Article 13): this exemption concerns payments to a beneficiary who has been designated as trusted by the cardholder. In this case, the registration operation of the trusted beneficiary must itself be strongly authenticated by the cardholder.
- **Payments initiated electronically via secure payment processes or protocols reserved for use between professionals** (Article 17): the use of this exemption requires 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.

PSD 2 provides that it is the responsibility of the institution holding the account of the cardholder to protect the latter against fraud. This provision implies that the application of an exemption cannot be taken for granted: even if a transaction meets the eligibility criteria from the point of view of the beneficiary, the cardholder's bank may reject its application if it identifies an aggravated risk for its client, and may then request strong authentication to secure the transaction.

The Observatory has endeavoured to rely on these qualification rules to determine the conditions for implementing strong authentication for certain specific use cases, summarised in Table 2.

T2 Conditions for implementation of strong authentication for special cases

Use cases	Description	Associated qualifications and requirements
"One click" payment	Payment initiated online by the cardholder for the purchase of a service or a physical or digital good, using a card registered in the customer area ("card on file").	Client-initiated transaction (CIT) requiring strong authentication unless one of the five exemptions provided for by the RTS is applicable. Registration of the card in the customer area, an action potentially involving a risk of fraud, must automatically be subject to strong authentication.
Payment(s) on dispatch or deferred	Payment(s) linked to an online order and deferred (pre-order, payment on dispatch, etc.).	At the time of purchase, strong authentication (CIT) is required unless one of the five exemptions in the RTS applies. Authentication at the time of purchase must be performed for the entire shopping cart. At the time of dispatch, an authorisation is requested (without authentication, as the transaction takes place when the customer is not present), together with the initial proof of authentication (MIT with chaining).
Recurring or staggered transactions	A series of payments linked to an online subscription or payment in instalments (payment facility granted to the customer, etc.).	At the time of purchase or subscription, strong authentication is required (CIT): • on an amount that covers the entire shopping cart, if known in advance; • on an amount at zero euros (or "request for information") if the amount is not known or cannot be estimated. For subsequent payment dates, an authorisation is requested (without authentication, as the transaction takes place when the customer is not present), together with the initial proof of authentication (MIT with chaining).
Payment associated with a booking	A payment for a good or service, the triggering and amount of which are dependent on actual consumption. This use case also covers non-consumption, when the bearer does not show up to consume the booked service ("no show").	At the time of booking, strong authentication (CIT) is required: • on the maximum value, if known; • on an amount at zero euros (or "request for information") if the amount is not known. When the final amount is known, an authorisation is requested, (without authentication, as the transaction takes place when the customer is not present), together with the initial proof of authentication (MIT with chaining).
Payment through an e-wallet solution	Payment via a payment or e-money account provided by an approved payment service provider (PSP), replenished by a payment card pre-registered by the user.	At the time of the e-wallet payment to the merchant: • Implementation by the PSP of its strong authentication solution in compliance with PSD 2 rules; • In the event that the payer's balance with the PSP is insufficient, the card account replenishment transaction is subject to PSD 2 rules (application of strong authentication unless exempted).

Source: Observatory for the Security of Payment Means.
Note: CIT: customer-initiated transaction; RTS: Regulatory Technical Standard; MIT: merchant-initiated transaction.

1.2.2 The plan to ramp up soft decline issuings

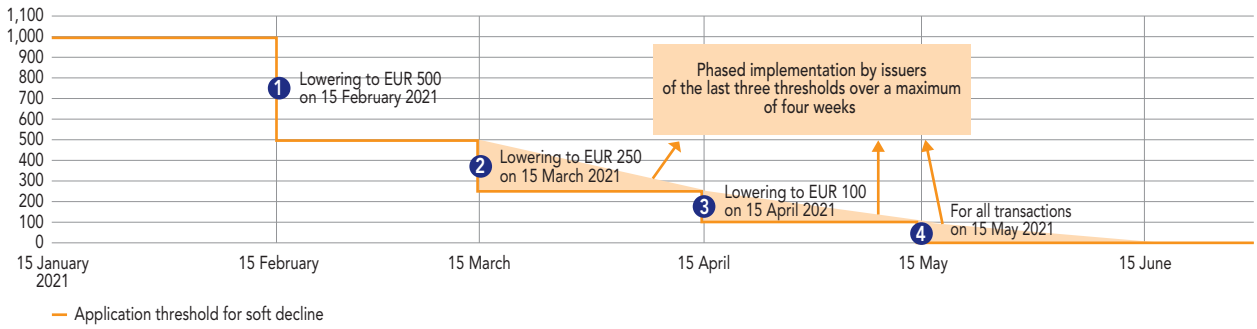
Soft decline is a standardised mechanism by which the card issuer rejects a transaction identified as non-compliant with the regulations (that is, without a request for authentication or an element that could justify the use of an exemption), offering the merchant the option of re-submitting the transaction via 3D-Secure. As foreseen in the initial migration plan, this mechanism was introduced in early April 2020, on a reduced basis so as to avoid any negative impact on e-merchants (issuance in response to previous rejection or hard decline).

The system was then used as a lever to bring the French market progressively into compliance, with a decreasing threshold approach (*cf. Chart 1*):

- 1 October 2020: non-compliant transactions of more than EUR 2,000 declined,
- 15 January 2021: non-compliant transactions of more than EUR 1,000 declined,
- 15 February 2021: non-compliant transactions of more than EUR 500 declined,
- 15 March 2021: non-compliant transactions of more than EUR 250 declined,
- 15 April 2021: non-compliant transactions of more than EUR 100 declined,
- 15 May 2021: all non-compliant transactions declined.

For the last three thresholds, which covered larger transaction and merchant volumes, the implementation of soft decline was phased in by issuers over four weeks.

C1 Trajectory for the implementation of soft decline in the first half of 2021 (y-axis: amount in euros)



Source: Observatory for the Security of Payment Means.

1.2.3 Strengthening the continuity of authentication infrastructures

The migration plan for the French financial sector validated by the Observatory provides for the widespread use of the 3D-Secure protocol, in particular version 2, which allows the merchant to benefit from the exemptions provided by PSD 2 upon request or at the initiative of the issuer.

This more systematic use of the 3D-Secure protocol makes the e-commerce sector dependent on the proper functioning of authentication infrastructures, in particular banks' authentication control servers (ACS) and the 3D-Secure flow routing servers set up by the card payment systems (DS – directory servers). These infrastructures having thus taken on a systemic dimension for e-commerce, the Observatory has endeavoured to define continuity mechanisms that are designed to ensure that merchants are able to continue their operations in the event of a failure of one of the links in the authentication chain.[2] It has taken steps to ensure that these mechanisms are appropriately applied by all market players.

1.3 Assessment of migration

The Observatory draws attention to the high level of mobilisation of all players in the payments ecosystem to complete the migration plan, despite the current public health crisis. At the end of June 2021, the progress indicators show a high level of compliance with the two components of the migration plan.

This achievement confirms the relevance of the system adopted, which enabled all stakeholders to be involved in the operational management of the migration plan on an almost continuous basis and provides support for the Observatory in its various roles.

It also highlights the value of regular exchanges or exchanges devoted to specific subjects for the purpose of reducing the level of fraud while taking into account the economic imperatives of e-commerce players in a particularly critical health crisis period.

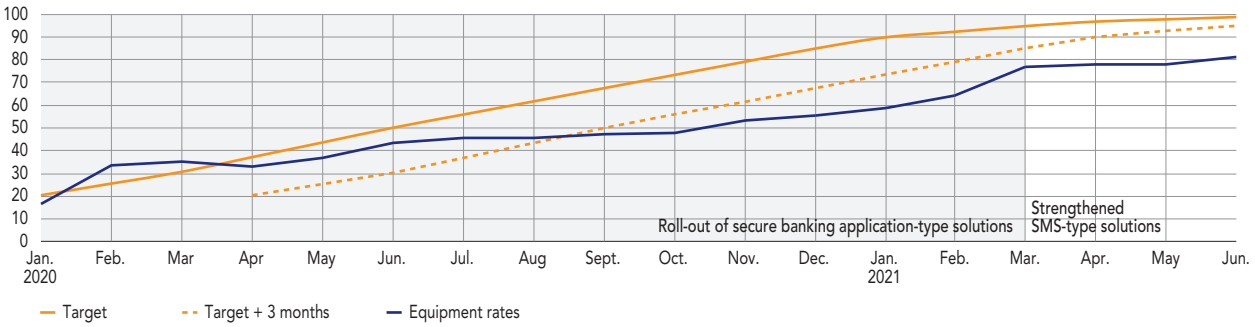
1.3.1 Equipping cardholders

The proportion of cardholders enrolled in a strong authentication system has increased throughout the migration plan. At the end of June 2021, the Observatory estimates that more than 80% 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.

The Observatory notes that, although the deployment of the cardholder equipment plan was delayed by the health crisis, the monitoring actions carried out at the individual level by the Banque de France made it possible to make up for some of the backlog experienced by certain banks in deploying their authentication solution using secure mobile applications in the first quarter of 2021. In the second

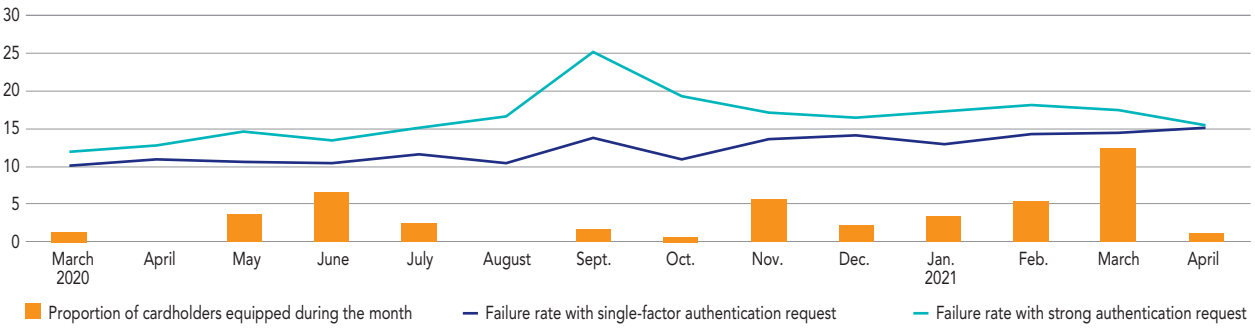
2 See Box 1.

C2 Monitoring the equipment trajectory of cardholders (% of active cardholders registered)



Source: Observatory for the Security of Payment Means.

C3 Failure rate monitoring by authentication mode (in %)



Source: Observatory for the Security of Payment Means.

quarter of 2021, banks began to switch cardholders who were not eligible for the mobile solution to alternative solutions, in particular strengthened SMS. It appears urgent for banks that have not finalised this second wave to do so before the end of the third quarter of 2021.

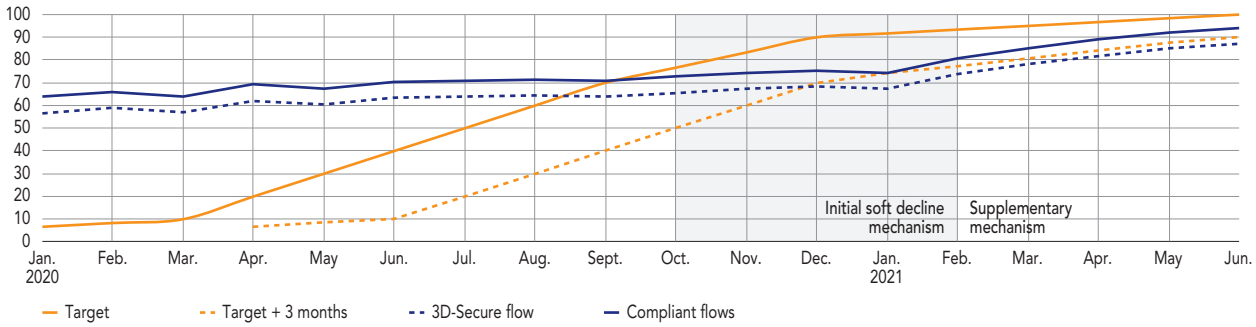
During this phase of equipping cardholders, the Observatory has endeavoured to monitor the pattern of failure rates for the various authentication solutions, which reflects both the level of acceptance by cardholders and the sensitivity of the solutions to the user context. Two findings emerge from these trends:

- On the one hand, the failure rate of strong authentication solutions appears to be structurally higher than that of simple authentication by SMS OTP, which is explained by the predominant use of secure banking applications, a technology that is more demanding in terms of conditions of use (Internet connection quality and stability, application and operating system update status, etc.) than the use of SMS-type technologies;
- On the other hand, the gap between the failure rates of the two solutions, which had reached more than ten points in September 2020, has subsequently been narrowing almost continuously, and now seems to have stabilised at a level of around three points, reflecting the high user take-up of the new authentication solutions.

1.3.2 Equipping merchants

The growth in the use of the 3D-Secure protocol 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 as a result of the ramp-up plan for the soft decline mechanism. As a result, at the end of June 2021, 87% of payment flows eligible for PSD 2 were transiting through the 3D-Secure protocols, thus ensuring their compliance; in addition, non-3D Secure flows of less than EUR 30, which qualify for an a priori exemption, represent approximately 7% of flows. The compliance

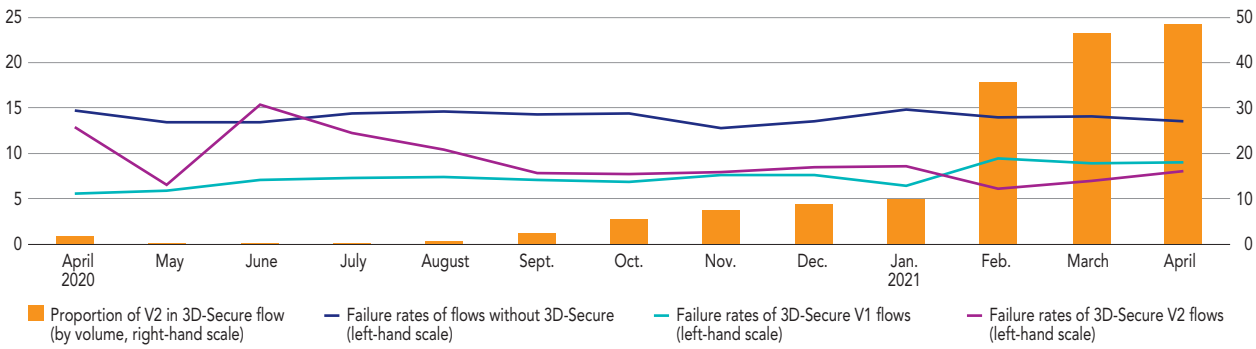
C4 Monitoring of the flow compliance trajectory by merchants (% of value-compliant CIT flows)



Source: Observatory for the Security of Payment Means.

Notes: Compliant flows include 3D-Secure flows and non-3D-Secure flows for small amounts.
CIT – customer-initiated transaction.

C5 Monitoring of failure rates by protocol version (%)



Source: Observatory for the Security of Payment Means.

rate at the end of June thus reached nearly 95% of CIT flows by value.

The Observatory also notes that version 2 of the 3D-Secure protocol has become the preferred protocol (with more than three quarters of 3D-Secure flows in June) and has made it easier for merchants to use exemptions: in May, approximately 60% of transactions were processed using a no-authentication mode validated by the card issuer.

Furthermore, the Observatory notes that a gradual running-in and ramp-up phase for version 2 of the 3D-Secure protocol was necessary in order to enhance its reliability and thus ensure effective control of the transaction failure rate. Since February 2021, the increase in flows on this version has been accompanied by a significant drop in the failure rate, which has become structurally lower than that of version 1. This is a logical development, given that version 2 allows merchants access to transactions that are exempt from strong authentication, with a success rate close to 100%.

1.3.3 Outlook for the period ahead

The Observatory welcomes the commitment of all stakeholders in achieving the success of the migration plan, which has made it possible to attain a high level of compliance with regard to both of its components while ensuring the smooth operation of the e-commerce sector throughout the migration process. In view of these results, the Observatory notes the conclusion of the collective migration plan for the French financial sector, as validated in October 2019. In their capacity as the competent authorities, the Banque de France and the French prudential control and resolution authority will ensure any residual compliance, liaising directly with the institutions concerned on an individual basis.

Looking beyond the fact that the French market has been brought into compliance, the Observatory wishes to stress

the need for proper application of all the rules provided for in PSD 2, and will thus continue to pay particular attention to several points:

- 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;
- Compliance with the transaction qualification rules, in order to prevent the abuse, by certain e-commerce players, of MOTO or MIT-type qualifications, which are exempt from the strong authentication requirement provided for by PSD 2;
- Monitoring the performance level of new 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;
- The gradual extension of PSD 2 requirements to the hospitality, transport and events sectors. Indeed, professionals in these sectors, particularly affected by the health crisis, have been exempted by issuers from performing soft declines. The Observatory will ensure that the use of strong authentication by merchants in these sectors is brought into compliance in a progressive and pragmatic manner, depending on the individual capacity of the players to make the necessary changes.

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.

BOXES

❶ Mechanisms for handling e-commerce payment flows in the event of authentication infrastructure or device failures

A – Common principles to be applied in the event of an incident

The occurrence of an incident affecting the authentication infrastructure and devices, whatever the cause, must immediately trigger implementation of the following measures (even if the mechanisms presented below cannot be activated):

- **suspension of the soft decline message mechanism by issuing institutions:** if the risk level of a given transaction is assessed to be too high, the bank must then proceed with the issuance of a hard decline message;
- **an assessment of the degree of criticality of the incident, in order to report any major incident to the relevant authority** (under PSD 2 for payment service providers – PSPs – and/or under the Eurosystem oversight framework for electronic payment schemes).

B – Mechanisms for handling incidents affecting the "issuer" sector

Where card issuers are concerned, banks' authentication control servers (ACSs) are responsible for processing the 3D-Secure authentication flows from e-merchants, and thus for either strongly authenticating the payer or for authorising the use of an exemption. In the event of an incident affecting the ACSs or another component of the issuing 3D-Secure domain, authentication requests remain unanswered at the issuer level, and are thus put on hold; moreover, in the event of unavailability of the strong authentication solution, the cardholder cannot finalise the transaction.

1. Incident affecting the infrastructures of the issuing domain

In order to ensure that merchants are able to issue transactions in the event of a failure of an ACS or other component of the issuing domain, the Observatory recommends implementation of the following mechanisms:

At scheme level:

- in the event that there is no response from the ACS after a predefined period of time (a timeout strictly defined by the rules governing the scheme), the scheme processing the transaction is asked to replace the ACS by issuing an authentication cryptogram, regardless of the context of the transaction (amount, risk score, transfer of responsibility);
- this issuance must be accompanied by an indicator enabling the issuer to identify that the transaction is covered by the issuer fallback mechanism;
- optionally, as for any other transaction, the scheme can provide value-added information to accompany this re-issue: risk level, eligibility of the transaction for a strong authentication exemption, etc.

At the level of the issuing banks' authorisation servers (IAS):

- assessment of the risk level of the issuer fallback transaction and validation of the transaction, if necessary, even if it does not qualify for an exemption; this assessment should take into account any future implications of the transaction (in the event of the initiation of a series of recurring transactions or a merchant-initiated transaction mandate,[1] for example);
- transactions resulting from the issuer fallback mechanism must not give rise to any soft decline: if the level of risk is deemed too high, the bank must issue a hard decline message;
- authorised transactions which are not exempted from strong authentication must be reported as unauthenticated, with the reason shown as "Other", in the semi-annual mapping of payment flows;
- the liability transfer conditions remain unchanged according to the scheme rules.

1 Transactions initiated electronically by the merchant.

Issuing institutions are required to:

(i) verify the proper use of this mechanism by schemes to ensure that it is not implemented outside the periods of unavailability of their ACS,

(ii) accept requests for authorisation in a risk-proportionate manner,

(iii) assess the level of criticality of the incident with regard to the criteria established by the European Banking Authority (EBA/GL/2017/10) and, if necessary, report it as a major operational or security incident to the Banque de France and the *Autorité de contrôle prudentiel et de résolution* (ACPR).[2]

Schemes monitor issuer response rates on transactions which are covered by the issuer fallback mechanism.

2. Incident affecting the issuer's strong authentication solution

In order to ensure that merchants are able to issue transactions in the event of a failure of an ACS or another component of the issuer domain, the Observatory recommends that the following mechanisms be put in place:

At the level of the issuing banks' authorisation servers (IAS):

- activation of a back-up authentication facility, potentially involving simple authentication (such as SMS OTP) in the event of the unavailability of an alternative strong authentication solution;
- transactions that have not been strongly authenticated should be reported as unauthenticated, with the reason shown as "Other", in the semi-annual mapping of payment flows;
- from the perspective of the applicable liability rules, the transaction should be considered as strongly authenticated from the schemes' standpoint.

Issuing institutions are required to monitor the proper use of this mechanism to ensure that (i) it is implemented in an expeditious manner in the event of an identified incident, and (ii) it is not used outside of the periods of unavailability of strong authentication solutions.

The nature of the incident on the issuer's strong authentication solutions may also need to be reported to the Banque de France and the ACPR as a major incident.

C – Mechanisms for handling incidents affecting the "acceptor" domain

For the schemes, the directory servers (DS) are responsible for routing the 3D-Secure payment flows from the e-merchants to the ACSs of the issuing banks. In the event of an incident affecting the DS or the access gateway, 3D-Secure payments cannot be made.

In order to ensure that merchants are able to issue transactions in the event of a failure of a directory server or their access gateway, the Observatory recommends that the following mechanisms be put in place:

At the scheme level:

- setting up an indicator to identify authorisation requests covered by the acceptor fallback mechanism.

At the merchant level:

- subject to feasibility with regard to the IFR – interchange fee regulation (in particular where there is no active brand selection by the consumer), switch to the second scheme if the card is co-badged;
- if unable to issue a transaction via 3D Secure, issue the transaction directly as an authorisation, identifying it as falling under the acceptor fallback mechanism.

At the level of the issuing banks' authorisation servers (IAS):

- assessment of the risk level of the fallback acceptor transaction and validation of the transaction, where appropriate, even if it does not qualify for an exemption; this assessment should take into account any future implications of the transaction (e.g. in the event of the initiation of a series of recurring transactions or an MIT mandate);

2 Major operational and security incidents of payment service providers must be notified under Article L. 521-10 of the French Monetary and Financial Code, thus complying with the criteria of the European Banking Authority's guidelines (EBA/GL/2017/10). Notifications are to be transmitted via a dedicated secure interface, in accordance with the relevant European Banking Authority guidance. PSPs are asked to email any request for documentation to the following address: *2323-NOTIFICATIONS-UT@banque-france.fr*

- transactions resulting from the acceptor fallback mechanism must not give rise to any soft decline: if the level of risk is deemed too high, the bank must issue a hard decline message;
- authorised transactions which are not exempted from strong authentication must be reported as unauthenticated, with the reason shown as "Other", in the semi-annual mapping of payment flows.

Acquiring institutions are required to verify that their merchants are using this mechanism correctly, to ensure that it is not implemented outside the unavailability periods of the directory servers or their access gateways.

Issuing institutions, for their part, are required to accept requests for authorisation in a risk-proportionate manner.

Finally, the schemes are required to put in place arrangements to monitor the utilisation rate of this facility on the acquirer side and the response rates of issuers. They are also required to notify the Eurosystem, if appropriate via the Banque de France as lead overseer, of major incidents affecting their infrastructures under the "Major incident reporting framework for payment schemes and retail payment systems" (2018).

2

FRAUD IN 2020

2.1 Overview

2.1.1 Means of payment

Against the backdrop of the Covid-19 crisis, payment activity generally held up well due to the exceptional financial flows it generated. Individuals, firms and public administrations carried out some 25.3 billion cashless payment transactions in 2020 (compared to 26 billion in 2019, i.e. -4%) for a total amount of EUR 35,902 billion (compared to EUR 28,658 billion in 2019, i.e. +25%).

In terms of payment structures, the dematerialisation of payments observed over the past several years further progressed in 2020, driven by the effects of the health crisis. Indeed, electronic payments grew in popularity among economic players: a portion of face-to-face payments was replaced by remote payments due to the lockdown and restrictions on movement, while health concerns prompted merchants to favour dematerialised or contactless payment methods for the remaining face-to-face transactions. As such:

- **Cards** remained the most widely used means of payment in France, accounting for more than half of all cashless transactions by volume (55% in 2020, unchanged from 2019) for a total amount of EUR 578 billion in 2020. However, use of payment cards declined slightly in 2020 (-4.3% in volume compared to 2019) due to the decrease in face-to-face payments (-8.7% for the number of transactions via this channel compared to 2019) associated with travel restrictions and shop closures. Face-to-face transactions still accounted for a significant share (nearly two-thirds) of card-based payments. Among these face-to-face payments, there was a marked increase in the share of contactless payment transactions, which rose from 9% in 2019 to 19% in 2020. In 2020, contactless payments accounted for 5.1 billion transactions (+37% compared to 2019) for a total amount of EUR 79.7 billion (+86% compared to 2019). Online card payments benefited from the effects of the crisis, with online transactions increasing by 13.2% in volume and 8.3% in value. In contrast, card withdrawals suffered from the health crisis, with just under 1.1 billion transactions in 2020 (i.e. -4.3% compared to 2019), for a value of just under EUR 116 billion (i.e. -3.4% compared to 2019). This is partly due to the preference for electronic means of payment over cash for in-store transactions.
- **Credit transfers** were not adversely affected by the health crisis. Indeed, the number of such transactions increased by 5% year-on-year, coming to 4.5 billion transactions in 2020, for a significantly higher total amount of EUR 32,712 billion (i.e. +30% compared to 2019). This sharp increase is mainly due to atypical financial transactions carried out by in particular by public authorities to cover the surge of expenditures incurred by the central government in the context of the health crisis. This trend can be explained by large-value transfers (LVTs), exchanged via dedicated payment infrastructures. Such transactions increased by 64.8% in value terms year-on-year, while traditional SEPA[1] transfers, which are used more by firms and individuals, decreased by 15.4% in value. Instant credit transfers, meanwhile, remained far behind other types of transfers and accounted for a minority of flows (1% in volume and 0.08% in value). However, the ramp-up of this means of payment accelerated in 2020, with volumes increasing more than threefold, to 45.5 million transactions, and total value growing almost fourfold to EUR 26.6 billion. The average amount of an instant transfer in 2020 was EUR 585. Credit transfers continued to be favoured for large-value settlements (salary and pension payments, business-to-business payments, etc.). They accounted for 91% of the total value of cashless payments and stood out as the third most used means of payment in France (17.7%) in terms of transaction volume, just after cards and direct debits.
- **Direct debits** remained the second most widely used non-cash payment instrument in terms of transaction volume. They accounted for 18.3% of transactions and represented 5% of the total value of cashless transactions in 2020, i.e. an increase of some 6% in volume year-on-year and a slight decrease of 1.6% in value terms.

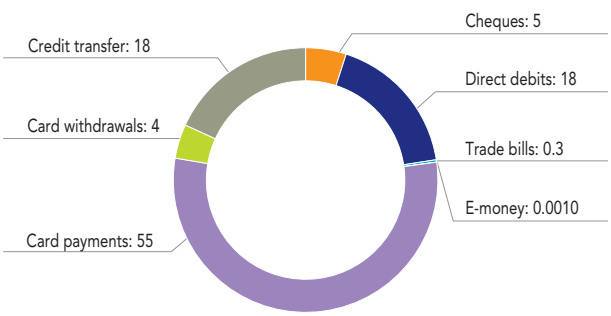
1 Single Euro Payments Area. SEPA covers the 27 European Union Member States, as well as Monaco, Switzerland, Liechtenstein, Norway, Iceland, the United Kingdom and San Marino.

Direct debits, which are used mainly for recurring payments, proved extremely flexible during the crisis, allowing for deferrals, reductions and even suspensions of payment deadlines.

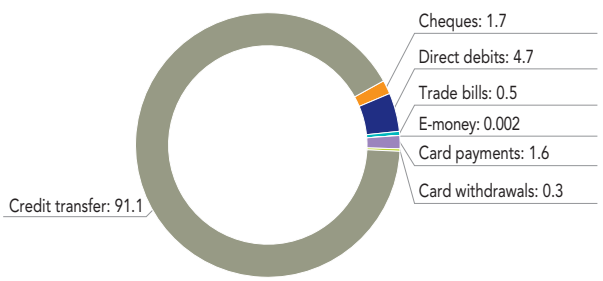
- The continued decline in the use of **cheques**, observed since the 2000s, was reinforced in 2020, in terms of both the number and value of transactions (-25.9% in volume and -24.6% in value terms), with just under 1.2 billion cheques issued, for a total amount of EUR 614 billion. While cheques still rank as the third most widely used means of payment in terms of transaction value (accounting for 1.7% in 2020), cards, with 1.6% of transaction value in 2020, are quickly catching up.
- **Trade bills** (bills of exchange and promissory notes) were used in less than 1% of cashless transactions both in terms of volume (0.3%) and value (0.6%), and thus continued to decline (-8% in volume and -15% in value compared to 2019).
- Lastly, **electronic money** continued to account for a marginal share of cashless transactions (less than 1% in terms of both volume and value). Nevertheless, this means of payment recorded an increase in total outstanding amount, which came to EUR 688 million (+22.6% compared to 2019).

C1 Use of cashless payment means in France in 2020 (%)

a) In volume terms

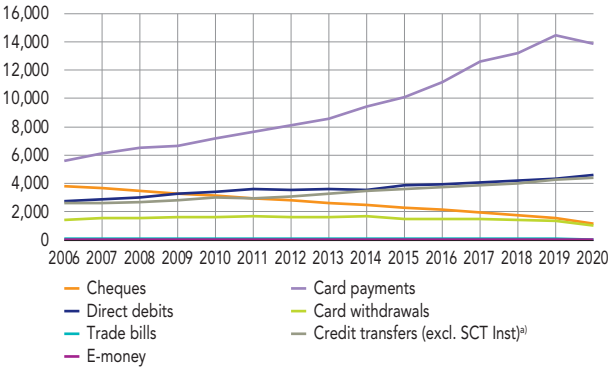


b) In value terms



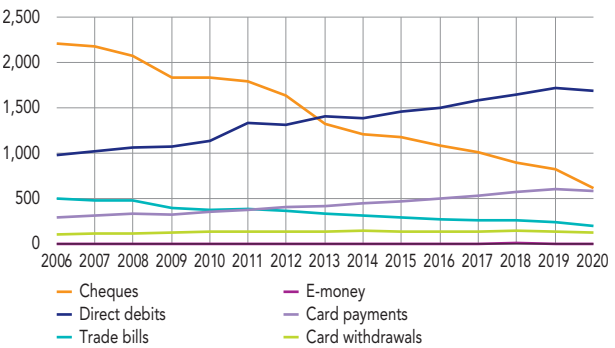
Source: Observatory for the Security of Payment Means.

C2 Use of cashless payment means in France since 2006
(in millions of transactions)



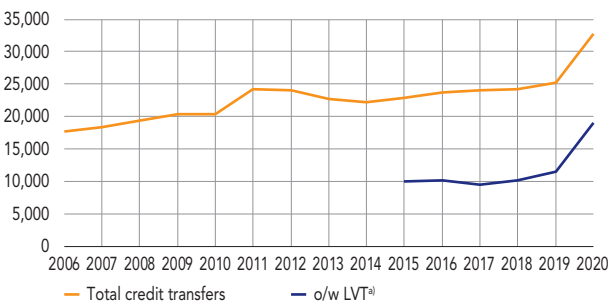
Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.
a) SCT Inst: SEPA instant credit transfer.

C3 Value of transactions in France since 2006, excluding credit transfers
(EUR billions)



Source: Observatory for the Security of Payment Means.

C4 Value of credit transfers in France since 2006 (EUR billions)



Source: Observatory for the Security of Payment Means.
a) LVT: large-value transfers, issued via large-value payment systems (Target 2, Euro 1); professional payments only.

2.1.2 Impacts of the Covid-19 crisis on means of payment

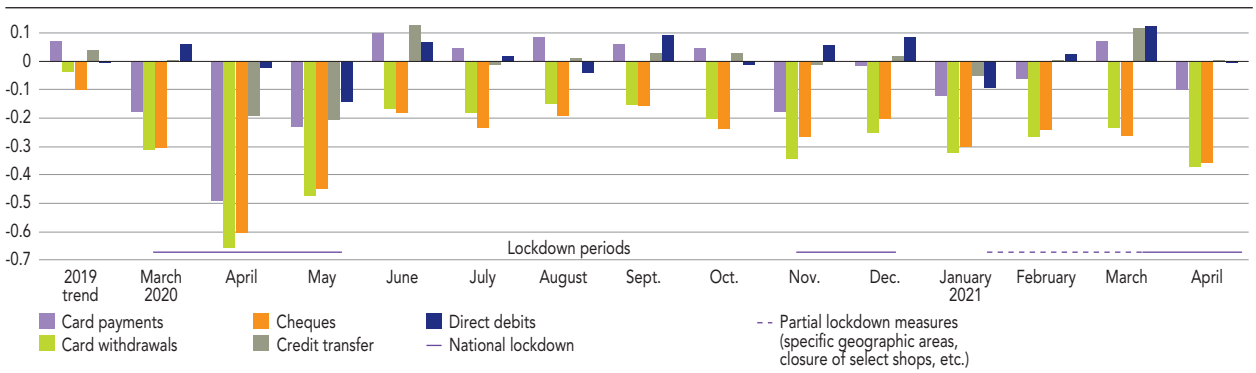
Going beyond these overall trends, the Observatory notes that the measures adopted by the French government in response to the health crisis have had varying effects depending on the means of payment and periods in question.

- The lockdown from mid March to mid May 2020 had a very strong impact on the flows of all means of payment, with a decline of more than 50% for cards and cheques, against a backdrop of sharp reduction in retail activity. SEPA payment flows (credit transfers and direct debits), which are indicative of the business and government activity, exhibited a much smaller decline of less than 20%.
- The summer season following the relaxing of lockdown measures saw a return to the historical growth rate for payment flows, with the exception of cheques and cash withdrawals, which subsequently experienced a much larger decline than in the past.
- The other two lockdown periods (from mid November to mid December 2020, and later in April 2021) had a much more limited impact on payment flows.

Trends in card payment flows during these periods point to a change in consumers' purchasing and payment habits.

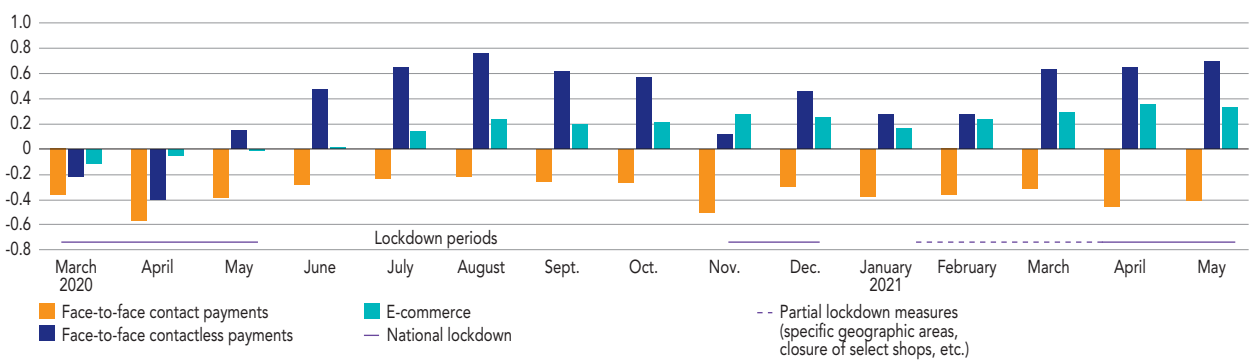
- Online payments were much less affected by the lockdown measures, growing almost continuously throughout the health crisis, particularly following the introduction of online facilities by local retailers, such as delivery and "click and collect" services. Online payments increased by more than 20% in volume compared to pre crisis levels.
- Contactless payments benefited from both the increase of the payment limit from EUR 30 to EUR 50 on 11 May 2021, and from a more pronounced aversion among consumers regarding physical contact payments (cash, cheque, card with code entry), becoming the preferred means of face-to-face payment. As a result, contactless payments experienced spectacular growth upon the lifting of lockdown measures in May 2020, with transactions increasing by more than 50% in volume and doubling in value during summer 2020. However, this means of payment was also affected by the health measures targeting local retailers (particularly the two subsequent lockdowns, as well as the closure of shopping centres from February to May 2021).

C5 Change in payment flows in volume terms compared to the pre-crisis reference period (March 2019 – February 2020) (%)



Source: Observatory for the Security of Payment Means.
Note: The "2019 trend" corresponds to annual growth in payment flows between 2018 and 2019.

C6 Change in card payment flows in volume terms compared to the pre-crisis reference period (March 2019 – February 2020) (%)



Source: Observatory for the Security of Payment Means.

- In contrast to these developments, card payments with PIN code entry dropped sharply since the beginning of the crisis, with a lasting decline of more than 20% in terms of volume, including outside the lockdown periods.

2.1.3 Fraud targeting means of payment

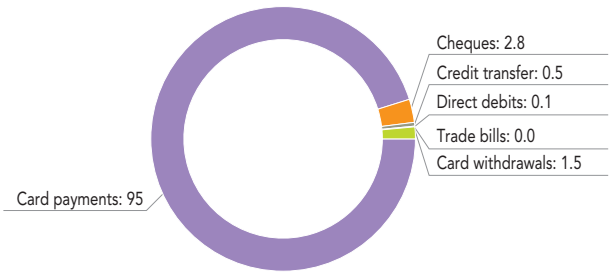
In 2020, nearly 7.8 million fraudulent cashless transactions were perpetrated for a total fraud amount of EUR 1.28 billion. This represented an increase of 8.4% in value and 4.2% in volume year-on-year. This rise in the value of total fraud was driven mainly by credit transfers and, to a lesser extent, card payments. However, fraud rates for most means of payment remained under control overall, with the exception of cheque fraud, which rose significantly. As such:

- **Cheques** remained the most widely used means of payment for fraudulent purposes in France for the third consecutive year, in terms of both volume and rate of fraud. Indeed, while fraud amounts were nearly stable at EUR 538 million, compared to EUR 539 million in 2019, the rate of cheque fraud as a proportion of total fraud concerning cashless means of payment remained the highest at 42% (compared with 46% in 2019), due in particular to high average fraudulent cheque transaction amounts, which stood at EUR 2,438. With the continued decline in cheque use in 2020 (-24.6% in value) and the increase in the use of lost or stolen cheques (+23.4% in value terms, accounting for 68% of cheque fraud), as well as that of fraud concerning valid cheques (+81% in value terms, representing EUR 37 million), the fraud rate rose significantly to 0.088% (compared to 0.066% in 2019), and thus remains higher than that of payment card fraud (0.068%).
- Taking payment and withdrawal transactions together, **payment card** fraud values remained nearly stable year-on-year (EUR 473 million, compared to EUR 470 million in 2019, i.e. +0.6%), but still accounted for an overwhelming majority (97%) of fraudulent transactions in terms of volume. With an average fraudulent transaction value of EUR 63, cards accounted for only 37% of overall fraud in value terms (34% for payments and 3% for withdrawals). The fraud rate on card transactions remained under control at 0.068% (compared to 0.064% in 2019), i.e. one euro of fraud for every EUR 1,470 paid, despite the massive shift in payment flows towards practices that are more susceptible to fraud, such as contactless payments (+86% of flows in value terms compared to 2019) and remote payments (+8.3% of flows in value terms compared to 2019), in relation to face-to-face card payments with PIN code entry (-17% of flows in value terms compared to 2019). However, this average rate covers contrasting situations, with very little fraud in point-of-sale payments (0.009%, i.e. one euro of fraud for every EUR 11,100 paid), along with a higher, albeit nearly stable, rate of fraud in remote payments (0.174%, i.e. one euro of fraud for every EUR 575 paid, compared to 0.170% in 2019). As in the past, a considerable majority – more than two thirds – of payment card fraud concerned online payments, even though such payments accounted for only 22% of transactions. With the growth of e commerce, this observation highlights the need to generalise the strong authentication measures provided for in PSD 2.
- **Credit transfer** fraud once again increased in 2020 (+65% in value terms compared to 2019), with an increase in annual fraud amounts from EUR 162 million to EUR 267 million, currently accounting for 21% of the total amount of fraud involving cashless means of payment. This increase was mainly due to social engineering fraud, which increased significantly in 2020 (+EUR 101 million year-on-year). The successive lockdowns and extensive use of teleworking undermined the structure and reference points of corporate financial and accounting departments. Fraudsters took advantage of the situation to request emergency transfers or to submit new bogus bank account details, ostensibly on behalf of suppliers. This also affected government transfers, with fraudsters posing as firms in order to obtain exceptional financial aid from public authorities, such as that linked to state-paid furlough schemes. However, despite this increase in the value of total fraud, the fraud rate on credit transfers, although rising significantly, remained low at 0.0008% (compared to 0.0006% in 2019). This represents one euro of fraud for every EUR 125,000 paid, due to the strong momentum of credit transfer flows (+30% in value terms compared to 2019 and a 91% value-based share of cashless transactions). Taking into consideration the different types of transfers, a significantly higher fraud rate continued to be observed for instant transfers (0.0397%, up slightly year-on-year. However, although instant transfers continue to take place under generally adequate security conditions, their widespread use calls for greater attention from users and professionals (*see Chapter 3, "Technology watch on real-time payment security"*), particularly when the beneficiary requests that the funds be sent to an account held abroad.
- **Direct debit** fraud continued to decrease, with fraud amounts dropping from EUR 11 million to EUR 2 million in 2020 (-82% in value terms compared to 2019). This means of payment thus exhibited the lowest annual amount of fraud among all cashless means of payment available to private individuals. The associated fraud rate was extremely low: 0.0001%.

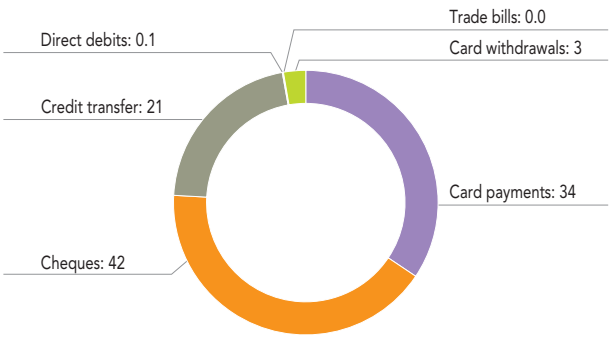
- Finally, **trade bills** remained relatively untouched by fraud, with an amount of approximately EUR 539,000 in 2020 and a fraud rate of 0.0003%, i.e. one euro of fraud for every EUR 365,500 paid.

C7 Breakdown of fraud on cashless payment means in 2020 (%)

a) In volume terms

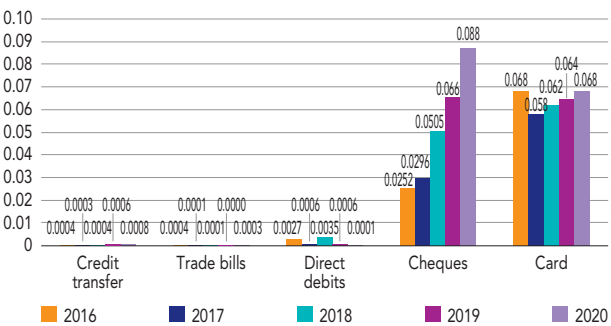


b) In value terms



Source: Observatory for the Security of Payment Means.

C8 Change in fraud rate for each payment means from 2016 to 2020 (%)



Source: Observatory for the Security of Payment Means.

2.2 Card payment and withdrawal fraud

2.2.1 Overview

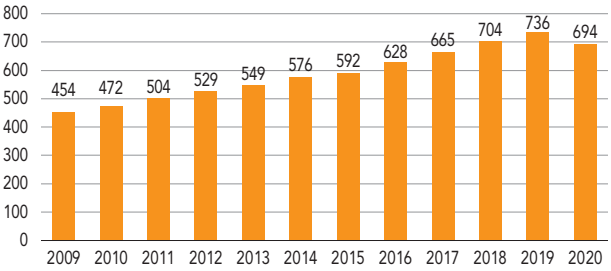
Many contributors enrich card payment statistics, providing useful insights into card payment fraud (*see Box 2 below*).

Fraud on payment and withdrawal transactions carried out in France and abroad with French cards increased very slightly in 2020 (+0.6% in value compared with 2019), representing EUR 473 million out of a total transaction value of EUR 694 billion, i.e. a decrease of 5.7% compared to 2019. The fraud rate on French payment cards increased very slightly, coming to 0.068%, compared with 0.064% in 2019, equivalent to one euro of fraud for every EUR 1,470 of transactions.

Card fraud in France, including transactions carried out with both French and foreign cards, came to EUR 525 million in 2020. This represents a 5.6% decline compared to 2019, for a total transaction value of EUR 725 billion, down 8.1%. Based on these data, the overall rate of fraud on payment card transactions processed in French electronic payment systems was stable at 0.072%, equivalent to one euro of fraud for every EUR 1,390 paid.

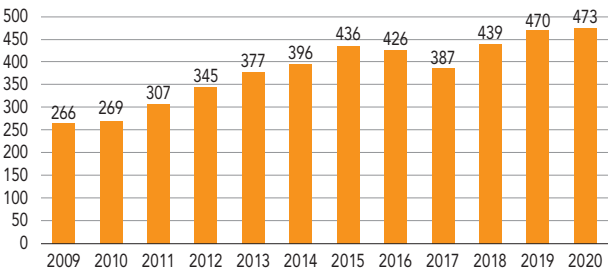
The number of French cards for which at least one fraudulent transaction was recorded during 2020 was 1.4 million, up 2.2% compared to 2019. However, this increase was not accompanied by a rise in the unit amount of fraudulent transactions, which decreased to EUR 63 from EUR 65 in 2019. This situation is due to a strengthening of measures to secure card payments (stronger authentication of online payments, risk analysis and transaction scoring systems, SMS alerts to cardholders, etc.). These measures make it possible to detect and deactivate compromised cards more quickly. Fraudsters are therefore forced to multiply fraud attempts, while reducing unit amounts in an attempt to evade fraudulent transaction detection mechanisms.

C9 Total transaction value, French cards
(EUR billions)



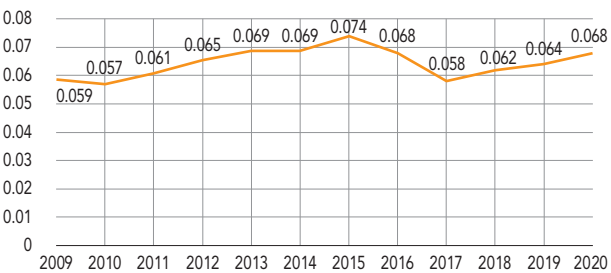
Source: Observatory for the Security of Payment Means.

C10 Total fraud value, French cards
(EUR millions)



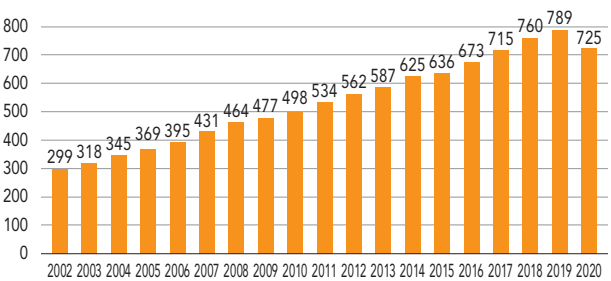
Source: Observatory for the Security of Payment Means.

C11 Fraud rate, French cards (%)



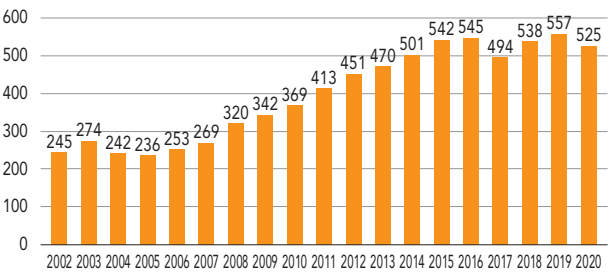
Source: Observatory for the Security of Payment Means.

C12 Total transaction values processed in French payment systems, French and foreign cards (EUR billions)



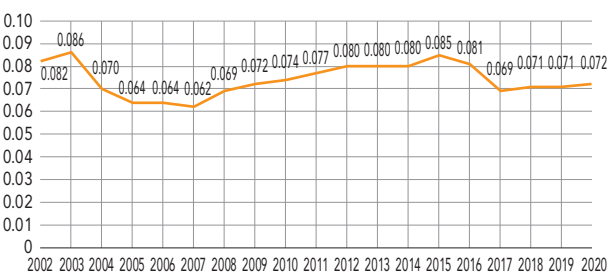
Source: Observatory for the Security of Payment Means.

C13 Fraud value on transactions processed in French payment systems, French and foreign cards (EUR millions)



Source: Observatory for the Security of Payment Means.

C14 Fraud rate for transactions processed in French payment systems, French and foreign cards (%)



Source: Observatory for the Security of Payment Means.

2.2.2 Geographical breakdown of fraud

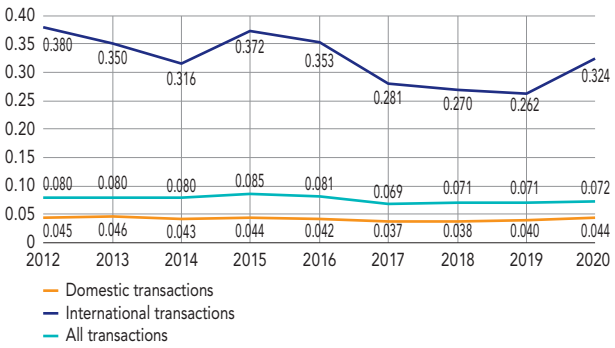
The amount of fraud on payment and withdrawal transactions carried out in France with French cards, i.e. domestic transactions, rose by 7.4% in 2020, to EUR 290.7 million, compared to EUR 270.7 million in 2019. Against a backdrop of falling flows of domestic transactions (-3.8% in value terms compared to 2019), the fraud rate on domestic transactions grew very slightly, while remaining relatively low at 0.044% (compared to 0.040% in 2019), equivalent to one euro of fraud for approximately EUR 2,270 of transactions.

With the sharp decline in international flows linked to the deferment of overseas travel (-34% in value terms compared to 2019), fraud amounts with regard to international transactions[2] naturally declined, albeit to a lesser extent (-18.2% in value terms compared to 2019). The fraud rate on international transactions thus rose to 0.327% (from 0.262% in 2019), i.e. seven times higher than that of domestic transactions. International transactions remain more vulnerable to fraud, accounting for a mere 10% of the total value of card transactions, but 45% of total fraud in value terms.

According to geographical areas, the following can be observed:

- for French cardholders, a significant increase in fraud rates both for transactions carried out in SEPA countries[3] (0.429% in 2020, compared to 0.333% in 2019) and for those carried out outside the European SEPA area (0.533% in 2020, compared to 0.441% in 2019);
- for French merchants, an increase in the fraud rate on approved transactions carried out with cards issued in SEPA countries (0.099% in 2020, compared to 0.080% in 2019). Conversely, the fraud rate on card transactions issued outside the SEPA area, while remaining particularly high, decreased to 0.290% from 0.311% a year earlier.

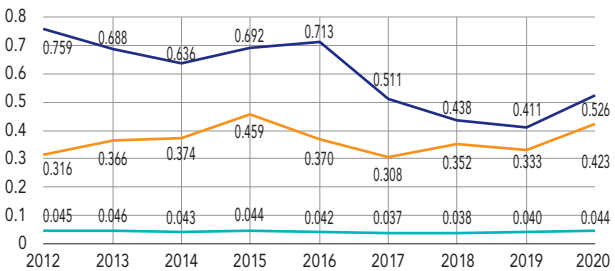
C15 Fraud rate by geographical area (%)



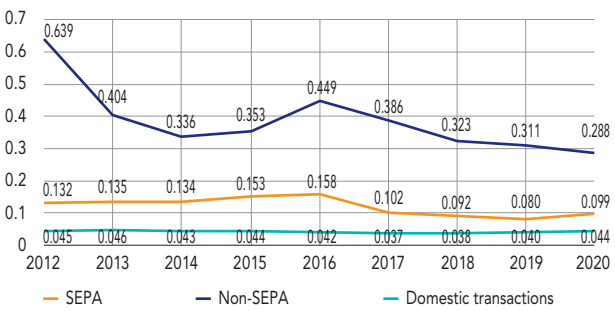
Source: Observatory for the Security of Payment Means.

C16 Fraud rate by geographical area (%)

a) French cardholders



b) French merchants



Source: Observatory for the Security of Payment Means.
Note : SEPA – Single Euro Payments Area.

2.2.3 Breakdown of fraud by transaction type

Fraud on domestic transactions

Although the total amount of fraud on domestic transactions increased in 2020 (+7.4% in value terms compared to 2019), fraud rates across all initiation channels remained stable overall.

Indeed, the following can be observed according to various transactions types:

- For face-to-face and unattended payment terminal (UPT) payments, a significant drop in the fraud amounts (-17.8% compared to 2019) linked to the decline in transaction flows (-5.4% in value compared to 2019), but also due to the very sharp drop in the use of lost or stolen cards (-19.5% in value terms for this type of fraud compared to 2019) arising from closure of points of sale during lockdown periods. At the same time, contactless payments increased significantly in 2020 (+37.7% in volume and +88.6% in value) and the corresponding fraud rate was higher than for transactions involving PIN code entry. In the end, the fraud rate on face-to-face payments was down very slightly to 0.009% (compared to 0.010% in 2019), making for extremely low levels of fraud.
- For remote payments, an increase in fraud (+16.4% in value terms compared to 2019). This can be explained both by the growth in e commerce flows (+13.5% in value terms compared to 2019) brought about by the health context, which modified consumer purchasing habits and encouraged merchants to develop online sales channels; and by a shift in fraud attempts to target these channels – more popular with consumers – via an increase in phishing[4] attacks. However, the fraud rate for remote

2 International transactions include payment and withdrawal transactions carried out abroad using French cards, as well as payment and withdrawal transactions carried out in France using foreign cards.

3 Single Euro Payments Area. SEPA covers the 27 European Union Member States, as well as Monaco, Switzerland, Liechtenstein, Norway, Iceland, the United Kingdom and San Marino.

4 Phishing generally involves sending emails that misuse visual identities and logos (e.g. those of a credit institution) that are recognisable to the receiver, inviting their victims to connect to a fraudulent website in order to collect card data.

payments remained under control at 0.174%, compared with 0.170% in 2019, thanks to security measures implemented by payment issuers, merchants and firms, which introduced cardholder authentication systems, as well as risk analysis and transaction scoring tools. This rate nevertheless remains excessive, standing 19 times higher than that of face to-face and UPT payment fraud. It is expected to improve thanks to the generalisation of strong authentication measures for online payments provided for by the second European directive on payment services (PSD 2), full implementation of which was delayed in 2020 due to the Covid-19 crisis (*see Chapter 1*). Fraud on remote payments remained largely concentrated in the "General and semi general trade" and "Personal and professional services" sectors (*see Box 3*).

- For Automated Teller Machine (ATM) withdrawals, a drop in fraud amounts (-9.4% in value terms compared to 2019) consistent with the decline in activity (-13.7% in value compared to 2019) insofar as both consumers and merchants tended to favour electronic payments over cash during the health crisis. The fraud rate remained nearly stable at 0.029%, compared to 0.028% a year earlier.

Fraud targeting international transactions

Although fraud on international transactions decreased overall in 2020, trends varied depending on the payment channel and geographical area. As a rule of thumb, fraud continued to be better contained for transactions carried out within SEPA than for those carried out with non SEPA countries. This is a result of the efforts made in Europe over the past several years to migrate all cards and payment terminals to the EMV (Europay, Mastercard and VISA)[5] standard and to generalise strong authentication mechanisms.[6]

- With regard to French cards, fraudulent activities in 2020 continued to focus largely on remote payments, which accounted for 94% of total fraud within SEPA (EUR 129.1 million and a fraud rate of 0.582%), and 90% of total fraud outside SEPA (EUR 40.5 million with a fraud rate of 0.921% in 2020). At the same time, face-to-face payments remained highly susceptible to fraud in some countries, where payment and withdrawal terminals continue to read the magnetic strips on cards, which are vulnerable to counterfeiting.
- With regard to foreign cards, fraud levels remained much higher for remote transactions, with rates of 0.207% for cards issued within SEPA and 0.711% for those issued outside the area. For the latter, French payment acquirers cannot always demand strong cardholder authentication, as PSD 2 is not applicable to cards issued outside the European Union.

Fraud on contactless payments

Against the backdrop of the Covid-19 crisis, consumers and merchants have shown a marked preference for contactless card payments as a factor of social distancing. As such, they once again rose sharply by 38% in volume and 89% in value terms at the national level compared to 2019. This growth in contactless payments was also encouraged by the rise of the payment limit EUR 30 to EUR 50, implemented on 11 May 2020 at the end of the first lockdown.

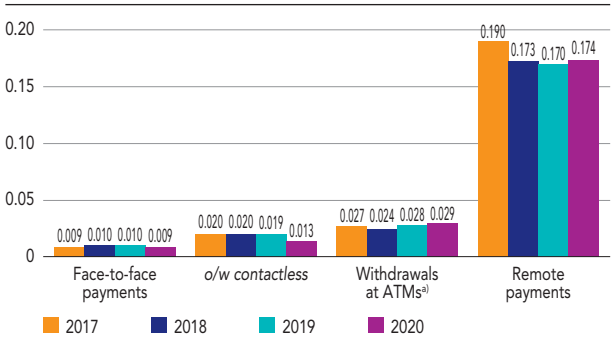
Nearly 5.1 billion contactless payments were carried out in 2020 (compared to 3.7 billion in 2019) for a total amount of EUR 78.4 billion (compared to EUR 41.6 billion in 2019). As such, almost half of face-to-face card payments (46% to be precise) were contactless, accounting for 19% of such payments in value terms. Subsequent to the rise in the payment limit to EUR 50, the average amount of a contactless payment was EUR 15.4, up from EUR 11.3 in 2019.

Taking domestic contactless payments together with those made in France using foreign cards and those made with French cards abroad (i.e. international payments), 5.3 billion transactions were carried out for a total amount of EUR 81.1 billion, reflecting an increase of 35% in volume and 83% in value year on year.

Despite the growth in contactless payments and the rise in the ceiling, the fraud rate on domestic contactless transactions did not increase, instead falling very slightly to 0.013% (compared to 0.019% in 2019), with a total amount of fraud of just under EUR 10.5 million. The fraud rate for contactless payments remains at an intermediate level between those associated with face-to-face payments (0.009%) and cash withdrawals (0.029%), and well below that for remote payments (0.174%). Considering fraud on domestic payments together with that on international transactions, the fraud rate once again improved, coming to 0.016% (compared to 0.020% in 2019), reflecting a total of EUR 13 million in value terms. However, this 2020 decrease masks an increase in the rate of fraud for contactless payments made with non SEPA countries, both for French cardholders and French merchants. In this respect, the Observatory recommends that French cardholders **deactivate their cards' contactless function when travelling outside the SEPA area** for optimum security, as the conventional payment limits are not always respected.

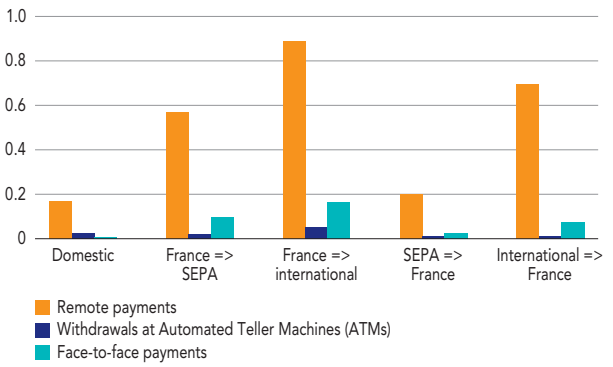
In 2019, as in previous years, the vast majority of contactless payment fraud could be traced back to the loss or theft of a card and did not involve advanced card data capture technologies. Insofar as card issuers set limits on the unit amount of a single transaction (EUR 50) and on the

C17 Comparison of fraud rates for domestic transactions by transaction type (%)



Source: Observatory for the Security of Payment Means.
a) ATMs – Automated Teller Machines.

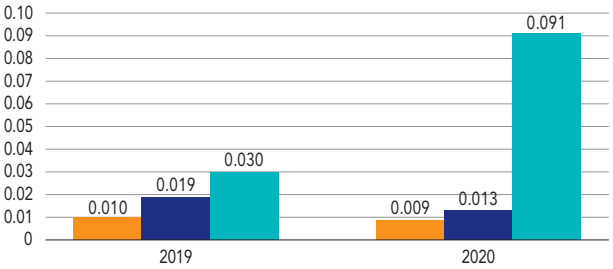
C18 Fraud rate by transaction type and geographical origin (%)



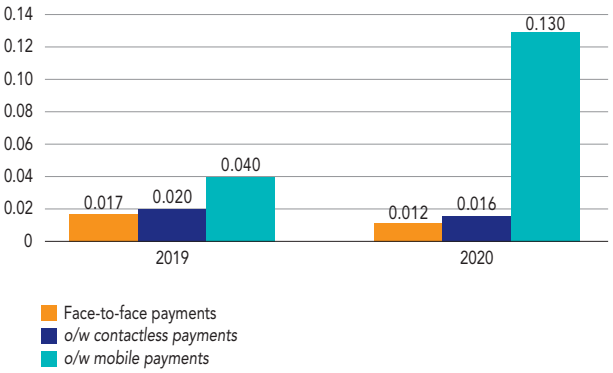
Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

C19 Fraud rate for face-to-face payments (%)

a) Domestic transactions



b) Domestic and international transactions



Source: Observatory for the Security of Payment Means.

number of consecutive transactions that can be carried out without entering the PIN code (maximum of EUR 250), the harm suffered by consumers in the event of loss or theft of a card is limited. It should also be noted that cardholders enjoy legal protection in the event of fraud and must be reimbursed for any fraud suffered as a result of illicit contactless purchases (*see Appendix 2*). As regards international transactions in contactless mode, the origin of fraud is different, resulting mainly from the use of counterfeit cards (40% of fraud amounts), followed by loss or theft of cards (29% of fraud amounts).

As regards mobile payments, the data for which are included in contactless payment data, this practice appears to have been fuelled by the Covid-19 pandemic, with a 135% increase in domestic transactions in terms of volume (126.9 million transactions) and a 179% increase in value terms for a total payment amount of just over EUR 2.7 billion. However, this payment method still represents a very marginal share of contactless card payment flows taken as a whole (2.5% in volume and 3.4% in value terms). The average amount of domestic mobile payments stood at EUR 21.2 in 2020, compared to EUR 17.8 in 2019. Considering payments carried out in France using foreign devices and those carried out abroad using French devices, the total number of transactions came to 147.7 million, representing just over EUR 3 billion,

5 EMV is an international technical security standard for smart payment cards, whose specifications were developed by the EMVCo consortium of American Express, JCB Cards, MasterCard and Visa. The EMV standard for face-to-face payments and withdrawals notably provides for the use of a combination of a secure card chip and a secret code, commonly referred to as "Chip and PIN".

6 Strong authentication devices are based on verification of the customer's identity via two of the three following factors: (i) a knowledge factor (password, PIN code), (ii) a possession factor (telephone, cards), and (iii) an inherence factor (fingerprint, iris or voice recognition).

i.e. an increase of 118% in volume and 144% in value terms year-on-year.

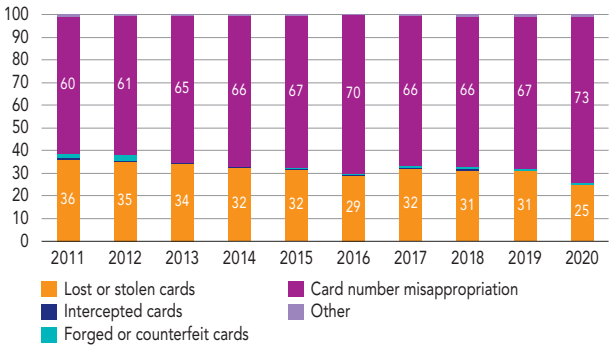
While in 2019, fraud on mobile payments was negligible, it increased sharply in 2020, commensurate with the rise in the use of this technology. Fraud concerning domestic mobile transactions thus increased sevenfold in both volume (29,807 in 2020, compared to 4,159 in 2019) and value (EUR 2.4 million in 2020, compared to just over EUR 330,000 in 2019). As a result, the fraud rate on domestic mobile transactions came to 0.091% in 2020 (compared to 0.03% in 2019). Mobile payment fraud, all geographical areas combined, increased significantly with a fraud rate of 0.13% (compared to 0.04% in 2019). As with contactless payments, transactions carried out with non-SEPA countries are particularly vulnerable to fraud. **It should be noted that, unlike contactless payments, mobile payments are not capped, the only limit being that of the payment card. As a result, those affected are liable to suffer greater harm.** Mobile payment fraud is mainly linked to lost or stolen cards registered in a mobile payment application. The Observatory therefore reiterates its recommendations to economic players – banks, card payment systems and technology solution providers – to implement strong authentication measures, both to secure user registration in mobile payment applications and to authenticate cardholders for subsequent transactions.

2.2.4 Breakdown of fraud by type

The origin of fraud on domestic payment card transactions, which is by far the most common type of fraud, remains linked to the theft of card numbers, thereby making it possible to carry out fraudulent payments remotely (73.1% of fraud amounts in 2020, compared to 66.9% in 2019). The same is true for international transactions: this type of fraud alone accounts for 90% of the fraud amounts for transactions carried out within SEPA area and 81% outside the area. In 2020, this type of fraud was based on phishing and malware attacks, which increased significantly during the crisis, particularly by taking advantage of the Covid-19 pandemic to capitalise on rampant fear and confusion among consumers. To circumvent payer authentication devices, some forms of email or SMS phishing successfully lure cardholders into providing both their card details and their authentication codes received via SMS. In some cases, fraudsters even manage to contact cardholders by phone and convince them to authenticate fraudulent transactions via their banking applications (voice phishing or "vishing").

The second type of fraud remains the use of lost or stolen cards, which mainly affects face-to-face transactions.

C20 Breakdown of card payment fraud by type (%)



Source: Observatory for the Security of Payment Means.

However, the share of this type of fraud in domestic transactions fell from 30.6% in 2019 to 24.7% in 2020 as a result of travel restrictions and shop closures during the lockdown periods.

Counterfeit cards remained marginal, accounting for only 1% of fraudulent domestic payments. The share of this type of fraud in fraud amounts on international transactions was slightly higher (5% for transactions within SEPA and 11% outside the area). This very low level is mainly attributable to most three-party card schemes adopting smartcard technologies and to enhanced security for existing EMV smartcards.

Lastly, tracking of physical points of weakness showed that the number of jackpotting or skimming attacks on ATMs, card-operated fuel pumps and payment terminals continued to decline in 2020 (*see Box 4 below*).

2.3 Cheque fraud

2.3.1 Overview

In 2020, while cheque fraud decreased during the first lockdown period due to the closure of bricks and-mortar stores and bank branches, it once again increased following the lockdown as cheque use resumed. Fraud amounts involving cheques thus remained virtually stable at EUR 538 million, compared to EUR 539 million in 2019. At the same time, the period saw a significant 20% increase in the number of cheques used for fraudulent purposes (220,730, compared to 183,488 in 2019). Cheque fraud is declining at a lower rate than cheque payments (-24.6% in value terms compared to 2019). Consequently, the fraud rate rose again significantly in 2020 to 0.088% (compared to 0.066% in 2019), which is higher than for payment

cards (0.068% in 2020). This represents the equivalent of one euro of fraud for every EUR 1,140 paid by cheque. The share of cheques in the total fraud involving cashless means of payment came to 42%, compared to 37% for cards, even though cheques are used twelve times less frequently than cards. These figures show that **cheques remain the means of payment most prone to fraud in France, in terms of both rate and value.**

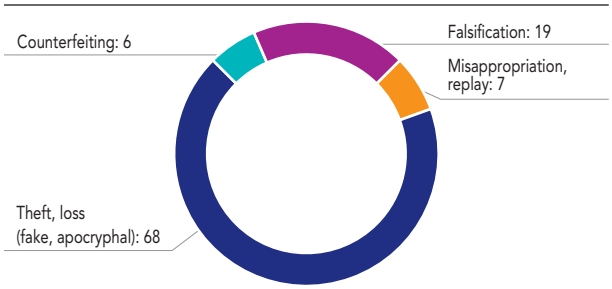
2.3.2 Breakdown of fraud by type

Use of lost or stolen cheques remains the main method of fraud, with the corresponding share in fraud value rising significantly to 68%, compared to 55% in 2019. Lost or stolen cheques also account for 89% of cheque fraud cases. This type of fraud consists in using lost or stolen cheques to pay for goods or services or to deposit them directly in a bank account. In the latter case, fraudsters use fraudulent back accounts opened with false identity documents or via identity theft. They may also call on a third party, sometimes known as a "mule", who agrees to cash the cheque on their behalf. Such intermediaries are usually recruited via social networks. Fraudsters instruct them, in return for a promise of remuneration or by deception, to cash the lost or stolen cheques and then transfer the funds. This phenomenon has been growing rapidly in recent years, and the Observatory reminds users that those who participate in this type of fraud run the risk of being recognised as accomplices and face prosecution. The Observatory also urges users to be particularly on their guard when receiving and storing their ordered chequebook (as mentioned among the recommended best practices in terms of vigilance presented in Appendix 1 of this report).

The second type of fraud encountered in 2020 remains falsification of valid cheques. This process consists in fraudulently modifying the amount or beneficiary of a valid cheque – taken from the mailbox of the cheque beneficiary, for example – and then cashing it. This type of fraud diminished in 2020 due to the decline in cheque payments. In 2020, falsification accounted for 19% of cheque fraud value (compared to 27% in 2019) and 6% of fraud cases.

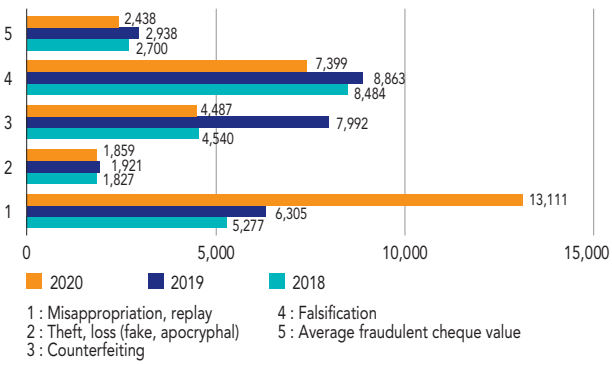
Misappropriation of valid cheques rose sharply in 2020 to EUR 37 million, compared to EUR 20 million in 2019, an increase of 81% year-on-year. This type of fraud mainly covers valid cheques that are intercepted on their way to the beneficiary and deposited in an account owned by a fraudster without any alteration. This type of fraud constitutes the third most common type of fraud in 2020, accounting for 7% of cheque fraud value.

C21 Value-based breakdown of cheque fraud by type (%)



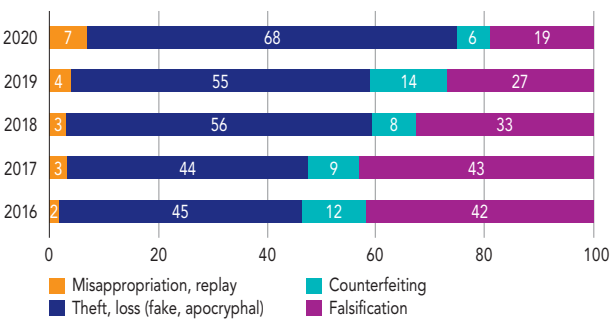
Source: Observatory for the Security of Payment Means.

C22 Individual fraudulent cheque values by fraud type, 2018–2020 (in EUR)



Source: Observatory for the Security of Payment Means.

C23 Value-based breakdown of cheque fraud by type, 2016–2020 (%)



Source: Observatory for the Security of Payment Means.

Cheque counterfeiting, i.e. the use of cheques entirely fabricated by counterfeiters and then resold on the dark web to third parties who use them with merchants or private sellers, accounted for 6% of fraud value (compared to 14% in 2019) and 3% of fraud cases. This type of fraud is declining compared to 2019, likely due to the closure of businesses and to law enforcement action against counterfeiters.

The average amount of a fraudulent cheque fell to EUR 2,438, compared to EUR 2,938 in 2019, due to the increase in lost or stolen cheques, which generally involve smaller amounts than other types of fraud. Unit amounts remained particularly high for cheque falsification (EUR 7,399, compared to EUR 8,863 in 2019) and misappropriation (EUR 13,111, compared to EUR 6,305 in 2019).

In view of the steady rise in cheque fraud over the past five years, the Observatory conducted a study on approaches to strengthening cheque security, calling on the participation of all stakeholders concerned (banks, public authorities, consumer, business and retail associations, as well as technical service providers involved in the processing cycle for this means of payment). The results of this study, which include recommendations for the various categories of actors involved, are presented in Chapter 4 of this report.

2.4 Credit transfer fraud

2.4.1 Overview

In 2020, fraud involving credit transfers issued from an account held in France once again increased, coming to just over EUR 267 million. This represents a significant rise of 65% compared to 2019, with the number of fraud cases more than doubling to nearly 36,000 fraudulent transactions in 2020. Consequently, the average amount of fraudulent credit transfers decreased, standing at EUR 7,436 compared to EUR 10,144 in 2019.

The fraud rate for credit transfers nevertheless remained very low at 0.0008% (compared to 0.0006% in 2019), i.e. one euro of fraud for every EUR 125,000 paid, which can be explained by the strong growth in flows for this means of payment (+30% in value compared to 2019) and their prominence in cashless transactions (91% of the total amount of cashless payments issued in 2020). **Of all payment means, credit transfers remained the least affected by fraud, even though they move the most significant overall values.** However, the fraud rate varies depending on the initiation channel for the transfer order, the type of transfer issued and the geographical destination of the funds.

2.4.2 Breakdown of fraud by initiation channel

Credit transfer initiation from online banking spaces (via the internet or a mobile phone application) was still the most affected channel, accounting for the majority of fraud amounts for this means of payment (54%, compared to 55% in 2019). Proportionally speaking, this figure remains high given that these types of credit transfers only account for 37% of all transfer flows in value and 26% in volume. Nevertheless, the fraud rate on this initiation channel dropped to 0.0012% (compared to 0.0023% in 2019), likely due to the gradual generalisation of strong customer authentication for access to online banking services and for sensitive transactions carried out on those platforms. This corresponds to one euro of fraud for every EUR 83,300 paid. Fraud on this channel involves false transfer orders initiated by fraudsters having stolen legitimate customers' credentials for their online or mobile banking spaces, as well as transfer orders initiated by customers themselves on the basis of manipulation by a fraudster.

The telematic channel, primarily used by professionals, accounted for 35% of fraud amounts for this means of payment, i.e. an increase compared to the 2019 level of 24%, with a fraud rate that, although still extremely low, nevertheless rose significantly year-on-year to 0.0008% from 0.0002% in 2019. While this remains the most secure transfer order initiation method, the increase in fraud in 2020 is due to a rise in fraud using social engineering[7] techniques, which exploit the human factor rather than technology.

Finally, fraud involving paper-based transfer initiation (post, telephone calls, etc.) decreased, accounting for a mere 12% of fraud amounts for this means of payment (compared to 21% in 2019). This drop reflects the decrease in flows initiated from this channel (-12% in value compared to 2019). The fraud rate on paper-based credit transfer orders remained nearly stable year-on-year at 0.0018% (compared to 0.0017% in 2019), albeit at a higher level than for other initiation channels. Fraud on paper-based transfers results either from fraudsters issuing false orders by stealing the identity of the holder of the debited account, or from social engineering manipulation techniques that aim to dupe account holders into issuing false transfer orders. This channel is particularly vulnerable to fraud given that its specific characteristics are incompatible with the implementation of advanced security solutions, particularly strong authentication.

2.4.3 Breakdown of fraud by type of credit transfer

Insofar as almost all credit transfers (98% in terms of volume) are issued as classic SEPA transfers, these logically account for a very large proportion of fraud amounts, i.e. 79% of fraud cases in 2020). However, since classic SEPA credit transfers only accounted for 31% of flows in value terms, the fraud rate was relatively low at

0.0019%, i.e. the equivalent of one euro of fraud for approximately EUR 51,630 paid.

With regard to SEPA Instant Credit Transfer, the corresponding share of fraud amounts remained low at 4% as this means of payment remains little used (1% and 0.08% in volume and value of transfers issued, respectively). However, the associated fraud rate stood at 0.0397%, i.e. almost 50 times higher than the overall rate for credit transfers (all types of transfers combined), and recorded a slight increase year-on-year (0.0311% in 2019). Indeed, the number of fraudulent instant transfer transactions increased almost tenfold compared to 2019, representing 20% of fraud cases, while the average amount was halved from EUR 3,022 to EUR 1,481. Although the ramp-up of instant transfers is taking place under generally adequate security conditions, their widespread use nevertheless calls for greater attention from users and professionals (see *Chapter 3, "Technology watch on real-time payment security"*), particularly when the beneficiary requests that the funds be sent to an account held abroad.

Finally, large-value transfers (LVTs), exchanged through dedicated payment infrastructures and corresponding exclusively to payments of high unitary or urgent amounts by corporate and government customers, were relatively unaffected by fraud, with an extremely low fraud rate of 0.00001%, which is equivalent to one euro of fraud for every EUR 10,000,000 paid.

2.4.4 Geographical breakdown of fraud

While all geographical areas showed growth in credit transfer fraud, the increase was particularly pronounced for transfers issued from non-SEPA countries, where fraud amounts increased more than threefold, but also for those sent to a SEPA country (68% increase in fraud amounts compared to 2019). Cross-border credit transfers were thus more prone to fraud, on a proportional basis, than domestic transfers, accounting for 55% of fraud amounts, whereas they represented only 12% of credit transfers issued in value terms. Fraud on domestic transfers increased as well, albeit to a comparably lesser extent (+44% compared to 2019). The fraud rate for domestic transfers nevertheless remained stable at 0.0004%, an extremely low level considering the value of these flows, which accounted for 88% of all transfers issued. In contrast, cross-border transfers continued to exhibit structurally higher rates of fraud, increasing further year-on-year to reach 0.0033% for transfers made to a SEPA country (compared to 0.0016% in 2019) and 0.0046% for those made outside SEPA (compared to 0.0011%). These figures demonstrate that fraudsters regularly use accounts opened abroad to collect fraudulently acquired funds. **The Observatory calls on users to exercise greater vigilance regarding the identity of contacts and the legitimacy of requests when the destination of funds appears to be a foreign account (IBAN number not beginning with FR).**

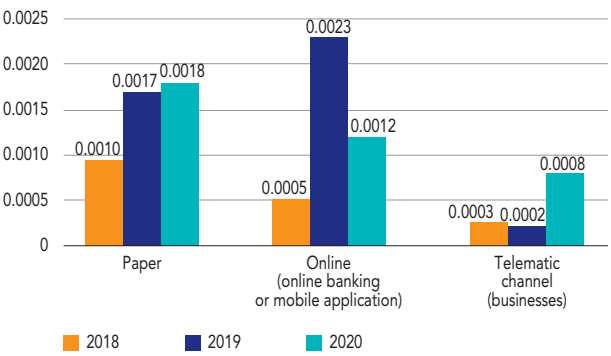
2.4.5 Breakdown of fraud by type

Misappropriation was the dominant type of fraud, accounting for 58% of fraud amounts compared to 35% in 2019, while remaining concentrated in a smaller number of cases, i.e. only 16% of the volume of fraudulent transfers. This situation was due to the fact that this type of fraud primarily targets firms and government actors, therefore affecting fewer victims while causing greater financial harm. The health crisis, with the resulting increase in digital exchanges and the disappearance of the usual reference points for financial and accounting teams, has been conducive to an upsurge in fraud based on social engineering techniques. The most widespread deception schemes in 2020 were those relating to CEO fraud, fraudulent change of bank account details and fake bank advisor scams. Government offices have also been victims of such frauds, including state-paid furlough scams, whereby fraudsters managed to impersonate firms (company name and identification number) in order to divert funds from the financial aid mechanisms implemented in the framework of the Covid-19 crisis.

Fake credit transfers initiated by fraudsters, which in 2019 accounted for 61% of fraud amounts, fell sharply to 34%. However, this type of fraud continued to account for the majority of fraud cases (79% in 2020) insofar as it primarily targets private individuals who are subject to value limits for remotely initiated transfers, thus leading fraudsters to carry out a greater number of offences for smaller amounts. For the most part, fake transfers are initiated from online banking spaces (via the internet or a mobile phone application) using personal login data obtained by fraudsters, most often by way of phishing or malware. As in 2019, fraudsters took advantage of the implementation of strong authentication solutions by banks to exploit the associated communication measures, e.g. sending fake messages aiming to collect personal login data for online or mobile banking spaces, where they then initiated fraudulent transfers. In addition, significant phishing attacks were observed during the lockdown periods, including fake online banking sites created by reproducing all or part of

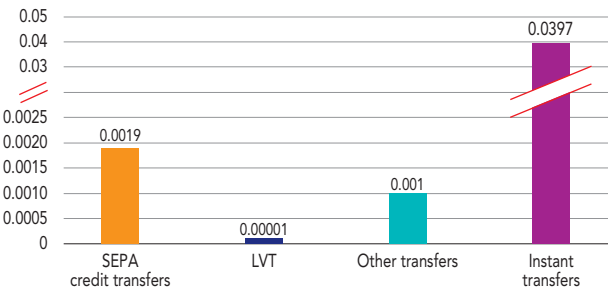
7 Social engineering is defined as "the art of manipulating people into performing actions or divulging confidential information".

C24 Credit transfer fraud rate by initiation channel (%)



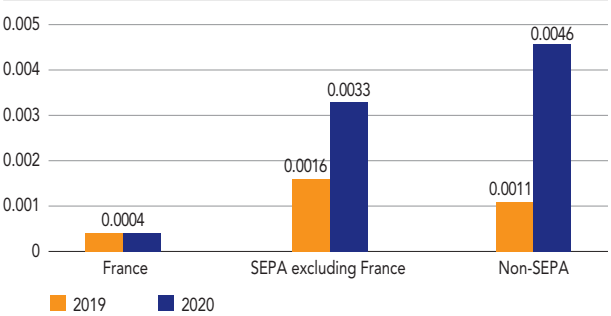
Source: Observatory for the Security of Payment Means.

C25 Credit transfer fraud rate by transfer type (%)



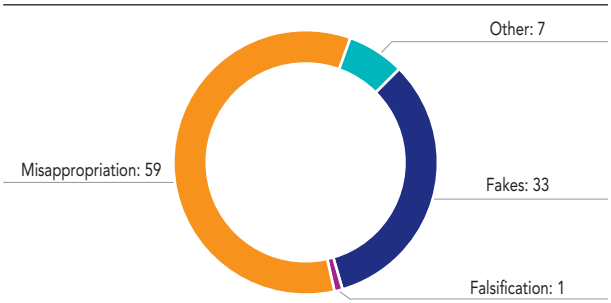
Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area, LVT – large-value transfers.

C26 Credit transfer fraud rate by geographical area (%)



Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

C27 Value-based breakdown of credit transfer fraud by fraud type (%)



Source: Observatory for the Security of Payment Means.

the content features on the portals of authentic institutions. With regard to this phenomenon, the Observatory invites the public to apply the precautionary measures recalled in Appendix 1 of this report when connecting to online banking spaces.

2.5 Direct debit fraud

2.5.1 Overview

In 2020, fraud on direct debit payments from accounts held in France fell sharply to EUR 1.9 million, compared to EUR 11 million in 2019, a drop of 83%, even though the flows issued fell only slightly to 1.6% in value terms. **Direct debits recorded the lowest annual fraud value of all payment means available to individuals, as well as the lowest rate of fraud** at 0.0001%, compared to 0.0006% in 2019, which is equivalent to one euro of fraud for every EUR 1 million of transactions. The average value of a fraudulent direct debit was EUR 292, compared to EUR 253 in 2019.

2.5.2 Breakdown of fraud by type

In 2020, the main source of direct debit fraud was fake direct debits, i.e. the issuance of direct debit instructions by a fraudulent creditor without any authorisation or underlying economic reality. Indeed, this type of fraud alone represented 95% of the fraud amounts and 94% of cases. Misappropriation, i.e. fraudsters stealing IBANs[8] in order to subscribe to services (e.g. telephony), was barely seen in 2020, accounting for less than 1% of fraud amounts, compared to 61% in 2019.

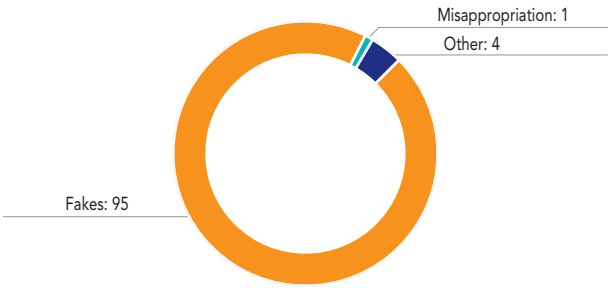
2.5.3 Geographical breakdown of fraud

Direct debit fraud increased on transactions issued to debtors' accounts held by institutions in SEPA countries, whereas such transactions were only marginally affected in 2019: they accounted for 25% of fraud amounts, while they represent a mere 2% of the total value of direct debit flows. Consequently, the fraud rate stood at 0.00164%, compared to an overall rate of 0.0001% for this means of payment. The fraud rate for domestic direct debits is extremely low at 0.00009%.

C28 Value-based breakdown of direct debit fraud by geographical area
(%)

Source: Observatory for the Security of Payment Means.
Note: SEPA – Single Euro Payments Area.

C29 Value-based breakdown of direct debit fraud by fraud type
(%)



Source: Observatory for the Security of Payment Means.

8 International bank account number.

Types of cheque fraud in 2020

Main cases of cheque fraud	Preventive measures
Fraud techniques derived from "cheque kiting", consisting in depositing a number of fraudulent cheques and then immediately removing the funds via credit transfers, cash withdrawals or card payments. These cheque deposits may be carried out: • either directly through accounts fraudulently opened under a false or stolen identity (e.g. the accounts of professionals and entrepreneurs that are credited with immediate effect when cheques are deposited), • or indirectly through a third party, often a private individual, who agrees to cash fraudulent cheques in return for a promise of remuneration or as a result of emotional blackmail ("mule" fraud).	**Identification of unusual deposit movements** in light of the customer's profile and habits in order to: • delay crediting the funds until the legitimacy of the deposit has been verified with the depositor and the soundness of the cheque verified with the issuing bank, • increase vigilance with regard to subsequent transactions immediately following a cheque deposit and involving the withdrawal or transfer of funds to another institution.
Theft of chequebooks in the distribution circuit: a number of external service providers are involved in the distribution circuit, notably during transport and delivery to the customer. Chequebooks and blank cheque specimens can be stolen at two levels: • before delivery to the customer, at the place at which they are manufactured and/or from where they are dispatched, at the transporter or deliverer to bank branches, in customers' postboxes; • during collection at bank branches, where fraudsters can use stolen or forged identity documents to collect a chequebook. **Chequebook theft when in the customer's possession** due to break in, theft or loss.	**Rapid and systematic reporting of lost or stolen cheques**, even if the victim is insured for such events. The loss or theft is to be reported to the banking institution. Issuance of regular reminders by banks that the holders of chequebooks and cheque letters must be on their guard, along with reminders of cheque fraud reporting procedures. **Traceable shipment processes** for chequebooks and cheque letters during the different transport phases. **Notifying the customer that a chequebook is available**, either for collection at the branch or for delivery by post, depending on the option selected by the customer when s/he applied for a chequebook, and indicating an expected delivery timeframe so that the customer can inform the bank in the event of a delay. **Merchants can protect themselves against lost or stolen cheques by consulting the Fichier national des chèques irréguliers (FNCI, the national register of irregular cheques)**, the Banque de France's official prevention service for unpaid cheques.[1]
Falsification of a valid cheque intercepted by a fraudster, consisting in altering a stolen cheque by scratching out, over-writing or erasing information contained on it. The fraudster exploits the vulnerabilities of a stolen cheque by for instance: • scratching out or erasing the name of the lawful beneficiary if it has been written in weak ink and replacing it with another name; • writing the name of a new beneficiary over the legitimate beneficiary's name; • adding something (for example a name or an acronym, a company stamp, etc.) after the name of the lawful beneficiary if blank spaces are left on the line; • adding an amount in letters and/or figures if any blank spaces are left before or after the handwritten amount.	**Fill out cheques preferably with a black ballpoint pen**, leaving no space before or after required information, e.g. by drawing a line to end each space. **Pay particular attention to cheques sent by post**, verifying receipt of the cheque by the lawful beneficiary and regularly consulting account activity. **For persons accepting cheques, systematic examination of the cheque and the information on it, as well as consistency with the payer's identity.** This involves a physical examination of the cheque to identify any alterations prior to acceptance, as well as verifying the identity of the payer, e.g. by requesting an identity document.
Counterfeiting of cheques, through the creation of a false cheque from scratch to be drawn on a false bank (although generally the name of an actual institution is used).	**For persons accepting cheques, in depth physical examination of the cheque and of the payer's proof of identity** (*see above*). This involves verifying the consistency of the data on the cheque and the presence of the security features typically used by the issuing bank (e.g. micro-letters visible under a magnifying glass on the lines of the cheque, fluorescent inks visible under an ultraviolet lamp, quality of printed patterns, etc.). **Merchants can protect themselves against bogus cheques by consulting the *Fichier national des chèques irréguliers* (FNCI, the national register of irregular cheques)**, the Banque de France's official prevention service for unpaid cheques.[1] This makes it possible to verify the consistency between the magnetic line and the image of the cheque, and to consult the file listing the bogus cheques known to banking institutions.

Source: Observatory for the Security of Payment Means.

1 See *https://www.verifiance-fnci.fr*

Types of credit transfer fraud in 2020

Main cases of cheque fraud	Preventive measures
In 2020, **misappropriation-type fraud through social engineering techniques** mainly took the following forms: • **CEO fraud**: the fraudster impersonates a senior company executive to trick an employee into making an urgent, confidential credit transfer to a foreign account. To do this, the fraudster uses information that s/he gathers on the company and its executives via the internet or directly from the company itself. • **Bank account details fraud**: the fraudster impersonates a supplier, lessor or any type of creditor and falsely informs the customer, tenant or debtor that there has been a change in the bank account details that they use to pay their bills, invoices or rent, misappropriating the funds for themselves. The fraudster sends the new bank details by email or by post in a properly worded letter from the creditor. • **Technical support scams**: the fraudster impersonates an IT technician (from the bank for instance) to run fake tests in order to recover log-in IDs and passwords, trigger fraudulent transfers or install malware. • **Bank advisor scams**: the fraudster uses the bank advisor's telephone number, generally in her/his absence, and contacts the customer to extract sensitive information and data.	**Tools that can monitor and detect unusual transactions** and can suspend the execution of a transfer that has been flagged as suspicious based on normal account activity, due to the amount involved or the country to which the funds are destined. The order can then be cross-checked with the customer before execution. **Initiatives** led by banks and payment service providers to inform and raise awareness among businesses and individuals.
In 2019, **cyber-attacks** essentially targeted online banking websites, and were mainly perpetrated using two methods. • **Malware**: Trojan horses, spammers, viruses, etc., which infect a person's or firm's computer without their knowledge when they open a fraudulent email, browse corrupted websites or connect to infected peripherals (e.g. USB flashdrives). Fraudsters can use this malware to analyse and collect data traffic on a customer's computer or information system. Therefore, when the customer logs into her/his online bank account, the malware can retrieve the ID and password that s/he has entered and use them to log in, request that a new beneficiary be added for credit transfers or initiate a fraudulent transfer order. • **Phishing**: fraudsters use this technique to gather personal and banking details by sending out unsolicited emails inviting recipients to click on a link that takes them to a fake website (online banking or e-commerce site), where the person is usually asked to enter their banking credentials. The tone of these emails is usually alarmist, urging the recipient to act quickly (to settle a bill in order to avoid the interruption of a service, to lift a banking suspension or to update security features). There are variants of phishing through other channels, such as "smishing" via SMS.	**Deploying a strong authentication system to approve credit transfer orders** entered online. **Triggering time delays or strong customer authentication when new transfer beneficiaries are added** on online banking sites. **Setting maximum transfer ceilings** on online banking sites. **Providing secure solutions to customers** to scan for malware-type infections on their terminals. **Implementing tools for monitoring and detecting** unusual transactions that can be used to suspend the execution of a transfer that has been flagged as suspicious based on normal account activity, due to the amount involved or the country to which the funds are destined, for example. A warning message can be sent to the customer giving her/him the possibility to block the transaction, if required, during the time delay. Initiatives led by banks and payment service providers to inform and raise awareness among businesses, in particular to update operating systems on a regular basis.

Source: Observatory for the Security of Payment Means.

Types of direct debit fraud in 2020

Main cases of direct debit fraud	Preventive measures
Illegitimate issuance of direct debit instructions (fake direct debits): a false creditor registers as the originator of a direct debit instruction with a payment service provider and originates a very large number of direct debit instructions using international bank account numbers (IBANs) that s/he has acquired illegally without authorisation.	**Tools to monitor the behaviour of creditors who originate direct debit instructions**, which can detect any unusual movements based on knowledge of the customer. It is important to note that a creditor must have a SEPA Creditor Identifier (SCI) to originate direct debit instructions, which is assigned following verification by the creditor's payment service provider of the suitability of this action. **Transmission of an alert to the customer** when a direct debit instruction is first received from a creditor to debit her/his account. **Optional services** through which a customer can set a maximum amount to be debited by creditor and by country or compile a list of creditors who are authorised to make direct debits on her/his account (white-listed creditors) or, alternatively, a list of creditors who are not authorised to do so (black-listed creditors). **Taking care when disclosing IBANs** in the course of business interactions and online activities.
Collusion between the creditor and the payer: a creditor with fraudulent intent originates direct debit instructions on an account that is held by an accomplice in a regular manner, gradually increasing the amounts. The payer disputes the debited amounts not long before the end of the statutory cancellation period (13 months after the direct debit is cleared), on the grounds that s/he did not sign a mandate for the direct debit. When the direct debit is rejected, the balance on the creditor's account is not sufficient to refund the disputed amounts as the funds have been transferred to an account held abroad.	**Tools to monitor the behaviour of creditors who originate direct debit instructions**, which can detect any unusual movements based on knowledge of the customer. It is important to note that a creditor must have a SEPA Creditor Identifier (SCI) to originate direct debit instructions, which is assigned following verification by the creditor's payment service provider of the suitability of this action.
Misappropriation of IBANs for subscription to services: a debtor with fraudulent intent provides the account details of a third party on the direct debit mandate, enabling her/him to obtain services without honouring the related payments.	**Transmission of an alert to the customer** when a direct debit instruction is first received from a creditor to debit her/his account. **Optional services** through which a customer can set a maximum amount to be debited by creditor and by country or compile a list of creditors who are authorised to make direct debits on her/his account (white-listed creditors) or, alternatively, a list of creditors who are not authorised to do so (black-listed creditors).

Source: Observatory for the Security of Payment Means.

❷ Fraud statistics for payment cards: respondents

The Observatory gathers data from all issuers of "four-party" and "three-party" card schemes,[1] in order to ensure that its fraud statistics are reliable and representative.

The 2020 statistics calculated by the Observatory thus cover:

- EUR 682.3 billion in transactions in France and abroad made with 89 million four-party cards issued in France (including 81 million cards equipped with a contactless function);
- EUR 11.9 billion in transactions primarily in France made with 5.6 million three-party cards issued in France;
- EUR 31.2 billion in transactions in France made with foreign three-party and four-party cards.

Data were gathered from:

- the 120 members of the CB Bank Card Consortium (Groupement des Cartes Bancaires CB), collected through the Consortium and from MasterCard Europe and Visa Europe France;
- seven three-party card issuers: American Express, Oney Bank, Crédit Agricole Consumer Finance, Cofidis, Franfinance, JCB and UnionPay International.

1 "Four-party" card payment schemes involve a large number of issuing and acquiring payment service providers, as opposed to "three-party" schemes, which involve a single payment service provider solely responsible for issuance and acquisition functions.

❸

Domestic remote payment fraud, by sector of activity

The Observatory gathers data providing information on the breakdown of remote payment fraud by sector of activity. These data cover domestic transactions only.

Remote payment fraud concerned mainly the following three sectors of activity: "General and semi-general trade", "Personal and professional services", and "Telephony and communication", which together accounted for 65% of fraud amounts in 2020. The percentage of total fraud attributable to the "Travel and transport" sector, which has traditionally been among the sectors most exposed to fraud, fell by half (6.7 in 2020 compared to 12.9% in 2019) due to the sharp drop in card payments received by this sector (– 81% in 2020 compared to 2019) in the context of the Covid-19 crisis.

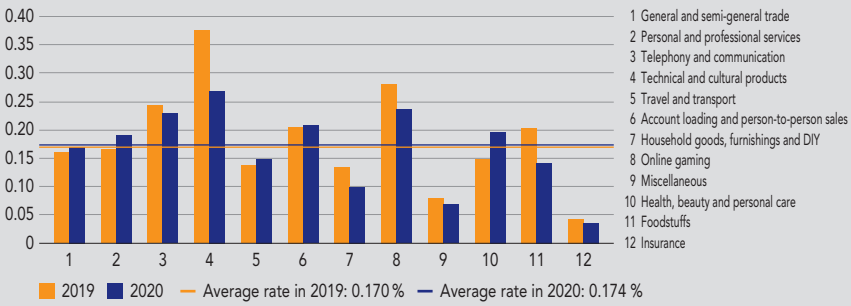
Fraud rates by sector of activity did not increase significantly year-on-year. Indeed, the "Technical and cultural products" sector even saw a clear reduction in fraud, with the corresponding rate falling from 0.376% in 2019 to 0.270% in 2020. Nonetheless, this sector, together with "Telephony and communication" and "Online gaming", showed above-average fraud rates and accounted for the highest rates of fraud of all sectors *(see Chart)*.

Breakdown of fraud by sector of activity (amount in EUR millions, share in %)

		Amount	Share
1	General and semi general trade	60.6	27.3
2	Personal and professional services	55.1	24.9
3	Telephony and communication	29.1	13.1
4	Technical and cultural products	18.7	8.4
5	Travel and transport	14.9	6.7
6	Account loading and person-to-person sales	14.2	6.5
7	Household goods, furnishings and DIY	10.9	4.9
8	Online gaming	6.3	2.8
9	Miscellaneous	5.3	2.3
10	Health, beauty and personal care	4.0	1.8
11	Foodstuffs	1.9	0.9
12	Insurance	0.9	0.4
Total		**221.9**	**100.0**

Source: International card payment systems.

Fraud rate for remote sales by sector of activity, domestic transactions (%)



Source: Observatory for the Security of Payment Means.

❹

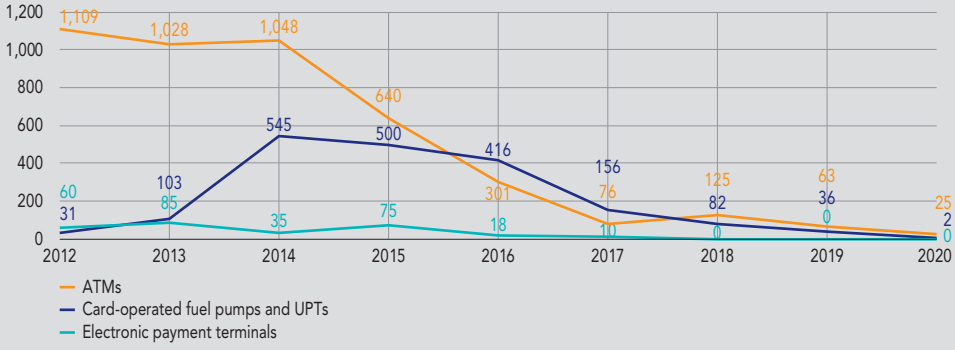
Indicators provided by law enforcement agencies regarding ATM and payment terminal attacks

Automated Teller Machine (ATM) attacks continued to decline in 2020 with 25 cases compared to 63 in 2019. Attacks on card-operated fuel pumps all but vanished, with only two cases recorded (compared to 26 in 2019). Finally, there were no reported cases involving hacking of payment terminals, whether public (e.g. car park terminals) or associated with individual merchants.

With regard to operating methods, the summer of 2020 saw a resurgence in ATM "jackpotting". This fraud technique consists of physically or remotely attacking an ATM by hacking into the embedded computer to activate the cash-dispensing mechanisms. It calls for highly sophisticated procedures that can only be implemented by organised crime networks or specialised criminals. In addition to physical and software protection measures implemented for ATMs by payment professionals, action by law enforcement agencies (infiltration, use of video surveillance images, bugging, etc.) makes it possible to dismantle these networks and contain this type of fraud.

On the other hand, "skimming" fraud, which involves capturing bank data stored on the magnetic strip of the card by means of compromised or altered payment terminals, appears to be under control. However, merchants must remain vigilant to prevent attempts to replace a legitimate payment terminal with a compromised one, as well as any installation of a fraudulent external device (reader, camera, keyboard, etc.) by a third party. The card data thus obtained by criminal networks are resold on dedicated dark web sites or through mobile phone applications. They are subsequently re-encoded on magnetic strip cards, which are then used for local payments and withdrawals abroad, (chiefly in countries where EMV – Europay Mastercard Visa – smartcard technology is not widely used, particularly the Americas and South East Asia, or to carry out remote payments, most often on e commerce sites that have not implemented cardholder authentication solutions.

Attacks on ATMs and terminals (number)



Source: Observatory for the Security of Payment Means.
Note: ATMs – Automated Teller Machines, UPTs – Unattended Payment Terminals..

Chapters 3 and 4 and the appendices are available in french only in the original version of the report, which can be found here:
https://www.banque-france.fr/rapport-annuelde-lobservatoire-de-la-securite-des-moyens-de-paiement-2020

Published by
Banque de France

Managing Editor
Nathalie Aufauvre
Director General, Financial Stability and Market Operations
Banque de France

Editor-in-Chief
Valérie Fasquelle
Director of Infrastructures, Innovation and Payments
Banque de France

Editorial Secretariat
Pierre Bienvenu, Véronique Bugaj, Olivier Catau, Caroline Corcy, Florian Dintilhac, Christelle Guiheneuc, Trân Huynh, Julien Lasalle

Technical production
Studio Création
Direction de la Communication

Contact
Observatory for the Security of Payment Means
Internal mail code: 011-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Legal deposit
July 2021
ISSN 2557-1230 (online version)

Internet
www.observatoire-paiements.fr

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

www.banque-france.fr