Observatoire de la sécurité des moyens de paiement
www.observatoire-paiements.fr

RECOMMENDATIONS OF THE OBSERVATORY

PROCEDURES FOR REIMBURSING FRAUDULENT PAYMENT TRANSACTIONS

1- BACKGROUND

1.1 Introduction of strong customer authentication to protect electronic payments

Use of strong customer authentication to initiate electronic payments is a key payment security provision introduced by the second European Payment Services Directive (PSD2).[1] In the case of online card payments, implementation of this provision at the level of the French market followed a migration plan adopted by the Observatory in autumn 2019, and strong authentication was subsequently deployed over a period of approximately two years.

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

- "knowledge": something only the user knows, such as a PIN, password or piece of personal information;
- "possession": something that only the user possesses and that may be recognised without risk of error by the payment service provider (PSP), such as a card, a smartphone, a USB key, a secure card reader, smart watch or bracelet;
- "inherence": something the user is, i.e. a biometric feature, such as a fingerprint, face or voice.

When a remote procedure is used to enrol a possession element, i.e. associate a user with an object that only the user possesses and that will act as a strong authentication factor, then the enrolment itself must also be validated by strong authentication.

PSD2 states that these elements should be independent: in other words, the compromise of one should not call into question the reliability of the others, in order to preserve the confidentiality of authentication data. PSD2 also includes an additional requirement for remote payments: authentication data must be linked to the payment transaction, such that they may not be used for subsequent payments. This is called a dynamic link:

- the authentication code generated for the transaction is specific to the transaction amount and the payee;
- any change to the amount or the payee requires a new authentication.

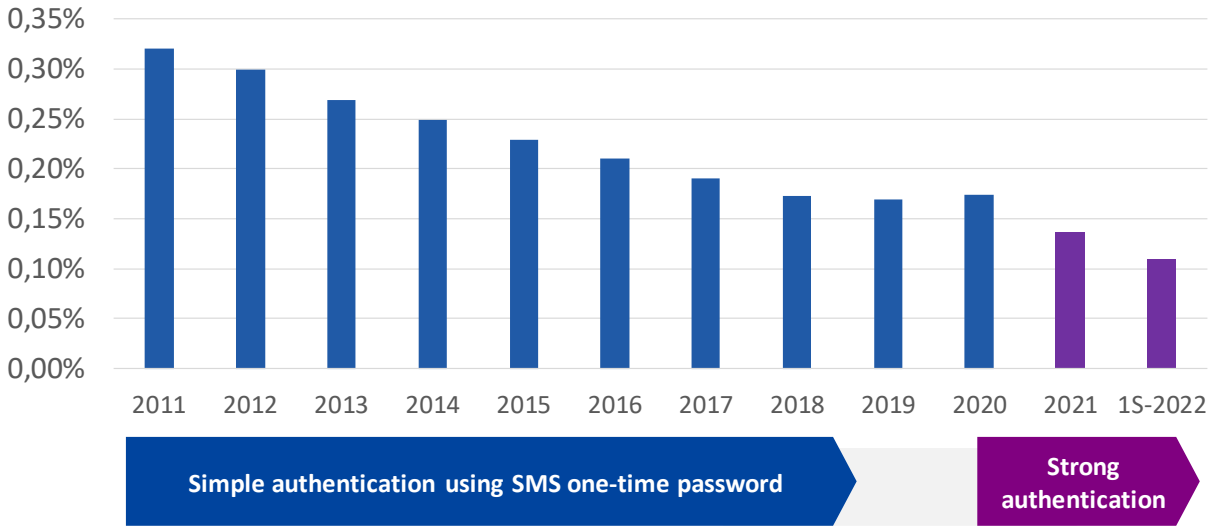
If a biometric factor is used, the validation key generated for the payment transaction after the factor is read should also be for one-time use only.

While it is still too early to make a definitive assessment of the strong authentication system, the Observatory notes that it has already helped to substantially lower fraud rates for internet payments,

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

following two years during which fraud rates stayed the same, underscoring how the simple authentication systems (SMS one-time password) deployed in the 2010s had reached their limits in terms of security. The first available data for 2022 indicate that fraud rates are expected to continue falling significantly.

Chart 1 – Fraud rate for domestic online card payments



Looking at all online card payments, including payments on foreign websites by French cardholders, the fraud rate for online payments, as measured by value, fell from 0.249% in 2020 to a record low 0.196% in 2021, while the value of card payment transactions climbed 21% to EUR 177.1 billion over the same year.

1.2 Development of new manipulation-based fraud techniques to get round strong authentication

While the introduction of strong authentication ensures a high level of technological security across the entire payment chain, this makes it all the more important for users, who are increasingly targeted by fraudsters, to be even more careful. If they cannot issue fraudulent payments themselves, fraudsters try to manipulate their victims over the phone or through instant messaging into validating fraudulent transactions for them, typically by posing as their bank. This could involve pretending that they are running security tests or anti-fraud measures, or saying that authentication checks are needed after an unusual transaction on the victim's account. They manage to persuade the victim to share information that enables them to use the payment instruments remotely. They start by gathering information on their victim through phishing-type attacks using SMS (text) messages or emails, third-party data theft, as well as social media and public sources, before contacting the victim directly. Fraudsters also make use of spoofing techniques, i.e. pretend to be calling from a bank branch to put the victim off their guard.

While the Observatory notes that the proportion of fraudulent payments with strong authentication remained contained in 2021, at 9% of the total number of fraudulent online card payments, their share of the total value of fraudulent transactions is much larger (30% of a total of EUR 103 million).

According to consumer associations, this new type of fraud is driving up the financial losses borne by consumers, despite the overall decrease in fraud. In fact, with the implementation of strong authentication, the risk that a bank might refuse to reimburse a customer for fraudulent transactions may have increased significantly.

In this regard, the Banque de France and the Observatory for the Security of Payment Means were contacted by consumer associations, which drew attention to difficulties encountered by members in exercising the statutory right to reimbursement in the event of fraud, especially in cases where the disputed transaction was subject to strong authentication.

1.3 Work by the Observatory on the treatment of fraud-related disputes

The Observatory decided to set up a working group tasked with issuing Recommendations on the treatment of reimbursement requests for fraudulent transactions, with a view to ensuring proper application of PSD2 provisions on the protection of consumers who are victims of fraud.

The group met five times between October 2022 and February 2023. Participants in the group include representatives of consumer associations, PSPs and their professional federations, ombudsmen and the authorities (law enforcement, ACPR, Banque de France).

The secretariat of the working group determined the inputs and expected deliverables.

Inputs	Expected deliverables
▪ Regulations and previous decisions applicable to the treatment of disputes ▪ Identification of recent developments in fraud case typology ▪ Experience of bank ombudsmen and consumer associations with rejected requests for reimbursement due to fraud ▪ Summary of on-site inspections conducted by the ACPR on the treatment of customer requests for reimbursement due to fraud	▪ Reminder of the applicable rules for the treatment of requests for reimbursement due to fraud ▪ Analysis matrix for reimbursement requests (identify cases where immediate reimbursement should always be issued) ▪ Recommendations for the treatment of requests for reimbursement due to fraud ▪ Review of reasons identified in reports to the Banque de France under Article 73 of PSD2 *(to begin following publication of the Recommendations in this document)*

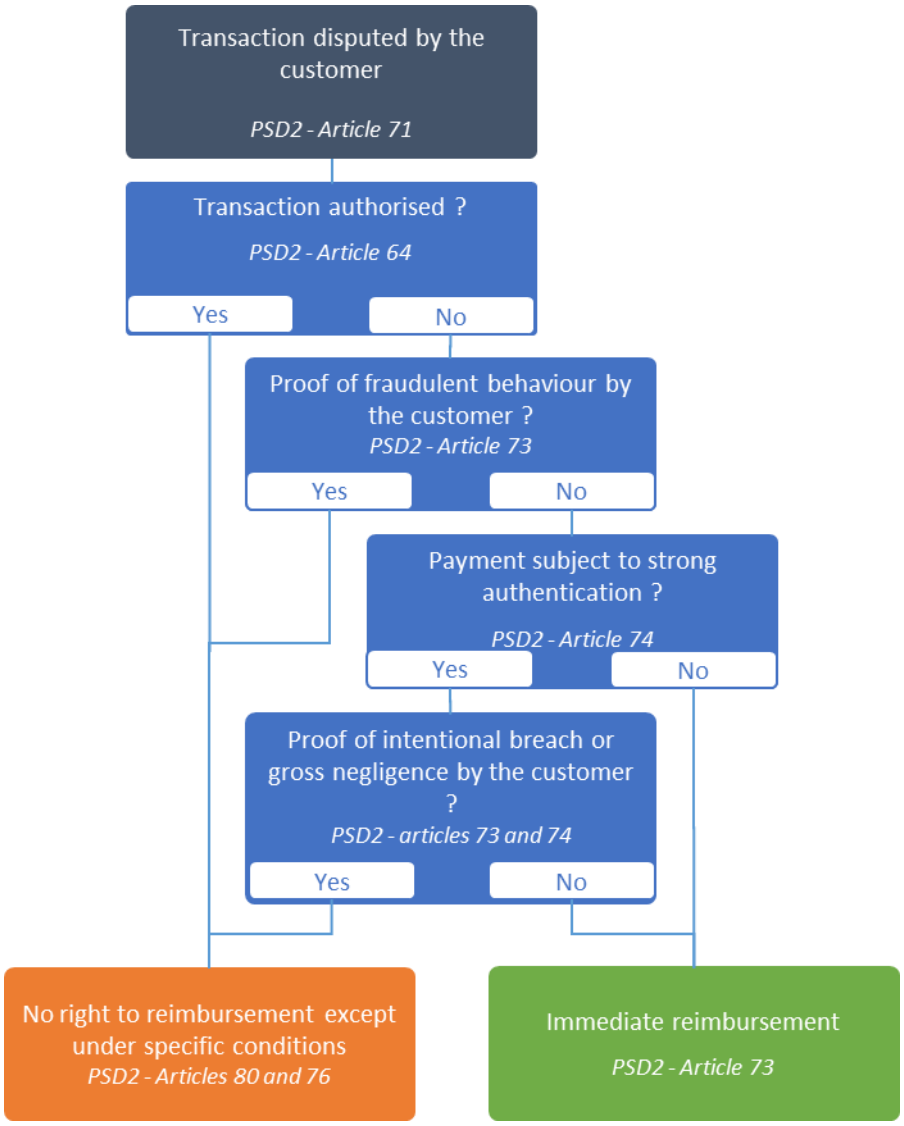
2- REGULATIONS APPLICABLE TO DISPUTED PAYMENT TRANSACTIONS

2.1 The "authorised" nature of the transaction as a determining factor

According to France's Monetary and Financial Code (MFC), the reimbursement of a disputed transaction depends on whether the transaction was authorised by the payer,[2] i.e. whether the payer consented explicitly to execution of the transaction under the terms of the account agreement, notably through the use of the strong authentication solution made available to the payer.

The following diagram illustrates the steps involved in handling disputed transactions and the associated MFC provisions.

[2] Excluding the specific case of the reimbursement regime applicable to certain authorised transactions, including direct debits that occurred less than eight weeks previously (Article 76 of PSD2).



- **If the transaction is recognised as being "authorised" and was not the subject of an execution error by the payer's PSP, the rules governing means of payment do not provide for the right to reimbursement**. This applies in particular to requests for reimbursement due to a commercial dispute between payer and payee (e.g. product not delivered or defective, purchase of a savings or credit product or financial service from a malicious intermediary). **While there may be no regulatory right to reimbursement, the fact that the transaction is classified as "authorised" does not prevent a claim or even a civil or criminal action being brought against the payee**.
- **If the transaction is recognised as "unauthorised", the payer is usually entitled to the immediate reimbursement provided for under the MFC**, although the procedures vary according to a number of factors, such as the nature of the payment instrument, whether it held personalised security data and whether strong authentication was used during the transaction. **However, reimbursement may be refused in the event of fraudulent behaviour by the user or, exclusively**

in the case of transactions subject to strong authentication in accordance with the law,[3] in the event that the PSP proves that the user was grossly negligent.

The assessment of whether or not a transaction is authorised is therefore a determining criterion for the reimbursement of customers who dispute a payment transaction due to fraud. This question is particularly sensitive in the case of transactions that are the subject of strong authentication, where it is necessary to determine to what extent successful strong authentication may or may not be considered to indicate consent by the holder of the payment instrument.

The purpose of the Recommendations set out below is to reduce the "grey area" when assessing whether a disputed transaction is "unauthorised", by reviewing several dispute cases, from the simplest to the more complex. The aim is to identify the circumstances under which a transaction may be assumed to be unauthorised and therefore give rise to immediate reimbursement, unless the PSP can provide proof of fraud or gross negligence by the user.

2.2 Contributions from previous decisions on assessing gross negligence by the payment service user

There is no explicit statutory definition of the elements that characterise gross negligence on the part of the user, which is the main reason given by PSPs for refusing to reimburse an unauthorised payment. Furthermore, the Cour de Cassation has not yet ruled on a dispute involving a transaction executed after the entry into effect of PSD2 and its transposing and implementing instruments. Past decisions (on disputes involving transactions executed before the entry into effect of PSD2) rely on the concept of the "reasonably attentive" user. PSPs that want to invoke this reason as grounds to refuse the right to reimbursement must therefore assess the case with respect to precedent, which is likely to be expanded over the coming years, although a number of previous rulings already provide insight.

3- General recommendations applicable to the treatment of disputes involving payment transactions

3.1 Timeframe for conducting investigations

When the PSP has to conduct investigations, such as investigations into a payment transaction subject to strong authentication (cf. paragraph 4.3 below), the period of time taken for such investigations should be limited. The aim is to ensure that information that is useful to the PSP is neither lost nor forgotten, and also to make sure that the customer has a sufficiently close and identified deadline for getting a clear and final answer on the dispute.

Recommendation No.1: maximum time period for investigations

Payment service providers are encouraged to conduct investigations as soon as the dispute is received, taking into account any descriptive elements provided by the user (as specified in Recommendation No. 8), **and to restrict the length of such investigations to no more than 30 days, except in unusual circumstances.**

3.2 Procedures and timeframe for the recovery of funds

There are several scenarios in which a PSP's initial decision to reimburse a customer could be reversed after the fact, for example in light of additional investigations or if the user is refunded through another

[3] Article 4 of PSD2, 30).

channel (e.g. by the counterparty to the transaction or via insurance), leading the provider to recover the funds. The user should be made aware of this possibility when the initial reimbursement is made.

Recommendation No.2: customer disclosure regarding fund recovery

In the event of a reimbursement that could give rise to a subsequent recovery of funds depending on the outcome of investigations, the payment service provider should inform the customer of this possibility when the reimbursement is made and ensure that funds are recovered within a period not exceeding 30 days from the date on which the reimbursement was made, except in unusual circumstances.

3.3 Information provided to the customer in the event that reimbursement is refused or if funds are recovered

Recommendation No.3: justification for the refusal to reimburse

If the payment service provider refuses to reimburse the customer or recovers funds from the customer, it should inform the customer about this decision and explain the reason, taking care to provide relevant supporting evidence, such as a direct debit mandate, information provided by the merchant, proof of gross negligence, etc. In the same communication, the provider shall also set out the procedures for filing a complaint.

4- RECOMMENDATIONS APPLICABLE TO THE TREATMENT OF SPECIFIC CASES

The cases described below intentionally exclude requests for reimbursement falling outside the scope of fraud involving means of payment, such as commercial disputes or scams (e.g. fake savings products, investments in fraudulent crypto-assets, credit scams, etc.), where the related transactions were authorised.

Likewise, the recommendations focus on enforcement of the right to reimbursement under the rules governing means of payment, and exclude other potential mechanisms, such as means of payment insurance or gestures of goodwill by PSPs.

4.1 Payment transactions executed without strong authentication

Note that not all transactions require strong authentication, since the rules arising from PSD2 provide for a number of exclusions and exemptions:

- **Payments outside the European Union (one-leg transactions)**;
- **Payment orders issued by the payee**, such as direct debits or card payments where the merchant issues the order without an active login by the user, which are referred to as merchant-initiated transactions (**MITs**). These can include split or deferred payments, subscriptions and per-use payments;
- **Payments eligible for a strong authentication exemption under the regulatory technical standards (RTS)** established by the European Banking Authority:[4]
    - Low-value online payments (Article 16), i.e. not exceeding EUR 30, up to five consecutive transactions or a cumulative amount not exceeding EUR 100;
    - Payments posing a low level of risk (Article 18), i.e. consistent with the customer's payment habits (purchase from usual terminal, known delivery address, type of purchase, amount, etc.) and in an amount not exceeding EUR 500;
    - Recurring payments (Article 14), i.e. a series of transactions with a set frequency and amount and the same payee, from the second transaction;
    - Payments to a trusted beneficiary (Article 13), i.e. a beneficiary designated as a trusted party by the payer, such designation having itself been subject to strong authentication. Note that the strong authentication performed when adding a beneficiary has neither the purpose nor the effect of acting as strong authentication for subsequent payment transactions to the same beneficiary;
    - Payments initiated electronically via secure payment processes or protocols reserved for use between professionals (Article 17).
- **Payments issued under authentication infrastructure continuity mechanisms** in the event of an incident preventing application of strong payer authentication, as well as bank card payments executed during the transitional phase (14 September 2019 to 15 June 2021) used to deploy strong authentication.

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

In all the cases listed above, the transaction cannot be considered to have been subject to strong authentication as defined by the regulations, and in most cases the absence of strong authentication is authorised or tolerated.

Recommendation No.4: principles applicable to transactions not subject to strong authentication

When a payment service user disputes one or more transactions that they deny authorising and where these transactions were not subject to strong authentication, the payer's PSP shall promptly reimburse[5] these transactions, unless it has good reasons to suspect that the user has committed fraud. This suspicion of fraud cannot be based solely on the use of the payment instrument.

Such immediate reimbursement shall not prevent the funds from being subsequently recovered if the PSP compiles evidence to show either that the transaction was authorised (e.g. a SEPA direct debit mandate),[6] or that the user committed fraud. Conversely, if the payer is negligent, even grossly so, this cannot be used as grounds to refuse to reimburse a transaction that was not subject to strong authentication.

In the specific case of payments initiated by the payee (MIT direct debits or card payments), the payer is additionally entitled to immediate reimbursement within eight weeks of the account being debited:

- **in the case of direct debits, reimbursement is unconditional, irrespective of whether there is a direct debit mandate;**
- **in the case of a card payment ordered by the payee, if the authorisation provided did not indicate the exact amount of the payment transaction and if the amount of the transaction exceeded the amount that the payer could reasonably expect given the profile of previous spending, the terms of the master agreement and the specific circumstances of the transaction.**

References: Articles 73, 74 and 76 of PSD2 and SEPA Direct Debit Core Scheme Rulebook V1.1 section 4.3.4

The PSP must be in a position to demonstrate that a transaction has been authenticated and to this end must retain the technical elements (audit trail) relating to that authentication. The same applies to the strong authentication audit trail created when enrolling an authentication factor.

4.2 Payment using a mobile application as a substitute for a payment instrument

To pay using a mobile solution with its own authentication mode, which is the case, for example, for the "X-Pay" mobile solutions offered by terminal manufacturers and operating system vendors, the user must first enrol the payment instrument with the mobile terminal's payment application. This enrolment is treated as a sensitive transaction under the regulations and requires strong authentication by the user (EBA Q&A 2021_6141). Responsibility for applying strong authentication lies with the PSP, which has to provide evidence of compliance with this obligation.

[5] The rules specify that reimbursement must take place immediately upon learning about the transaction or being informed about it and in any case no later than the end of the first business day following the date on which the dispute was submitted, and should include any additional fees incurred on a transitional basis as a result of recognition of the fraudulent transaction, such as overdraft fees or loan interest.

[6] Except in the case of direct debits disputed within eight weeks of the account being debited, for which the payer is entitled to unconditional reimbursement.

Recommendation No.5: principles applicable to transactions conducted with a mobile application replacing a payment instrument

When a payment service user disputes a payment transaction that they deny authorising and that was executed using a mobile solution where the payment instrument was not enrolled with strong authentication, the payer's payment service provider shall promptly reimburse this transaction.[7]

References: Article 73 of PSD2 and EBA Q&A 2021_6141

4.3 Payment subject to strong authentication

As mentioned earlier, much of the "grey area" involves disputed transactions that were the subject of strong authentication. The investigation process followed by PSPs should seek to examine elements and parameters that could affect the user's strong authentication.

Analytical elements that need to be taken into account include:

- **The possibility that a third party has taken possession of the strong authentication solution**, notably if one or more of the following has occurred:
    - transfer of the strong authentication solution prior to the fraud (e.g. enrolment of a new mobile phone);
    - issuance of a new SIM card by the phone company in connection with an enhanced SMS-type strong authentication solution;
    - input of login information by a third party and/or on a terminal not identified as belonging to the user (case of strong authentication solutions requiring authentication data to be entered on the payment page).

- **The transaction's parameters, aimed at identifying to what extent the user was or was not the source of the transaction:** this analysis is needed to distinguish, on the one hand, cases potentially connected with a commercial dispute rather than means of payment fraud (in a commercial dispute, the transaction was initiated by the user), and on the other, cases where the transaction was clearly initiated by someone other than the user (although the user may be contacted by the fraudster when authentication takes place).

- **Elements relating to the context of the transaction**, including **the quality and exhaustiveness of information supplied by the PSP** when the transaction was authenticated or via real-time alert mechanisms, as well as **elements reported by the user (cf. Recommendation No. 8)**.

Recommendation No.6: principles applicable to transactions subject to strong authentication

When a customer disputes a payment transaction that they deny having authorised and where this transaction was subject to strong authentication, the payment service provider shall carry out an initial analysis of the transaction within one business day. Taking into account the three

[7] The rules specify that reimbursement must take place immediately upon learning about the transaction or being informed about it and in any case no later than the end of the first business day following the date on which the dispute was submitted, and should include any additional fees incurred on a transitional basis as a result of recognition of the fraudulent transaction, such as overdraft fees or loan interest.

sets of parameters mentioned below, this analysis shall seek to assess whether it is likely that the user consented to the transaction or whether the transaction was unauthorised:

- **technical parameters associated with the transaction,** such as the source of the transaction, the terminal used for the purchase or to log on to online banking, and the geographical location, to determine the likelihood that the user was the source of the transaction;
- the **strong authentication procedures applied,** such as the type of solution, the integrity of authentication factors and the communication channel, proof that the user employed the solution in the past or conversely that enrolment occurred recently, to check the user's effective role;
- **available contextual elements**, such as the information provided to the user at authentication (cf. Recommendation No. 11), any alerts linked to the transaction and sent to the user through various communication channels, or the elements reported by the user (cf. Recommendation No. 8), including any manipulative processes encountered**.**

Following this initial analysis:

- **either the payment service provider finds that the transaction was unauthorised or has doubts about whether consent was given for the transaction, in which case it shall promptly[8] reimburse the transaction;**
- **or the payment service provider has good reasons to suspect fraud by the user[9] and shares these reasons with the Banque de France, in which case it may refuse to reimburse the transaction immediately, under the conditions provided for by Recommendation No. 3;**
- **or the payment service provider has enough evidence to consider that the transaction was authorised by the user[10] or that the user was grossly negligent[11] or deliberately failed to fulfil their obligations, in which case the provider may refuse to reimburse the customer for the disputed transaction, under the conditions provided for by Recommendation No. 3.**

In the first two cases, and based on the same abovementioned criteria and any new elements provided by the user, the payment service provider is encouraged to continue its investigations, if need be, under the conditions provided for by Recommendations No 1 to 3 to determine the user's right to be reimbursed.

References: Articles 73 and 74 of PSD2

5- RECOMMENDATIONS FOR CONSUMERS AND THEIR REPRESENTATIVES

5.1 Best practices for the security of means of payment

[8] The rules specify that reimbursement must take place immediately upon learning about the transaction or being informed about it and in any case no later than the end of the first business day following the date on which the dispute was submitted, and should include any additional fees incurred on a transitional basis as a result of recognition of the fraudulent transaction, such as overdraft fees or loan interest.

[9] As defined by Article 73 of PSD2.

[10] As defined by Article 64 of PSD2.

[11] As defined by Articles 73 and 74 of PSD2.

Given the ingenuity of fraudsters, as they seek ways to get round increasingly sophisticated security solutions, consumers have, through their vigilant and responsible behaviour, a key role to play in maintaining the security of their own means of payment.

Particularly when it comes to online practices, consumers need to protect the data associated with their means of payment and avoid divulging them to third parties, which could enable fraudulent attacks to be carried out. These data are just as sensitive as a payment card's PIN, and failure to comply with these best practices could be a factor taken into consideration when characterising negligence on the part of the user.

Recommendation No.7: best practices for the security of means of payment

Consumers must endeavour to be vigilant in protecting the security data associated with their payment instruments (password, PIN, security code), by observing the following best practices:

- **never share these data with a third party;**
- **do not keep these security data on any kind of physical medium (notebook, post-it) or electronic medium (email, hard drive, mobile device);**
- **never respond to contact from people purporting to be employees of payment service providers, such as a bank adviser or the anti-fraud department. Always use a secure and known channel to make contact with a payment service provider. Never open a link sent by email or SMS if you are not sure of the source;**
- **never give your payment instrument to another person (relative, courier);**
- **pay attention to security-related communications from your payment service provider and the authorities.**

Remember that employees of a payment service provider will never be required to ask for this information when calling a customer and do not need it to cancel a fraudulent transaction.

Consumers are also encouraged to prioritise the safest authentication solution offered by their payment service provider, if they are able to use it. These are generally solutions based on a robust hardware element, such as the banking app on a smartphone (the most widespread solution in France), or a standalone physical device provided by the payment service provider, such as a card reader or USB key.

References: Article 69 of PSD2

5.2 Transparency when reporting cases of fraud

The fight against fraud, no matter what the type of transaction, requires all stakeholders, including users of means of payment who are the victims of fraud, to cooperate and be totally transparent when describing the facts of fraud cases. Exhaustive information must be passed on in order to review the case, but also to identify the perpetrators and take criminal action against them, and to improve the anti-fraud screening mechanisms used in the payment industry. It is also critical to enhancing the warnings issued to consumers, thereby helping to raise awareness among payment service users.

In France, the Perceval and Thésée platforms[12] are the preferred means of making contact with law enforcement, in order to facilitate investigations. Furthermore, remember that a PSP cannot require a user to file a complaint as a pre-requisite for reviewing a reimbursement request.

Recommendation No.8: duty of fraud victims to be transparent

When filing statements with their payment service provider or law enforcement (whether using the online Perceval or Thésée platforms or filing an in-person report at a law enforcement facility), **consumers and their representatives must provide all the elements in their possession about the fraud to which they fell victim.**

In particular, users shall take care to provide all available information on:

- **The nature and background of the transaction:** for example, how much they know about the payee, the technical or manipulative methods that the fraudster allegedly used, the instrument and terminals used for the payment transaction, messages or calls received, steps taken because of manipulation by the fraudster, etc.
- **Steps taken once the fraud was discovered:** such as blocking the instrument, contacting law enforcement through the Perceval or Thésée platforms (provide receipt), filing a complaint with law enforcement, etc.

The treatment of fraudulent transactions by PSPs typically includes several levels of appeal:

- the initial dispute should be sent to the customer advisor at the account-keeping institution, who acts as the primary contact person for the user, or submitted in accordance with the dispute procedure specifically provided for by the institution, for example via online banking;
- if an unsatisfactory response is obtained, the user files a complaint with its PSP;[13]
- finally, the customer may contact the ombudsman named by the PSP.

The customer may also take legal action at any time after the initial dispute is rejected.

6- RECOMMENDATIONS AIMED AT PREVENTING FRAUD

6.1 Checking customer accounts using online banking or a mobile application

In one currently observed fraud scenario, fraudsters employ phishing techniques to obtain a customer's online banking login and password along with private information, such as first and last name and phone number.

Using this information, the fraudster logs in to the customer's online banking space to gain information about the products held by the customer and the latest account information, such as the current balance and recent transactions. At that point, the fraudster can contact the customer, posing as the

[12] Perceval is a remote service used to report online bank card fraud to law enforcement; Thésée is a platform for filing online complaints about internet scams, especially where credit transfer fraud is involved.

[13] If the user appeals against the financial decision by the PSP following the dispute, ACPR Recommendation 2022-R-01 of 9 May 2022 on the treatment of complaints becomes fully applicable and supplements these Recommendations. https://acpr.banque-france.fr/sites/default/files/media/2022/05/17/20220517_Recommendation_2022-r-01_traitement_reclamations.pdf

PSP. The scam is made credible because the criminal holds specific bank information about the customer that a third party would not be expected to know. Once their trust is won, the customer will be inclined to agree to the fraudster's request to validate transactions (add payee, issue credit transfer order) by means of strong authentication.

This type of scenario could be prevented by applying strong authentication every time online banking is accessed, except where the connection is made from a teminal that is regularly used by the user and the most recent connection using strong authentication occurred in the last 180 days.

Recommendation No.9: apply strong authentication when accessing online banking from a new internet access point or a new terminal.

Payment service providers are encouraged to require strong authentication when accounts are accessed via online banking or a mobile application from a terminal and/or an internet access point that was not previously used by the customer.

6.2 Information provided to the customer when a credit transfer payee is added

Under current payment security rules, the names of credit transfer payees do not have to be systematically checked: a credit transfer order can be executed as long as the payee's bank account number (IBAN) is valid, the payee account exists and has not been closed, irrespective of whether the name of the payee provided by the payer matches the name of the actual account holder.

Some fraudsters have exploited this situation. For example, in an “IBAN swap” scam, the fraudster sends the IBAN for an account that it holds (or that is held by another party who is an accomplice to the fraud) but associates that number with the name of a trusted payee, such as the Treasury or a notary.

When adding a payee, the issuer of a credit transfer is asked to enter the payee’s name. Some institutions even say on their online banking site or mobile application that checking the IBAN can take up to several days. The issuer of the credit transfer may thus wrongly believe that the names are being checked to see if they match and that the credit transfer will not be executed or could be cancelled by the payer if the actual holder of the payee account does not match the name entered when adding the account's IBAN.

This situation is however set to change in the coming years: in its proposal to revise the Regulation on a Single Euro Payments Area (SEPA),[14] the European Commission proposes to increase trust in instant payments, with an obligation on providers to verify the match between the bank account number and the name of the beneficiary provided by the payer in order to alert the payer to a possible mistake or fraud before the payment is made.

Recommendation No.10: procedures for registering IBANs of credit transfer payees

Whenever a credit transfer payee is added, payment service providers are encouraged to clearly indicate whether the match between the IBAN and the payee name was checked. Otherwise, the user should be informed that the “Payee name” field is exclusively intended to make it easier for customers issuing credit transfers to track transactions and that its content is not checked to ensure that it matches the identity of the holder of the payee IBAN.

[14] Legislative proposal of 26 October 2022 (2022/0341 (COD)) to make instant payments in euro accessible to all individuals and businesses with bank accounts in the EU or in an EEA country.

Payment service providers based in France are additionally encouraged to be proactive in exploring the possibility of promptly implementing a payee confirmation service as described by the European Commission in its proposal to revise the SEPA Regulation.

6.3 Information and options presented to the payment service user during strong authentication

In the event of fraud through manipulation, the fraudster relies on its hold over the victim to persuade that person to ignore messages and warnings sent by the payment service provider. This task is made easier when these messages and warnings are insufficiently precise and exhaustive concerning the nature and characteristics of the transaction awaiting validation. Making the information provided more explicit and exhaustive, and strengthening the choice given to the user during the authentication process, would be effective in helping to prevent manipulation-based fraud.

Recommendation No.11: information and options offered to users during strong authentication

At each stage in the authentication process, payment service providers should endeavour to provide users with explicit information about the nature of the transaction, mentioning in particular the amount, the payee, whether the transaction is a one-time or recurring transaction, the frequency in the case of a recurring transaction and the irrevocable nature of a validated payment order. In the event of a first credit transfer to a given account, if the match between the name of the payee and the bank account number provided is not checked, this should be explicitly stated during the authentication process.

Furthermore, payment service providers should make sure that the authentication process offers an explicit option allowing the user to refuse the transaction.

6.4 Ease of access to procedures to block payment instruments

If users notice unusual activity on their accounts or payment instruments or identify gaps in their data protection, they should be able to block affected payment instruments through their PSP. This procedure should be easy to access to promote the swiftest and most effective response, along the lines of France's national stop payment call centre for payment cards.

Recommendation No.12: ease of access to procedures to block payment instruments

Payment service providers should provide users with mechanisms allowing them to block each of their payment instruments. These mechanisms must be easily accessible, free of charge and always available.

References: Articles 69 and 70 of PSD2

6.5 Role of information services and technology providers in fraud prevention

Phone companies and digital service providers are key stakeholders in the security of remote payment transactions, as they put the different parties in contact and handle data exchanges. Accordingly, they have a responsibility to help fight the techniques used by fraudsters to gather payment data without the user's knowledge, including phishing and smishing (sending emails or SMS text messages that purport to be from a legitimate party), spoofing (having the phone number of a legitimate caller appear on caller ID when making a scam call) and setting up fake mirror sites.

Recommendation No.13: role of information services and technology providers

Participants from the information technology sector, such as phone companies, content hosters, publishers of online directories, search engines and messaging service providers, should seek to protect users against the risks of identity theft and threats to the integrity and confidentiality of their data. They should endeavour to prevent the use of fraudulent techniques such as phishing, spoofing and SIM-swapping.

7- How to apply these Recommendations

The Observatory's 13 Recommendations set out best practices for payment market participants and detail the expectations of the French authorities with regard to European regulations. They are not intended to replace the applicable regulations or previous legal rulings in this area.

Payment service providers undertake to take Recommendations 1 to 6 into consideration in their practices for handling disputes involving unauthorised payment transactions, and all participants undertake to play a proactive role in payment security by endeavouring to apply Recommendations 7 to 13, where applicable, in the day-to-day running of their business.

At a time when fraud mechanisms are evolving at a rapid pace, the Observatory undertakes to review these Recommendations and, if necessary, to revise them within a maximum of 18 months from their adoption.