GENERAL SECRETARIAT

Anti-Money Laundering and financing of Terrorism Directorate

Policy, Coordination and Analysis Division

Report on the prevention of the use of rebound accounts for laundering the proceeds of scams and other frauds

Areas of vulnerability requiring particular attention from the financial institutions most exposed to this risk

July 2025

In 2024, the AML/CTF Directorate of the Autorité de contrôle prudentiel et de résolution (ACPR - AML/CTF Directorate) conducted a thematic study on French accounts receiving transfers suspected of being the proceeds of scams or frauds between 2022 and 2023, and on AML/CTF systems set up by financial institutions under its supervision to address the money laundering risks associated with such schemes.

This study was based on an analysis of data provided by a sample of financial institutions particularly exposed to this risk, supplemented by interviews or on-site inspections. This included an analysis of qualitative and quantitative information on their internal frameworks and experience in dealing with this risk. The ACPR also collected, for each institution, a sample consisting of the 50 largest cases by amount over a certain period.

The analysis of the case studies makes it possible to identify areas of vulnerability that are exploited by illicit actors to channel the proceeds of scams and frauds through bank or payment accounts for laundering purposes ("rebound accounts"[1]). For example, a rebound account can be used to receive one or more transfers initiated by a victim of fraud or scam. Then, the funds received can be swiftly transferred through one or more debit transactions, either simultaneously and / or successively, to one or several accounts held abroad. These operations aim to conceal the proceeds of fraud or scam and prevent administrative, civil or criminal proceedings (e.g. recalls, right of opposition, seizure by authorities). Examples have been provided by Tracfin[2], notably in its information report on the evaluation of the fight against financial criminality[3].

Based on this assessment, a non-exhaustive list of points of attention or best practices can be drawn up. The document outlines the main points of French and European AML/CTF regulation and guidance. Embedding these points of concern may help financial institutions particularly exposed to this risk to assess and, where appropriate, improve the effectiveness of the procedures and frameworks they have in place to prevent the products and services they offer from being used as money-laundering vehicles or as rebound accounts.

The report was shared within the ACPR's AML/CTF Consultative Commission to raise awareness among professionals about the risks of rebound accounts and enrich the study with their experiences.

However, the best practices and areas of concern identified in this study are primarily addressed to the financial institutions most exposed to this risk. A high number of recalls related to fraud, suspicious transaction reports, judicial requisitions – or a significant year-on-year increase in such requests – are key indicators to be taken into account when assessing the level of exposure to this risk.

[1] Any account that can receive funds can be used as a rebound account.
[2] In French, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2015, Tracfin.
[3] In French, Rapport d'information n°1822 sur l'évaluation de la lutte contre la délinquance financière, 28 mars 2019.

Overview of areas of concern for financial institutions particularly exposed to money laundering risks through rebound accounts

In terms of governance, financial institutions whose activities present a high money-laundering risk related to the use of accounts to channel illicit funds, should ensure that their risk management framework is adapted to prevent their services from being used by criminal networks to launder the proceeds of frauds or scams. This entails the monitoring of Key Performance Indicators and Key Risk Indicators by senior management, which materialize the risk appetite. These indicators should provide an overview of the size and proportion of funds flowing through these "rebound accounts". Furthermore, when major deficiencies exploited by a criminal network are detected[4], the financial institution should consider taking swift actions such as suspending the relevant products and processes until the necessary corrections are implemented. (technical access controls, product adjustments, additional checks for the customers concerned).

The intensity of criminal organizations' efforts to open or mobilize rebound accounts used to launder the proceeds of scams or frauds is very high: creation of short-lived companies, usurpation of real identities, use of fake identities, or the purchase of existing companies or the use of 'mules' (initially legitimate customers who lend or sell their accounts for laundering purposes). While the study cannot determine how frequently each technique is used, several examples show that these criminal networks know how to take advantage of new generative artificial intelligence technologies to circumvent the usual identity verification measures (use of *deep-fakes*). The study also shows that significant amounts are laundered through recently created companies.

When onboarding new customers, and based on risks, financial institutions should, where appropriate, combine several identity verification measures and rely on supporting documents collected from reliable independent sources. For instance, when onboarding a legal person remotely, FIs should systematically collect supporting documents from the commercial register and carefully verify the identity and powers of the representative acting on behalf of the legal person customer. Measures should also be taken to detect potential mules, examining weak signals that may indicate changes in operations or in the devices, or more generally changes regarding where and how users connect to online financial services. These measures would not eliminate any money-laundering risk related to the use of rebound accounts but would reduce it.

Effective mitigation also requires to take into account the risk associated with the use of rebound accounts in the design of financial products and services. The range of financial products and services offered should match the customer profile, particularly at onboarding. This could include setting transaction ceilings (unitary and cumulative) tailored to the verified customer's business or income, to ensure that the nature and amounts of transactions are consistent with the customer's business and profile. Such ceilings could thus limit of the flows of suspicious money through these accounts (credit transfers, bank cards, etc.) and allow, when required under Article L.561-10-2 of the French Monetary and Financial Code, to conduct enhanced due diligence of transactions exceeding the

[4] For example, one financial institution identified multiple cases of deep-fake and temporarily suspended onboarding through the affected process until a patch was implemented.

ceilings. More generally, the European Banking Authority (EBA) guidelines on risk factors require financial institutions to define, based on risks, transactions that should be monitored in real time[5].

The risk of laundering the proceeds of frauds and scams should also be reflected in the business wide risk assessment and the individual customers' risk profile, as well as more generally in the risk management framework. This should ensure effective risk-based due diligence. Thus, for high-risk clients, additional measures may be necessary to achieve an accurate assessment of the customer's profile and to determine the expected transactions (for example, for a legal entity, expenses related to premises, staff, social and tax contributions, and more broadly the types of income and expenditure consistent with its business activity).

Adopting a risk-based approach, transaction monitoring systems may also include real-time monitoring capacities, in order to be able to suspend transactions until enhanced due diligence procedures are carried out and suspicions are lifted (see Sections 156 et seq. of the joint guidelines issued by the ACPR and Tracfin on due diligence on transactions and on reporting and information obligations to Tracfin, updated in 2025[6]).

Indeed, the enhanced transaction review is a crucial stage in this process. In case of suspicious transactions, an enhanced review should be carried out and, where appropriate, could lead the financial institution to check if other associated accounts had similar characteristics, taking into account all available data (same customers, beneficial owners or authorized representatives, connection devices, locations, contact points, dates or arrangements for opening the accounts, same source or destination of funds, etc.). If the transaction remains suspicious despite of the enhanced transaction review, a suspicious transaction report should be submitted to Tracfin without delay.

Finally, internal control and periodic audit can improve the reliability of risk-management frameworks. The review of suspicious transactions (statistics, high amounts, outstanding cases) may reveal temporary or structural, as well as technical or human deficiencies in AML/CFT systems. These deficiencies should be corrected to reduce the risk that the services offered by financial institutions could be exploited by criminal networks.

***

[5]Paragraph 4.74 of the EBA Guidelines on the risk factors mentioned above: "Financial institutions should deter mine: (a) which transactions they will monitor in real time and which transactions they will monitor ex post. As part of this, financial institutions should determine: i. which high risk factors, or combination of high risk factors , will always trigger real time monitoring; and ii. which transactions associated with high ML/TF risk will be subj ect to real time monitoring, in particular those for which the risk associated with the business relationship is alr eady increased". In addition, pursuant to Article 2 of the Arrêté of 6 january 2021, the design of new products a nd services must be accompanied by an assessment of the ML/TF associated risks
"in order to take appropriate measures to manage and mitigate these risks", see Section 158 et seq. and Box 15 of the joint guidelines issued by the ACPR and Tracfin on due diligence on transactions and reporting and infor mation obligations to Tracfin, published on April 23, 2025.

[6] In French : Lignes directrices conjointes de l'ACPR et de Tracfin relatives aux obligations de vigilance sur les opérations et aux obligations de déclaration et d'information à Tracfin | Autorité de contrôle prudentiel et de résolution

Table of content

List of best practices and points of concern drawn up by the ACPR and financial institutions 6
CHAPTER 1: Background and scope of the study 12
CHAPTER 2 - General elements 15
2.1 Volume of suspicious transfers / General statistics 15
2.2 Outstanding features of particularly exposed financial institutions 16
2.3 Outstanding features of accounts receiving suspicious transfers 17
CHAPTER 3 - Detailed study of 650 business relationships 19
3.1 Suspicious incoming flows to the accounts of the 650 business relationships analysed 19
3.2 Destination of outflows 21
3.3 Age of accounts receiving suspicious transfers 23
3.4 Features of business relationships holding rebound accounts 23
CHAPTER 4 - Overview of identity verification practices 25
4.1 Identity verification procedures applied to private individuals and representatives of legal entities 25
4.2 Identity verification procedures applied to legal entities 27
CHAPTER 5 - Overview of customer onboarding frameworks 28
5.1 KYC at onboarding: risk classification 28
5.2 The collection of supporting documents corroborating the information reported by the customer 30
CHAPTER 6 - Overview of systems and practices for detecting suspicious transactions 32
6.1 Responsiveness of financial institutions following an alert 32
6.2 Transactions monitoring system 32
CHAPTER 7 - Overview of the integration of money-laundering risk into governance, organisation, and internal controls 35
7.1 The framework for managing money-laundering risk 35
7.2 The resources devoted to onboarding 35
7.3 Financial Products Design 35
7.4 Lessons learned by financial institutions that could reduce the laundering of scams and fraud 37

List of best practices and points of concern drawn up by the ACPR and financial institutions

This section outlines the best practices and points of concern identified during the review and shared with financial institutions and the ACPR's AML/CFT Consultative Commission. These are primarily intended for financial institutions that are particularly exposed to the risk examined in this review, but they may also more broadly inform sector-wide efforts. A more detailed analysis, as well as comparative insights, is provided in the following chapters.

1. Due diligence management

- As part of a risk-based approach, the risk of accounts being used to launder the proceeds of fraud or scams should be specifically considered and monitored by the relevant business lines and management functions, up to the level of the governing bodies where appropriate.

- Take into consideration the risk of fraud laundering or scam laundering in the business-wide risk assessment and ensuring that the customer risk rating take this risk into account.

- Adjust the framework continuously and as quickly as possible when new fraud schemes appear or when major weaknesses exploited by a criminal network are detected. In such cases, the financial institution should rapidly take the necessary corrective actions (including suspending faulty processes or reviewing all business relationships that have been established on the basis of a system that has proven to be flawed, prioritizing the higher[7] risk business relationships and, where appropriate, implementing additional due diligence measures such as for example a limit on the volume of transactions, or even suspending the business relationship).

- Ensure sound risk management when commercial strategies aim for rapid growth in the number of accounts.

- Establish performance indicators (KPIs) and an internal monitoring system to improve the processing of recall requests or seizures by authorities related to fraud or scams and use such information to improve the risk management framework (see the following point)

- Periodically carry out an ex post analysis of major recall or seizure cases (by internal control or internal audit), to ensure independently that the systems are operating properly.

2. Onboarding and identity verification

Due diligence is recommended when onboarding new customers to identify any risk that the account could be used by the customer as a rebound account.

[7] Application of at least the measures planned in paragraphs 18 and 19 of the EBA Guidelines on the use of solutions for establishing non-face-to-face business relationships; see Guidelines EBA/GL/2022/15 of 22 November 2022 (GL remote customer onboarding solutions (EBA GL 2022 15)_FR_REV.pdf)

- Implement at least two verification measures in case of remote onboarding (Article R. 561-5-2 of the CMF). Pursuant to Article L. 561-1-10 of the CMF, "*when the risk of money laundering and terrorist financing presented by a business relationship, a product or a transaction appears high to them, the persons mentioned in Article L. 561-2 shall implement the provisions of Articles L. 561-5, L. 561-5-1 and L. 561-6 in the form of enhanced due diligence measures*". Therefore, in case of high risk, financial institutions could choose a higher number of measures and strengthen the conditions for the implementation of such measures, taking into account the EBA Guidelines on the use of remote[8] customer onboarding solutions (including on the selection and monitoring of such solutions). Obliged entities should also take into account the specific vulnerabilities of each verification method (including the examples below).

- Regarding the ID verification measure consisting of requiring that the initial transaction crediting the account comes from another account in the name of the customer, it should be borne in mind that:
  - the first card payment can be accepted only if "the financial institution ensures (i) that the card is not attached to an electronic wallet and (ii) that the holder of the card is indeed the holder of the payment account used. (cf. ACPR[9] guidelines);
  - the risks of a failure of identity verification by the payment service provider from which the first transaction crediting the account originated (accounts maintained by providers known to the institution for their failures in identity verification or for above-average fraud rates)[10];
  - that the provision of card-based payment into an account is subject to the transparency obligations related to transfers of funds, in particular to the disclosure of the name of the payer by the payment service provider of the payer (Article 2§3 of EU Regulation 2023/113 of 23 May 2023).

- Ensure that the person requesting the opening of the account is the holder whose identity is being verified, and if not, verify the powers and identity of the third party acting on behalf of the customer under Article R. 561-5-4 of the CMF: some measures in Article R. 561-5-2 are insufficient in this respect, and using a remote identity-verification provider certified compliant by the French Cybersecurity Agency (ANSSI)[11], appears to be a good practice.

- Adjust to the risk level of the account opened the way legal acts or extracts from the official register are obtained t, so as to avoid the risk of falsification. When onboarding remotely, the extract from the register may be verified or certified by a third party independent of the person to be verified (Article R. 561-5-2). The certified copy may be obtained directly through the commercial register, as provided for in Article R. 561-5-1. It should also be noted that verifying the identity of the legal person (including certifying an extract from the register referred to in point 2 of CMF Article R.561-5-2, including the name of the representative) does not constitute a measure to verify the identity of persons acting on behalf of the legal person required by Article R. 561-5-4: financial institutions should in particular pay close attention to the risk of identity fraud of legitimate companies and their representatives.

[8] see Section 38 et seq. - Guidelines EBA/GL/2022/15 of 22 November 2022
[9] see ACPR guidelines on customer identification, verification and KYC, 16 December 2021, §46, p.14
[10] see ACPR's Sectoral Risk Analysis, p. 26 and Chapter 4 of this report.
[11] Prestataires de vérification d'identité à distance (PVID) | ANSSI

3. Customer knowledge

Opening payment accounts to new customers exposes financial institution to the risk of laundering the proceeds of fraud or scam, the level of which must be assessed following a risk-based approach and taking into account analyzes conducted by the Conseil d'Orientation de la Lutte contre le Blanchiment (COLB – French national AML/CFT steering committee), the ACPR and the financial intelligence unit Tracfin.

- Professional activity and financial situation: The customer's occupation and/or function, income or resources are "*essential information for the purpose of ongoing due diligence*". Information on wealth may also be required in some cases[12].

  The collection of information related to the customer's financial situation may be carried out in the form of income brackets, provided that they are sufficiently precisely defined or adapted to customer characteristics. It is not sufficient for a high-risk profile.

  For corporate business relationships, the information to factor in should include annual accounts, tax return as well as key suppliers and customers.

  As mentioned in Section 142 of the abovementioned guidelines, "*For newly established companies that do not have information on their financial situation, financial institutions shall collect, for example, a forecast balance sheet and the expected volume of customer/supplier billing, the average monthly level of expense, the professional background of the manager and any associates, and the material, financial and human resources used to set up the business*."

- Justification of the address of domicile or head office in the following cases:

  - in the event of high risk (Articles R. 561-12 of the CMF and [1] of the Arrêté of 2 september 2009 taken for its application), the internal procedure of financial institutions must determine the cases in which the justification of the address of domicile must be collected and, in this case, the type of evidence to be collected.

  - where the address is to be provided in a transfer of funds pursuant to Regulation (EU) 2023/113 of 23 May 2023 on the information accompanying transfers of funds)[13].

- Other elements of customer knowledge: The nature and extent of the information collected, in the case of opening an account in a high[14]-risk situation, must be adapted, in particular (see aforementioned 2009 Order):
  - Amount and nature of planned transactions
  - Source of funds: e.g. source IBAN, if not available type of source, country, ...
  - Destination of funds: e.g. amount and nature of expected expenditure, geographical destination.

[12] In French : 20220404_lignes_directrices_revisees_relatives_identification_verification_connaissance.pdf
ACPR guidelines on customer identification, verification and KYC, 16 December 2021, §133, p.31

[13] Article 4(5) allows the verification not to be repeated at each transfer, but should, if the address is mentioned in the transfer, have been one of the elements verified when onboarding. The presumption laid down in that provision does not seem to apply if the financial institution is aware that the information is incorrect because of the updates that have since taken place based on risk or other factors (e.g. undelivered mail, IP addresses that never correspond to the known postal address).

[14] High risk is assessed based on all the factors mentioned in Article L.561-4-1 of the CMF, and not solely on the level of customer risk.

- Use robust supporting documents less exposed to identity fraud. Thus, when onboarding remotely, financial institutions may, for the purposes of combating document fraud:

  - Collect a proof of domicile with a 2D-Doc bar code to check the integrity of the document and the information it contains[15],

  - Use *open banking* (direct access to information on the customer's other accounts according to the account information service provided by the Directive on payment services),

  - Send letters with some form of acknowledgement of receipt.

- Best practices for dealing with high risk include, following a risk-based approach, open[16]-source research on the customer's counterparties or checking that the purpose of the company is consistent with the operation of the account (rents, salaries, social security contributions, taxes, business-related suppliers, geographical areas of origin and destination of funds).

- When combined with other risk factors, multi-banking should be considered as a factor likely to increase the risk justifying the implementation of enhanced due diligence (Article L. 561-10-2 of the Code monétaire et financier).

- When onboarding, establish and update the risk profile of the business relationship according to a determined frequency adapted to this risk profile, factoring in all the information collected, so that it can be taken into account when performing ongoing due diligence.

4. Detection of atypical transactions through monitoring systems

- Factor in KYC information for scenario setup. In accordance with the ACPR - Tracfin[17] guidelines, "*as part of the tool settings, financial institutions should ensure that the thresholds and/or the period of transactions under review are likely to detect inconsistencies with regard to:*
  - the transaction profile expected by the business relationship or the transaction history actually performed by the customer (where this history is consistent with the knowledge of the customer);
  - where applicable, information planned by the Arrêté of 2 september 2009 taken in application of Article R. 561-12;
  - where applicable, the characteristics of the corresponding peer group transactions, such as the average transaction value."
  The monitoring system should make it possible "*to detect, for example, a total amount of transactions over a given period (month, year) that is unusual or inconsistent with the customer's income or turnover, a typology of transactions that is atypical in relation to the customer's profile, and unexpected counterparties in relation to their geographical location, number or nature*".

[15] In French, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, §131, p.30

[16] *see §21 of the ACPR - Tracfin guidelines updated in 2025 "Financial institutions collect relevant information on knowledge of the business relationship and, where applicable, of the beneficial owner, from the customer but also from third parties. Pursuant to Articles R. 561-38 and R. 561-38-1, they shall identify reliable sources of information among the media, information published by the authorities or provided by call for vigilance/caution, and databases of third parties that may supplement or confirm knowledge of the customer*'.

[17] see Section 38 et seq. of the joint ACPR and Tracfin guidelines on due diligence on transactions and reporting and information obligations in Tracfin, 22 January 2025

- For the payment service provider holding the rebound account, verify that the name of the beneficiary of a credit transfer matches the name of the holder of the account receiving the transfer. A significant discrepancy, despite the provision of a verification service (see Regulation EU 224/886 of 13 March 2024 on instant transfers in euro), is a risk factor.

- Implement automated tools to suspend transactions within a short period of time, or even before execution, following a risk-based approach. Financial institutions should define the transactions they monitor in real time and those they monitor after completion, in line with their risk level (see paragraph 4.74 of the EBA Risk Factors Guidelines), as well as the risk factors (combined or not) that should trigger ex ante monitoring.

- Put in place ceilings on the amounts of transactions that can be executed by a customer without the intervention of staff, to reduce the increased risk of payment accounts being used for money laundering purposes in a remote business relationship environment and transaction immediacy.

- Factor in the technical modalities for accessing products and services offered remotely to facilitate the detection of illegitimate uses of financial institutions' services (usurpation, use of mules through the use of the account or means of payment of third parties with or without their consent, etc.).

  The implementation of biometric security procedures when activating the application for access to payment services mitigates the risks that financial services be used by third parties.

  A change of connection device or an atypical place of access to services may, where appropriate, when combined with other weak signals and/or alert criteria, justify an enhanced transaction review (with manual validation or updating of the customer knowledge).

5. Enhanced transactions reviews

- Ensure swift enhanced transaction review measures and, where necessary, the suspension of debit transactions in the event of transactions that do not appear to have a lawful purpose. As indicated below, allowing the possibility to suspend outflows in the event of a high-risk typology makes it possible to carry out the enhanced transaction review, and where appropriate to report to Tracfin, before carrying out the operation.

- If an account is suspicious, check during the enhanced transaction review that other accounts with similar characteristics (same customers, beneficial owners or authorized representatives, connection devices, locations, contact points, dates or procedures for opening accounts, same source or destination of funds, etc.) would not also be suspicious.

6. Product and service design

- Adjust the range of financial products and services offered to reflect the profile of the business relationship, in addition to the configuration of the monitoring system, to prevent the execution of atypical transactions that require an enhanced transaction review.

  The best practices consisted in adapting the products' features (maximal withdrawal amounts, credit card limits, transfer ceilings in number and value) to the profile of the business relationship (activity, expected counterparties, number of accounts or means of payment expected), its

duration (lower ceilings during the first months of account operation) and its financial behaviour (account record, transaction frequencies).

As mentioned in Section 158 of the 2025 ACPR - Tracfin Guidelines, “pursuant to Article 2 of the Arrêté of 6 january 2021, the design of new products and services must be accompanied by an assessment of the ML/TF risks linked to them “in order to take appropriate measures to manage and mitigate these risks”. Contractual clauses may therefore reserve the possibility of such manual validations by the financial institution’s staff, where appropriate after enhanced transaction review.

CHAPTER 1: Background and scope of the study

This study is based on data provided by 13 financial institutions supervised by the ACPR particularly exposed to the risk of laundering of proceeds from fraud or scams through suspicious credit transfers, particularly in light of data collected in 2022 by the Observatory for the Security of Means of Payment (hereafter "OMSP").

This study was conducted in the context of a significant rise in scams and other fraud and the growing involvement of French accounts in the laundering of their proceeds. This work is intended to complement recent analyses of victims by other French organizations, within the scope of their tasks.

➢ A significant increase in the laundering in France of the proceeds of fraud and scams

Crime statistics show that scams and fraud cases in which the proceeds of the fraud are credited to an account following a non-cash payment **increased rapidly in France between 2016 and 2023, both in volume (64%) and in amount (100%).** According to a July 2024 report by the Ministry of the Interior's Statistical Service (SSMSI), based on complaints to the police and national gendarmerie for this type of fraud, **the number of victims reached 411,700 in 2023.**

Furthermore, only one in ten victims files a complaint, so that, taking into account victim surveys, the SSMSI estimates that the amounts of scams and fraud doubled between 2016 and 2023, to reach EUR 4.5 billion in 2023, mostly to the detriment of natural persons and to a lesser extent legal persons (EUR 600 million to EUR 800 million)[18].

These scams and fraud can take many forms, including financial scams, romance scams and means of payment scams.

According to a survey conducted for the French Financial Markets Authority, the share of French victims of financial investment scams almost tripled in three years (3.2% in 2024 compared with 1.2% in 2021).[19] The Paris public Prosecutor's Office estimates that the overall losses suffered by victims of financial scams in France amount to at least EUR 500 million per year. These scams generally involve making transfers to an account controlled by the scammer.

Payment fraud, in particular credit transfer fraud, has increased sharply both in terms of value and volume in recent years. The Banque de France recorded EUR 311.6 million credit transfer frauds in 2023 through the OSMP[20], four times more than in 2016. While the value of fraud is slowing down, the number of fraudulent transfers is rising sharply (+200% compared with 2021, for a total of almost 90,000 transfers), and the average amount of a fraudulent transfer has been divided by four in five years to reach EUR 3,446 in 2023. Victims are increasingly private individuals.

Credit transfers initiated by victims are now sent to French accounts for 65% of their value, whereas until 2018, more than two thirds of their amounts corresponded to transfers abroad. As a result, fraud laundering through French IBAN transfers has increased almost eightfold in six years, from EUR 26

[18] combining complaints with the results of victimization investigations

[19] https://acpr.banque-france.fr/fr/communiques-de-presse/arnaques-financieres-les-autorites-mobilisees-dans-la-lutte-contre-ce-phenomene-massif-qui-piege-de

[20] Based on updated data published in September 2024.

million in 2017 to EUR 203 million in 2023, in terms of the amounts reported to the Banque de France by the victims' payment service providers.

The total amount of fraud and scams involving a transfer from a French victim to a scammer was estimated at around EUR 1.3 billion in 2023[21], excluding social and tax fraud.

➢ Scope of the ACPR's thematic study: selection of financial institutions surveyed

In addition to the above analysis and on-site inspections conducted in half a dozen financial institutions that are particularly involved in receiving suspicious credit transfers, the ACPR decided to conduct a simultaneous cross-sector review of 13 institutions. Indeed, as corrective actions were taken in some cases, the money laundering flows shifted to other financial institutions**.**

The aim of this study is twofold:

- Identifying risky practices, and conversely good risk management practices, in order to **conduct awareness-raising initiative** on all exposed institutions and limit the shifting of risk;
- **Guide individual supervisory actions** and better identify early indicators that help to identify the actors most at risk so that they can intervene as quickly as possible.

The 13 institutions included in this study were identified through a questionnaire sent out by the Banque de France to a dozen major French banks. The questionnaire was designed to identify the main institutions receiving fraudulent credit transfers for which the customers of these major banks were victims**.** This survey showed that newly established institutions or institutions opening a large number of accounts seemed to be overrepresented in the receipt of fraudulent credit transfers (around 50% of the amount), as well as online service providers (around 35% of the amount). While some large traditional financial institutions are involved, their exposure to laundering of the proceeds of payment fraud is still far below that of others (as a proportion of the total value of credit transfers they receive).

In 2022, the 13 selected institutions (or their predecessors) had collectively received around 50% of the amount of transfers reported to the Banque de France by banks of victims of payment fraud in the survey mentioned above. Given the share of foreign players (not supervised by the ACPR) in receiving such transfers, these 13 institutions accounted in 2022 for almost 90% of the total number of transfers received by financial institutions supervised by the ACPR.

The 13 institutions were selected mainly on the basis of two criteria:

- The ACPR identified the 19 institutions that accounted for **at least 1% of the total value of credit transfers resulting from fraud** reported by the victims' banks in 2022. Then, financial institutions not supervised by the ACPR were excluded;
  The ACPR also identified the 10 institutions under its supervision with **the highest ratio between the value of fraudulent transfers and that of all transfers received in 2022**. This proportion ranged from 2.5% for the worst of the 10, to 1 per 1,000 for the best, while credit transfer fraud accounted in France in 2022 on average for €1 per €100,000 exchanged[22].

In total, the 13 institutions include 10 institutions that are mainly online and three that mainly distribute their services through physical branches.

[21] This estimate of EUR 1.3 billion is the result of applying to the EUR 5 billion estimated by the SSMSI, the proportion of credit transfers in payment fraud compared with other forms of payment (check, bank card). It is consistent with the amount of suspicious transfers identified by the 13 institutions covered by this study, as compared with their share of recalls.

[22] OSMP report for 2022

➢ Scope of the ACPR's thematic study: type of targeted transactions

This analysis focuses on the involvement of accounts held by financial institutions supervised in France, in the laundering of funds suspected of being the proceed of scams or fraud. These are accounts of French residents and accounts of foreign residents with a French IBAN. As we will see, in some cases the owners of these accounts are not necessarily money launderers, but sometimes they sell a good or service that will itself enable money laundering.

This study does not focus on transfers initiated by victims, but rather on the accounts receiving the transfers that the financial institutions responding to the survey have suspected:

- Of being fraudulent[23] (false transfer order, misappropriation or falsification of a regular payment order, payment order using a means of a payment under a false identity); these fraudulent transfers are those targeted by the studies conducted by the Banque de France on the security of means of payment;
- Or to be issued in the context of a scam (including, for example, public aid fraud, welfare fraud, romance scams, false investments, false online sales): the transfer order itself was deliberately initiated by the victim, but has been manipulated.

These flows will be referred to below as “suspicious transfers”.

Suspicions of money laundering or fraud can arise from the receipt of a recall request, a request by law enforcement or a request from the authorities, or the financial institution’s internal due diligence system. It may also result in the implementation of enhanced due diligence, in the drafting of a suspicious transaction report, or in the closing of the relevant account on the grounds of laundering of the proceeds of fraud or fraud.

The questionnaire used by the ACPR contained three categories of information:

- General statistical data for 2022 and 2023,
- Measures and procedures to reduce the risk of laundering the proceeds of scams or fraud (onboarding procedures, prevention of document fraud, transaction monitoring, enhanced due diligence and fund-blocking procedures, risk monitoring).
- A collection of 650 individual cases, corresponding to the 50 business relationships of the financial institutions surveyed that received the largest amount of transfer recall requests in 2023 on French IBANs.

[23] The survey data stem from the internal identification and monitoring work of the institutions consulted and cannot be considered exhaustive.

CHAPTER 2 - General elements

The following estimates reflect data reported by the institutions surveyed, which are based on their respective atypical transactions monitoring system. They may therefore vary according to the procedures and settings specific to the financial institutions surveyed.

2.1 Volume of suspicious transfers / General statistics

	2022	2023	Growth between 2022 and 2023
Gross amount of suspicious transfers	€457 million	€661 million	45%
Number of suspicious transfers received	510,392	757,432	48%
Average amount of a suspicious credit transfer received	€896	€873	-2.6%

In 2023, **EUR 661 million in credit transfers received were identified as suspicious** by the financial institutions surveyed. Despite significant disparities, the data provided by respondents are much higher than those obtained from the aforementioned Banque de France survey of the victims' banks conducted in 2022 (around EUR 156 million). Apart from the broader definition used in this study, this is partly due to the fact that the banks surveyed do not represent all the victims, and especially because the victims do not always ask for a transfer recall. This recall request appears to be one of the main markers allowing the victims' banks to identify the amounts involved. However, this amount is in line with the estimated EUR 1.3 billion resulting from the aforementioned SSMSI victimization surveys, assuming that the thirteen financial institutions in the sample account for half[24] of the laundering of fraudulent credit transfers.

The total amount of suspicious transfers received by the financial institutions surveyed increased by more than EUR 204 million between 2022 and 2023, from EUR 457 million to EUR 661 million (representing an increase of 45%). The number of business relationships identified as receiving at least one suspicious credit transfer increased by 31% between 2022 and 2023 (from 101,000 to 133,000).

The comparison between 2022 and 2023 also shows a worrying trend for six financial institutions, where the amounts involved have doubled or, in some cases, have multiplied by more than five for newly established financial institutions. By contrast, some financial institutions have reduced the amount of the suspicious transfers they received by at least 8%.

The share of the amount of suspicious credit transfers received by financial institutions in 2023, compared with the total amount of credit transfers received, remains low for the retail banks surveyed, between 0.003% and 0.004%, but may be up to 1,000 times higher in the rest of the sample: some financial institutions stand out at a rate above 0.5% when others are well below this threshold.

The average amount of suspicious transfers received appears stable between 2022 (EUR 896) and 2023 (EUR873). Several financial institutions reported low average amounts of suspicious transfers

[24] According to the Banque de France study, which, although is not covering all victims, appears representative when it comes to measuring the most involved institutions.

(less than EUR550). However, some of them have much higher average amounts. Indeed, five financial institutions have an average amount of suspicious transfers exceeding EUR 7,000.

The share of business relationships that received suspicious credit transfers varies significantly across financial institutions. While five financial institutions identified less than 1% of business relationships affected in 2023, other financial institutions identified a high share of business relationships receiving suspicious transfers.

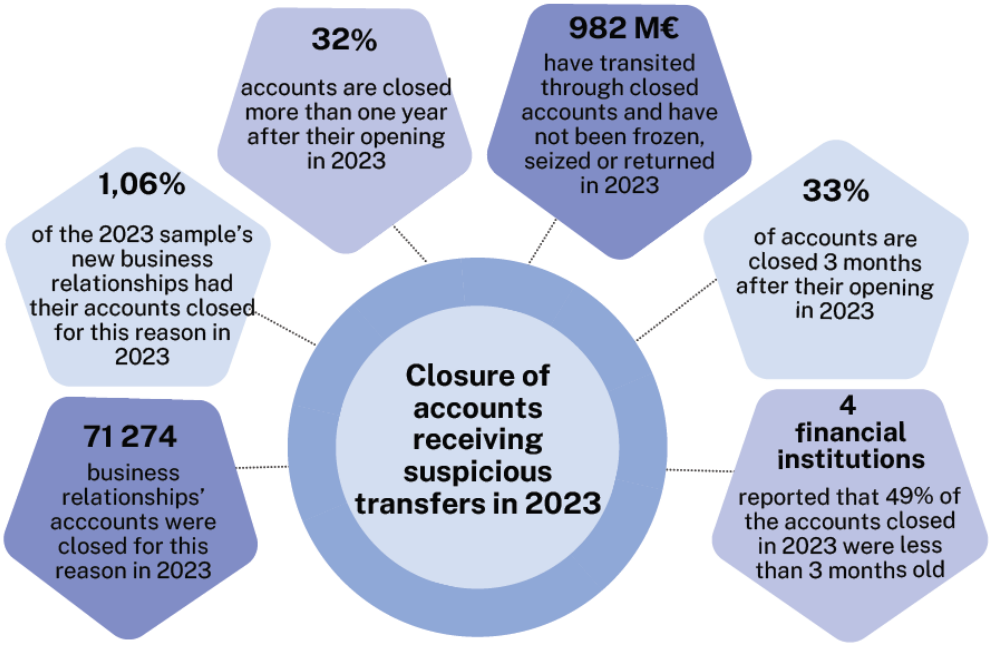
2.2 Outstanding features of particularly exposed financial institutions

Respondents mainly recorded remote onboardings in 2023 (76%), for natural persons (76%), legal persons (72%) and individual entrepreneurs (81%).

Significant growth in retail customers in 2023. Eight of the financial institutions in the sample experienced customer growth of more than 20% between 2022 and 2023. For the financial institutions included in the sample, the new business relationships established in 2023 mainly involve, natural persons (95%). However, some financial institutions of the sample have indicated that 99% their new customers are professionals (legal persons and sole proprietorships).

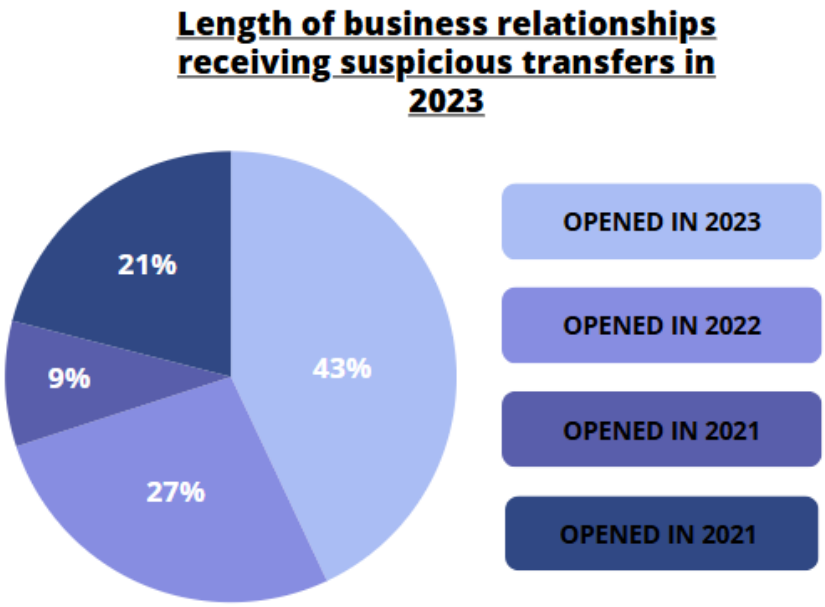
A significant number of recent account terminations in financial institutions particularly exposed to the risk of laundering the proceeds of scams or fraud. 71,274 business relationships were terminated in 2023 following an event that raised suspicions that their account may have received suspicious transfers, which represents 0.17% of the customers in our sample (and 1.06% of new onboardings in 2023).

33% of accounts are terminated within three months of their opening for reasons connected with receiving suspicious transfers, and 32% more than one year after their opening. The interval between account opening and closing is longer for retail banks, which report that more than 50% of the accounts terminated in 2023 for the same reason had been open for over a year. This may indicate a higher proportion of “mules”, i.e. customers who initially used their account normally but later handed it over or made it available to a third party for laundering purposes. Conversely, several institutions mention that more than 49% of the account terminations in 2023 concerned accounts with less than three months of age.



2.3 Outstanding features of accounts receiving suspicious transfers

Accounts receiving transfers that were identified as suspicious in 2023 are mainly opened in the name of recent business relationships.



The overall monitoring of business relationships receiving suspicious transfers from the financial institutions surveyed shows that:

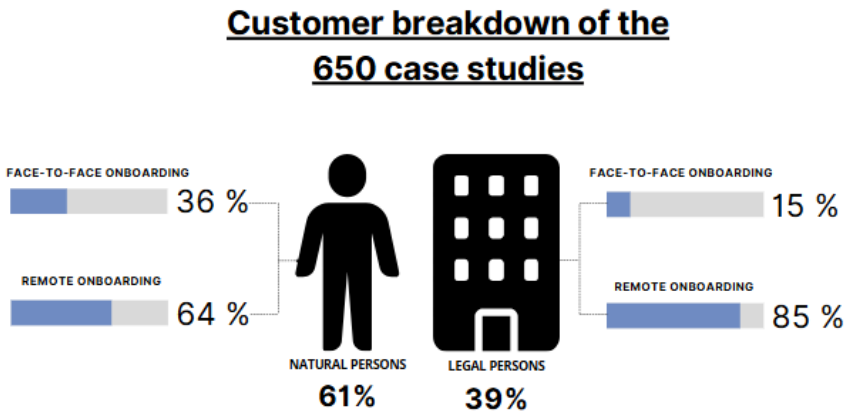
- Of these business relationships, 43% were opened in 2023
- 27% opened in 2022
- 9% were opened in 2021
- 21% were opened before 2021

The accounts receiving suspicious transfers are mainly natural persons (91%). However, some high-risk financial institutions are targeting professional customers / clients

CHAPTER 3 - Detailed study of 650 business relationships

The third part of the questionnaire compiles standardized information from 650 individual cases, which is to say the "top 50" cases within each financial institution, concerning business relationships that received the largest cumulative amount of transfer recall requests in 2023 on FR IBANs. These cases, which present a particularly strong suspicion of money laundering, will be referred to below as "the cases under review".

In addition to the recall requests, the accounts of the studied customers recorded other suspicious transactions worth approximately EUR 73 million. This €138 million represents around 20% of the total suspicious transfers received by these financial institutions in 2023[25].



The 650 business relationships included in the survey were mainly remote onboardings (72%), of which 61% were natural persons and 39% were legal persons.

3.1 Suspicious incoming flows to the accounts of the 650 business relationships analysed

	Credit transfer recall requests	Suspicious transfers received (excluding recalls)	Total suspicious transfers received
Total amount	€65.7 million	€73 million	€138.7 million
Total number	4,145	15,469	19,614
Average amount per business relationship	€101,070	€112,310	€213,380
Average amount per transaction	€15,848	€4,719	€7,071

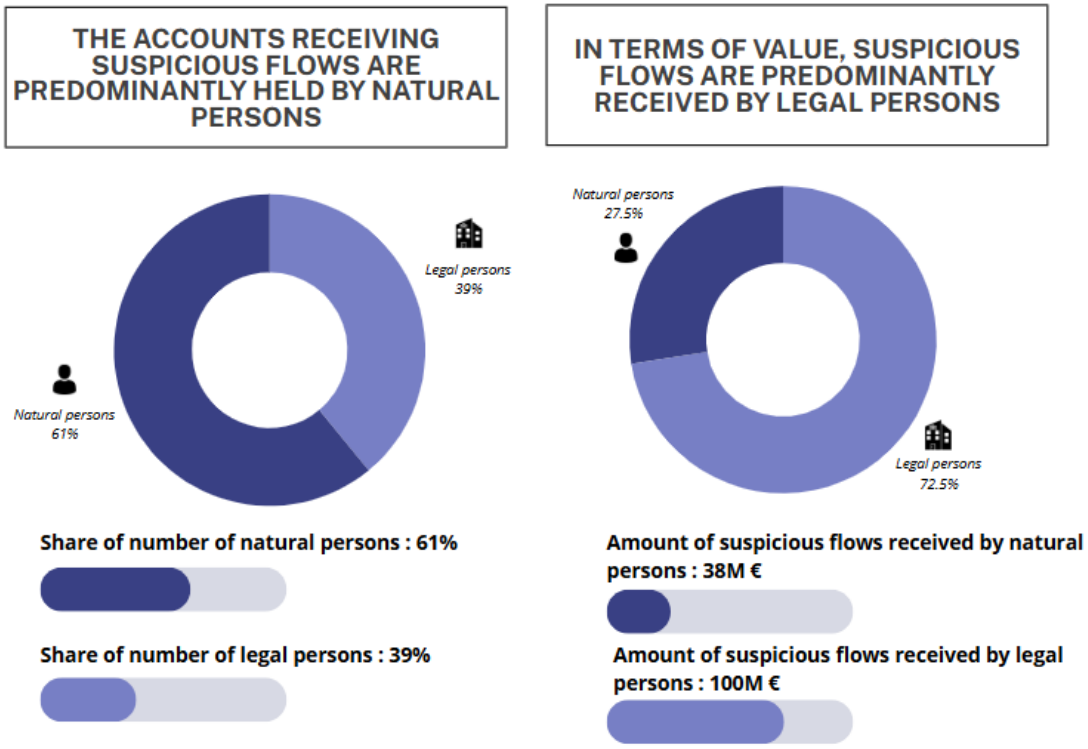
Volume of suspicious incoming flows to the analysed business relationships' accounts

[25] For the 650 cases that received the highest number of recall requests in 2023, the suspicious amounts are not limited to 2023 and institutions were asked to report all suspicious amounts since the opening of the account. However, most of the accounts concerned were opened in 2022 or 2023.

- **Amount of transfer recall requests**

The business relationships studied received, during the account's existence, requests to recall transfers for a cumulative amount of EUR 101,070 on average, the average amount per transaction is EUR 15.8,000. The business relationships of the 650 case studies each received an average of 6.3 recall requests in 2023.

As regards recall requests, natural persons account for 61% of the 650 cases. However, requests concerning legal persons' accounts targets considerably higher amounts (57% of the total amount, i.e. EUR 37 million, compared with EUR 28 million for recall requests for natural persons' accounts).



Of the EUR 138 million in suspicious transfers, EUR 100 million was received in accounts belonging to legal persons and only EUR 38 million was received in natural persons' accounts. Suspicious transfers received on accounts opened for legal persons (EUR 8.3k) are of a higher unit value than those on accounts owned by natural persons (EUR 5k).

- **Proportion of suspicious flows across all flows through accounts affected by the main request for recalls**

For the vast majority of the 650 cases, financial institutions considered most of the flows received by these customers to be suspicious. Eight of the financial institutions included in the sample reported that more than 79% of the incoming flows received on the accounts in the cases analysed are suspicious.

However, the proportion of suspicious flows can sometimes be low (6% of cases concern business relationships whose suspicious flows received represent less than 10% of the total flows received during the existence of the business relationship, i.e. EUR 6 million).

3.2 Destination of outflows

- **The rebound destination of flows transiting through accounts suspected of money laundering**

  The analysis of the destination of flows was carried out using the following method:

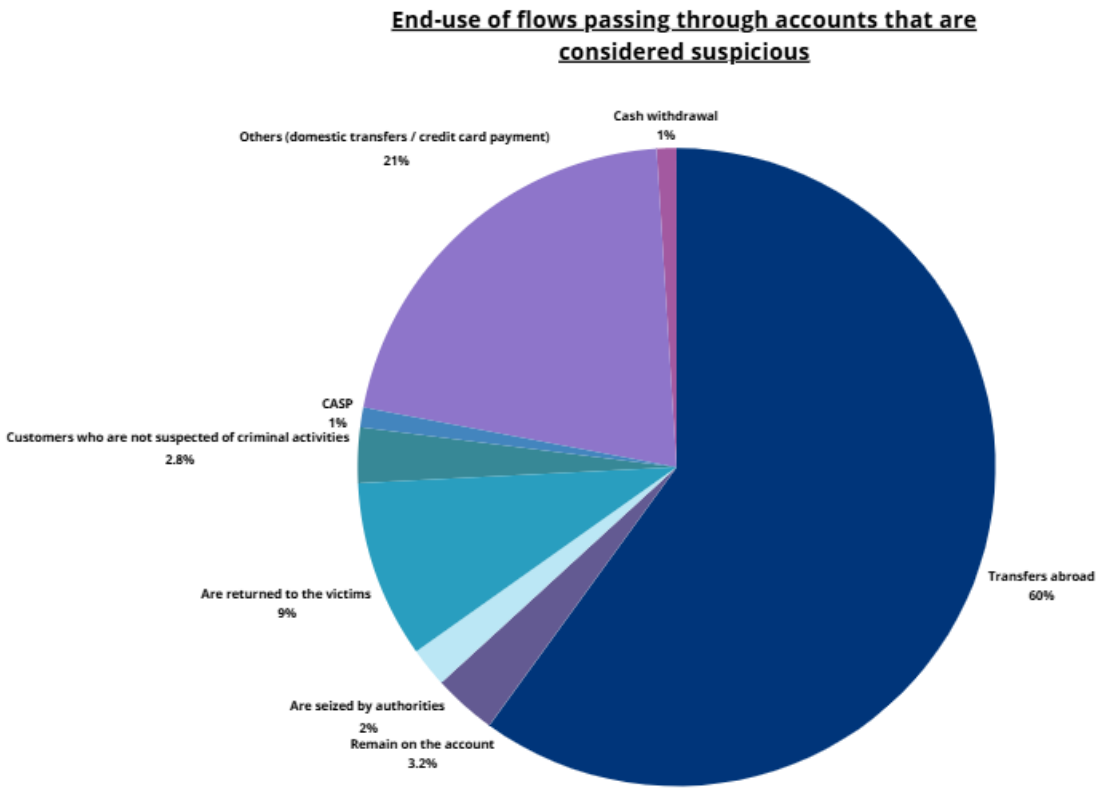
- For the 32 cases where the customer is not suspected of illicit activity, only suspicious flows were considered, for a total of EUR 7.5 million;
- For the remaining 618 cases, all flows from the accounts were included. These cases met either or both of the following conditions: (i) accounts where at least 80% of the flows received by the customer were considered by the financial institution itself to be suspicious; (ii) cases where the accounts had been terminated. For the 618 cases selected, the amount of flows considered suspicious by the financial institution amounted to 131 million and the total incoming flows amounted to 203 million. This approach helps to correct the fact that some institutions seem to underestimate the proportion of suspicious flows on the targeted accounts.

In total, EUR 210 million of incoming flows are analysed. Their destination is broken down as follows:

- **60% of these flows were transferred abroad;** in some institutions, the share of funds that were transferred abroad exceeded 85%. Several financial institutions are taking precautions against credit transfers outside the European Economic Area: some do not offer credit transfers outside the Single Euro Payments Area (SEPA), some financial institutions mention interviewing their professional customers about their business outside the European Union, and others indicate that they factor in the destination of funds when setting limits for online banking transactions. However, **rebound credit transfers are almost exclusively directed to countries within the EU** (mainly Luxembourg, Lithuania, Germany, Ireland, Belgium and Spain), as well as to the United Kingdom**.**
- In at least three cases, the holder of the accounts to which the suspicious transfers were addressed was a **crypto asset** service provider, with a total amount of recall request of EUR 1.6 million (of which around EUR 28,000 was returned to the victim).
- The 28 suppliers of goods and services mentioned above received EUR 5.8 million in recall requests and 1.6 million were returned.
- 1% were withdrawn in **cash**; for 5 financial institutions, cash withdrawals account for between 5% and 7% of suspicious outflows. However, in other cases, some of the customers out of the 50 cases studies withdrew more than EUR 60k in cash. Differences across institutions can be explained by withdrawal ceilings. For natural and legal persons, these limits vary between EUR 500 and EUR 3,000 of withdrawal per day.

14% of the amount were **not transferred**: 9% (18.9 million) were returned to the victims following recalls; 2% (4.1 million) seized by the authorities, 3.2% (6.7 million) remained on the accounts when they closed. The data collected does not allow us to determine the destination of the 21.4% of funds

that have transited through these accounts. However, these are likely to be domestic transfers or card payments in France or abroad.



In 32% of cases, outflows from business relationships identified as receiving fraudulent transfers mainly went to certain financial institutions in the sample, or to other entities of their group abroad, whereas these institutions account only for a 6% market share in France.

- **Freezing, seizure or restitution to the victim**

Transfer recalls were successful for 31% of the amounts recalled in 2023, which represents more than EUR 20 million returned to victims out of EUR 66 million. Seizures made by the authorities accounted for EUR 4.2 million of the suspicious flows that had transited through the accounts of the 650 case studies.

According to the data reported by the respondent financial institutions, the proportion of suspicious incoming funds that was stopped (either returned or seized by authorities) for the entire customer base in the sample in 2023 is much lower (8.9%) than in the 650 case studies perhaps because transfers of higher amounts in the 650 case studies were more likely to be detected and blocked than those of lower amounts.

However, the success rate of recalls and seizures varies considerably from one financial institution to another:

- Of the 650 case studies, more than half of the suspicious amounts were detained, seized or returned to the victim for some institutions, while the share was less than 15% for others.
- For all customers included in the sample, the best-performing institutions held, seized or returned one-third of the amount of suspicious transfers received, compared with less than 4% for the worst-performing institutions.

3.3 Age of accounts receiving suspicious transfers

- **Newly / recently opened accounts**

The business relationships for which there is the highest / strongest suspicion of money laundering have been recently established and have a relatively short lifespan:

- 70% of the accounts identified as having received the largest recall amounts had been in existence for less than one- year;
- Some financial institutions reported that this applies to more than 80% of the accounts identified as receiving suspicious flows;
- Conversely, other institutions reported that less than 50% of accounts that received suspicious transfers had been in existence for less than one year.

- **Few dormant accounts**

For an account suspected of laundering the proceeds of scam or fraud the average time from the opening of the account to the first debit transaction is 46 days for the sample analysed. In 44% of cases, the first transaction takes place within the first 15 days following the opening of the account and only 1.7% of cases carries out their first transaction one year after the opening of the account.

- **The termination of accounts**

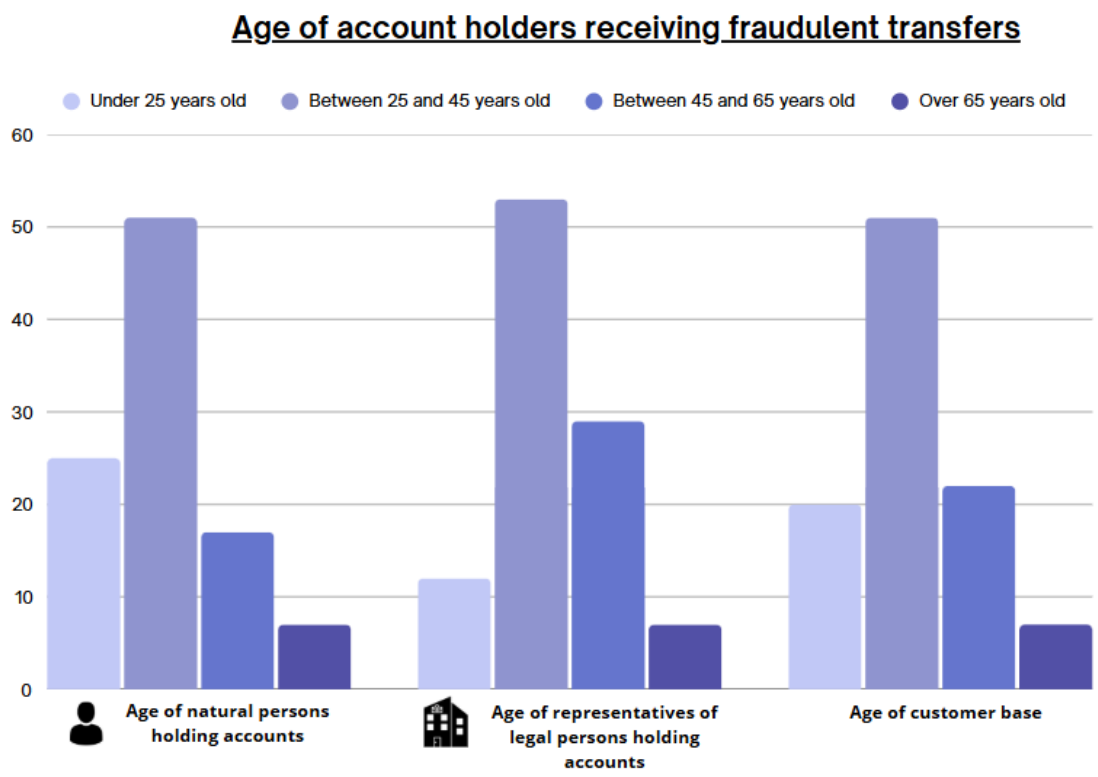
The vast majority (90%) of the accounts that received the largest cumulative transfer recall requests in 2023 were terminated on the financial institution's initiative.

3.4 Features of business relationships holding rebound accounts

- **Average age of business relationships**

On average, the individuals holding the accounts affected by the main recall requests and their representatives are 39 years old.

- Three financial institutions indicated that more than one-third of the customers concerned were under 25 years old and three others said that less than 6% of their business relationships were under 25 years old.
- For nine institutions, more than half of their customers is between 25 and 45 years old.
- Finally, four institutions reported that more than 12% of their customers are over 65 years old.



- **Country of residence of transit account holders**

97% of the case studies involve French residents, but some institutions indicated that more than 14% of the business relationships involved foreign residents.

However, the customers' place of residence appears to be insufficiently verified, as in most cases the declared address is based solely on self-reporting. In fact, proof of address is collected for only 26% of business relationships and verification of the customer's address with a letter requiring some form of acknowledgement of receipt (RLAR, code to be entered, etc.) is applied to only 14% of cases and only by a few institutions.

CHAPTER 4 - Overview of identity verification practices

4.1 Identity verification procedures applied to private individuals and representatives of legal entities

The identity verification measures are provided for in Articles R. 561-5-1 and R. 561-5-2 of the French Code Monétaire et Financier (CMF). The application of a single measure under Article R. 561-5-1 of the CMF is sufficient, whereas for identity verification under Article R. 561-5-2 of the CMF, at least two measures must be applied.

- **Face-to-face onboardings**

In the sample of 650 case studies, for 36% of natural persons and for 15% of legal persons onboarding was carried out face-to-face (representing 27.8% for all types of customers). For this purpose, the person to be identified (the natural person or the representative of the legal person) must be physically present in the same place as the employee of the financial institution or the person acting on behalf of the institution and must present a valid official identity document or extract from an official register according to Article R. 561-5-1, 3° and 4° of the CMF. Four financial institutions reported using these identity verification measures face-to-face. Three out of these four financial institutions are strengthening their identity verification procedures by applying an additional measure set out in Article R. 561-5-2 of the CMF: the first transaction crediting the account is made by an account opened in the customer's name by a financial institution established in the European Economic Area.

- **Remote onboardings**

Financial institutions in the sample do not use the electronic identification method provided for in Article R. 561-5-1 1° and 2° of the CMF (such as La Poste's Digital Identity).

Financial institutions prefer the application of at least two out of the six measures provided for in Article R. 561-5-2 of the CMF:

- 1. Obtaining the copy of an identity document

The requirement of obtaining a copy of an identity document with a valid photograph is applied by all financial institutions and for all their customers without distinction between private individuals and representatives of legal persons. However, copies of identity documents can be easily obtained, for example by misusing copies of documents obtained for other purposes (rentals, etc.) or by falsifying them allowing identity fraud. Six financial institutions indicated reducing this risk by using *liveness testing* whereby the holder of the identity document clearly demonstrates that he is providing the document for the purpose of onboarding[26], without the financial institution relying on a remote identity verification provider certified by the National Information System Security Agency (thereby not complying with item 5 of this Article R. 561-5-2). Furthermore, several institutions use biometric comparison. For three out of the nine financial institutions that have introduced this measure, the comparison is made between a selfie and the identity document provided.

- 2. Identity document certification procedure

Article R. 561-5-1 2° of the CMF provides for the verification and certification of the identity document by an independent third party. Some financial institutions are applying this measure to more than 98%

[26] Analyse Sectorielle des Risques de l'ACPR, p. 26

of their customers. The exact conditions for using this certification procedure still need to be worked out.

- 3°) The first transaction crediting the account

The measure requiring that "*the first payment of transactions be made from or to an account opened in the customer's name*" is applied to both private individuals and representatives of legal persons in two-thirds of cases (63% and 56% respectively). In its 2023 Sectoral Risk Assessment, the ACPR pointed out that some financial institutions do not sufficiently take into consideration the risk that the other account itself may have been opened as a result of fraud. This happened even though the financial institution was aware of this risk, particularly when the institution taking the other account is subject to public measures aimed at correcting identity verification failures or when it becomes aware of an abnormal number of frauds associated with a given account servicing financial institution. Furthermore, in 18% of cases, the first transaction crediting the account comes from a debit card, without it being clear that the institution is verifying that the card is linked to an account belonging to the person whose identity is to be verified, and not to a third party or to an electronic[27] wallet.

- 4. Obtaining confirmation of identity by a third party

The 4th measure consists in obtaining a confirmation of the customer's identity by a third party. This measure is used by some financial institutions for a portion of their customers.

- 5. Use of a remote identity verification provider

The use of a '*service certified as complying by the French Cybersecurity Agency, or a certification body authorized by that agency, maintaining a substantial level of guarantee for requirements relating to proof and verification of identity*', more commonly referred to as 'PVID'. It is used by some institutions.

- 6. Electronic signature

Electronic signature is used in 17% of the business relationships' onboardings in this study. However, some institutions are applying this procedure to more than 86% of their clients onboarding remotely and use the same provider for this purpose. Moreover, some institutions seem to have introduced this measure after the onboarding of the cases studied here.

Financial institutions are required to apply <u>at least</u> two measures provided for in Article R. 561-5-2 of the CMF. The measures are combined as follows:

- Financial institutions most often combine obtaining a copy of an identity document (1°) and the 1st transaction crediting the account. Indeed, eight institutions are using this combination to verify the identity of their customers, six of which go further and apply an additional measure, which may imply that financial institutions are aware of the risk associated with the 1st transaction crediting the account measure.
- In some financial institutions, the first transaction crediting the account (3°) is made only by credit transfer, which reduces the risks associated with the first card payment mentioned above. Other institutions refer to restrictive measures (limited list of accepted institutions or exclusion of certain high-risk institutions).
- Some financial institutions use the electronic signature (6°) in addition to obtaining a copy of the identity document.
- Several institutions onboarding their customers face-to-face (Articles R. 561-5-1, 3° and 4° of the CMF) are also applying an additional verification measure which is systematically the first transaction crediting the account the account (3°).
- Other financial institutions are obtaining the copy of the identity document and have a third party subject to AML/CFT regulations confirm the customer's identity.

[27] In French : ACPR Sectoral Risk Analysis, p. 26

- **The analysis of the 650 case studies revealed that some institutions are only collecting the customer's identity document without applying a second measure required by Article R. 561-5-2 of the CMF for remote onboarding.**
- The financial institutions surveyed in the study make no distinction between natural persons and representatives of legal persons. Indeed, financial institutions with clients that are both natural and legal persons are applying the same measures to all clients. In addition, financial institutions that only have professional clients are applying the same measures to representatives of legal persons as financial institutions that only have natural persons clients.

4.2 Identity verification procedures applied to legal entities

Verification of the legal persons' identity is an additional procedure to the verification of the legal person's representatives' identity described above.

For the purpose of verifying the legal person's identity, financial institutions are systematically collecting the extract from an official register. However, the means by which this document is obtained varies from one institution to another. Indeed, out of the eight financial institutions that reported having at least one legal person customer in their 50 cases sample, a minority of institutions with an exclusively professional customer base indicated that the extract from the register was obtained directly from a competent authority. In other cases, the copy is obtained directly from the prospect, which comes with the risk that the copy may have been falsified, for example in terms of the identity of the legal person's representative.

As regards the verification of the authority of the legal entity's representative, almost all the institutions that replied to this question indicated that this verification is carried out by consulting the companies register or another public register mentioning the name of the representative.

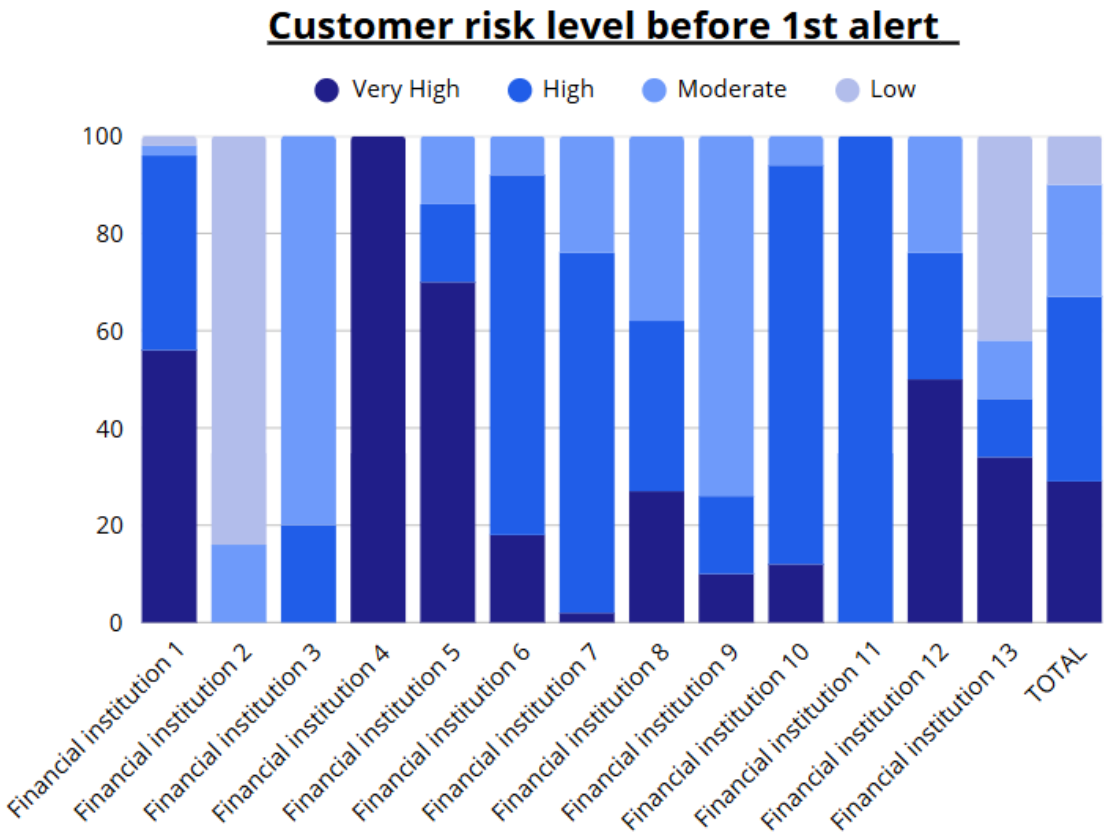
CHAPTER 5 - Overview of customer onboarding frameworks

5.1 KYC at onboarding: risk classification

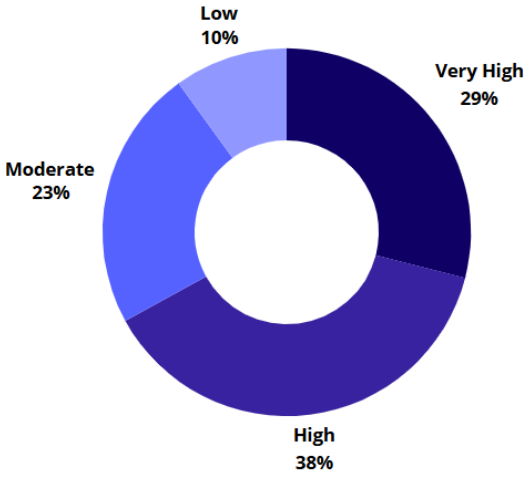
Article L. 561-5 of the CMF provides that financial institutions must identify their customers and, where applicable, their beneficial owners. The Ministerial order of September 2nd, 2009 specifies the information that may be collected throughout the entire business relationship for the purposes of assessing the risks of money laundering and terrorist financing.

Article R. 561-20-2 of the CMF states that institutions "*shall define and implement tailored procedures to the risks of money laundering and terrorist financing to which they are exposed*". Therefore, at the beginning of the business relationship, financial institutions categorize customers, both natural and legal persons, by giving them a risk score. This score will define the procedures that will be applied to them and more particularly the additional elements that will be asked of them in terms of KYC. With regard to the 650 case studies that received the largest cumulative amount of recall requests in 2023: 29% of the cases were classified as very high-risk, 38% as high, 23% as moderate and 10% as low.

Three financial institutions in the sample did not categorize any of their cases as very high-risk, and one of them had classified all 50 as moderate-risk (16%) or low-risk (84%). Conversely, two institutions classified the majority of their cases as very high risk, including one for all of its clients.



Customer risk level before 1st alert



Less than one third of the cases in the study were classified as very high risk before the first alert, while 70% of the 650 relationships surveyed had been established less than a year before the first recall. Around 80% of legal entities were very recently established (or even in the process of being established) and many legal entities were engaged in high-risk sectors of activity (29% in construction industry and 26% in trade). This seems to indicate that the risk is underestimated by financial institutions when onboarding, which affects the extent of the information collected.

- **Know Your Customer**

The financial institutions surveyed indicated in their procedures that they were deepening their knowledge of the customer by collecting other data, including: the country of residence, postal address, marital status (single, married, etc.), tax residence, tax identifier, professional status (professional category, occupation), contact details (email, phone number etc.), housing status (owner, tenant, etc.), wealth situation, monthly income or income bracket of the customer, name of the employer, etc.

Half of the financial institutions reported collecting the tax residence and/or the tax identifier. The collection of these data makes it possible to meet the requirements provided for in Article 1649 AC of the Code general des impôts (CGI) and specified by Decree No. 2016-1683 of 5 December 2016 laying down the rules and procedures concerning the automatic exchange of information relating to financial accounts known as the “common reporting standard”.

The ACPR's guidelines on customer identification, verification and KYC procedures state that KYC information is collected using a risk-based approach that allows for the assessment of the risk profile of the business relationship and allows for ongoing due diligence.

However, some financial institutions perform more due diligence than others, as the amount of data collected when onboarding varies considerably across institutions. Indeed, the 650 case studies showed that in practice the amount of income or income bracket of the natural person business relationship was collected in 68% of the cases and 16% for the representatives of the legal person.

In addition, data on income or income bracket are collected by:

- Only four institutions for all of their customers

- Two institutions for at least half of their customers
- Three institutions collect the data for less than a third of their customers.

The level of detail in the information requested varies across financial institutions. When such information is collected, it is mostly self-reported, as supporting documents evidencing income (tax assessments, payslips, etc.) are obtained in only 15% of cases.

Financial institutions also have obligations relating to collecting the purpose and nature of the business relationship, according to Article R. 561-12 of the CMF[28]. In order to gain this knowledge, financial institutions mentioned collecting in particular:

- The intended use of the account
- The nature of transactions
- Purpose or reason for opening the account
- The maximum estimated amount per transaction
- Whether it's a primary account or a secondary account....

➢ **Know Your Business**

Financial institutions subject to AML/CTF obligations must collect the following identification data when their customer is a legal person: legal form, name, registration number, address of head office and centre of effective management. This identification information is obtained from an official register, an extract of which is collected by all institutions when onboarding legal entities.

For all business relationships involving legal persons, the information on the activity carried out is systematically collected.

Turnover is not systematically collected by the financial institutions. Indeed, the study of the most fraudulent cases showed that the amount of the turnover of the legal person is collected in 52% of the cases. Turnover data is collected by:

- Some institutions collect it for all or a very large majority of their legal entities customers;
- Others do not collect the turnover of their legal entities customers.

5.2 The collection of supporting documents corroborating the information reported by the customer

Proof of address or income, or evidence specific to legal persons and beneficial owners seems rare considering the level of risk.

➢ **Supporting documents relating to the customer knowledge for the natural person or the legal person's representative**

The banker is no longer required to systematically verify an applicant's address before opening an account, following the repeal of this obligation by Decree 2020-118 of 12 February 2020. Nevertheless, such verification remains mandatory in some cases as described in Section 3 of this report. Financial institutions are collecting at least one proof of income for 16% of natural person customers. More specifically, a tax return is collected in 11% of cases and another income statement (pay slip, etc.) is

[28] Article R. 561-12 of the CMF: Financial institutions must "*1° Before onboarding, collect and analyse the information needed to know the purpose and nature of the business relationship;2° Throughout the business relationship, collect, update and analyse the information that makes it possible to maintain appropriate and up-to-date knowledge of their business relationship*."

collected in 6% of cases. Only 7 institutions are collecting a proof of income, 3 of which are collecting this information for less than 14% of their natural person customers. However, no institution reported collecting proof of income for all of its customers.

Only four financial institutions are collecting proof of income of the legal person's representatives and only for 14% of this customer base.

In most case studies, the place of residence is self-declared, since proof of address is collected only for 21% of business relationships involving natural persons and for 34% of legal persons' representatives. Then, address verification using a letter with acknowledgement of receipt (RLAR, code to be entered, etc.) is also rarely used. Indeed, it is only used for 14% of the 650 case studies and only by a few financial institutions. Two of these institutions use it for 80% of their natural-person customers.

The 2D-Doc system, designed to fight against fraud and secure data exchanged between the user and the administration, was seldom used by the institutions surveyed in the 650 case studies.

- It is used in 6% of cases to check proof of address and only three institutions are using it,
- In 4% of the cases, for the verification of the tax return and only two institutions are using it.

- **<u>Supporting documents relating to the legal person's customer knowledge</u>**

Copies of the customer's articles of association are not systematically requested, they are collected in 55% of the case studies:

- Some institutions specialized in professional customers are collecting the articles of association for all customers that are legal persons, while others collect them for more than 86% of legal person.
- In contrast, other institutions reported never collecting copies of the articles of association, or for a very small proportion of legal persons.

Tax return or other evidence of turnover is collected in only 18% of cases and only by a minority of financial institutions. Several institutions with legal person customers are not collecting any evidence of turnover. However, many of the legal entities surveyed are new, which may explain the absence of such documents, although the financial institutions do not seem to have obtained the alternative information suggested in this case by the abovementioned ACPR guidelines.

CHAPTER 6 - Overview of systems and practices for detecting suspicious transactions

6.1 Responsiveness of financial institutions following an alert

- **Detection of suspicious transactions**

The origin of the alert following a suspicious transaction varies strongly from one institution to another. Financial institutions reported that 65% of the first alerts were internal and 35% were external. However, there are strong differences within our sample, since one financial institution reported that it had received no internal alerts for the 50 cases of its sample, while another reported that an internal alert always preceded external alerts for all of its 50 cases. Of these internal alerts, 76% are automated and 24% are human alerts. Finally, 57% of the initial external alerts came from transfer recall requests, 28% from the authorities and 15% from other external alerts.

- **Time between the first recall request and a suspicious transaction report**

The average time between the first recall request and a suspicious transaction report (STR) is 29 days. However, one institution stands out with a very long lead time (on average 145 days after receiving the recall request).

In 80% of the case studies where suspicious transactions were reported, these occurred after the recall request was received.

- **Time between the first recall request and the termination of the account**

On average for the 650 business relationships suspected of having transit accounts, the time between the first recall request and the closing of the account by the financial institution is 65 days. This timeframe varies from one financial institution to another. Indeed, three institutions reported an average timeframe of between 10 and 23 days, while four institutions reported a timeframe of at least 3 months.

With regard to the accounts receiving a recall request that were terminated, 36% were not reported as suspicious. Four institutions reported having received a recall request and having terminated the account but did not issue a suspicious transaction report in more than half of the cases.

6.2 Transactions monitoring system

- **Scenarios based on transaction characteristics**

Financial institutions reported numerous scenarios based on specific criteria related to transaction and the account's activity. The scenarios are based on several criteria, including quantitative criteria that make it possible to assess the risk of laundering the proceeds of scams or fraud. Scenarios can be used to detect:

- Individual transactions that are remarkably large, for example because the amount is above/below a threshold or is a round figure; or a series of transactions when aggregated, over a given period, exceeds a threshold, the threshold possibly being an amount or a number of transactions (which varies by institution); or a transaction or series of transactions that may reveal a change in the behaviour of the customer's account compared to a reference period (all institutions)
- A transaction or series of transactions where there is a counterparty abroad

- A transaction or series of transactions as related to a well-identified money laundering/terrorist financing typology such as scenarios centred on the detection of mule accounts with rapid cash withdrawals after account opening, or a "Many-to-One" typology
- A transaction or series of transactions where a counterparty has been identified as suspicious
- A transaction due to specific keywords in the various text fields of the payment/credit transfer message.

Some financial institutions reported more atypical scenarios based on transaction characteristics:

- Some institutions reported scenarios based on the unusual timing of the transaction
- Other financial institutions have included in their monitoring tools a blacklist of high-risk institutions, along with an outgoing credit transfer suspension system. Some institutions also have similar alerts on the source of funds. These lists vary from one financial institution to another.

➢ **Scenarios based on customer characteristics**

Scenarios based on the score and risk level assigned to the customer at onboarding. Several financial institutions assign their clients scores or categorize them in peer groups, allowing for the scenarios to adapt not to each client, but to categories of clients.

The risk score assigned to customers is based on several criteria: place of residence, housing situation, age, nationality, telephone operator, sector of activity... Some financial institutions also indicated taking into account the number of customers related to the same address as well as the brand of the device used to onboard remotely. Financial institutions indicated that this score may change over the course of the business relationship, especially in the event of an alert on the customer's account or as a result of a KYC update.

Then, respondents also indicated that their transaction monitoring tools are based on several criteria, including:

- The recent nature of the account is an indicator that emerges for our 650 case studies
- Recent changes in contact details, connection to a new device as well as any recent events that could be an indicator of fraud
- The age of the customer.

More than half of the financial institutions surveyed indicated taking into account the customer's profession in their transaction monitoring tools.

Moreover, a large majority of financial institutions mentioned collecting the natural person's income. The case studies show that more than a quarter of natural persons having reported income when onboarding (amount or bracket) have received suspicious transfers more than five times higher than their expected income over the existence of their account.

➢ **Alert blocking mechanisms**

Almost all financial institutions reported that they had set up rules and alert scenarios that block outflows or the account itself:

- Some financial institutions have blocking alerts for standard credit transfers only;
- Other institutions reported that their monitoring tools allow to block standard credit transfers, as well as instant transfers. However, the scenarios that generate alerts blocking instant transfers are more limited than those blocking standard transfers.

In addition, most financial institutions set up online transaction limits: in some cases, these are fairly low amounts, beyond which validation by staff is required; in other cases, the amounts cannot be exceeded but are very high and supplemented by blocking alerts.

These limits apply to both standard and instant transfers. In contrast, instant transfer limits are often much lower since the transfer is immediate and because of the lack of a mechanism allowing to block funds in many institutions. However, some financial institutions stand out with very high instant transfer limits per transaction.

For traditional credit transfers, the limits vary by financial institution within very wide ranges. Some financial institutions with the highest limits show very high suspicious transfer rates and extremely low rates of fund freezing, seizure or return.

CHAPTER 7 - Overview of the integration of money-laundering risk into governance, organisation, and internal controls

7.1 The framework for managing money-laundering risk

Financial institutions reported that they factor in directly or indirectly the risk of laundering the proceeds of fraud in their risk map, but five of them do not specifically take this risk into consideration (but only for money laundering in general).

Three financial institutions have set up specific committees or sub-committees dedicated to fraud, in addition to the monitoring carried out by other internal bodies dedicated to risk or compliance.

Risk Department or Compliance Department are responsible for fraud-related issues. However, some internal organizations provide that the risk of fraud is monitored by the Risk Department, while the risk of laundering the proceeds of fraud is monitored by the Compliance Department.

In any case, fraud-related issues are most often addressed by various monitoring committees. Thus, when the compliance department is responsible, the risk of fraud is also monitored at the risk level, provided that this risk is systematically factored in in the business-wide risk assessment. Conversely, even if the risk department is responsible, the risks of fraud and laundering of its proceeds are taken into account when monitoring transactions through dedicated scenarios and AML/CTF procedures.

Most financial institutions reported that they have set up performance indicators that include the risk of money laundering. A minority of institutions have not yet implemented any specific monitoring indicators, but one of them should soon do so.

The examples of monitoring indicators reported are mainly based on indicators of fraud itself, such as the monitoring of recall requests for fraud, rates of fraud involving incoming credit transfers, or document fraud.

The frequency of the performance indicators concerned is either monthly, daily or quarterly, without any apparent prevailing practice.

7.2 The resources devoted to onboarding

To effectively combat the risk of laundering the proceeds of scams or fraud, financial institutions must commit significant resources, resulting in longer and more costly account-opening processes. They must also have sufficient human and material resources, including staff dedicated to ML/TF risks.

Onboarding is only made remotely for a majority of financial institutions in the sample.

For some institutions, the **time taken to open an account is very short** (for some 10 minutes or less) and the **cost of the resources committed to onboarding is low,** less than €12 for 6 institutions (excluding enhanced due diligences). Financial institutions with very low suspicious transfer rates (for example one euro per 100,000 or less) are spending at least 20 minutes for the opening of the account, considering that this timeframe varies according to the complexity (up to 6 days).

7.3 Financial Products Design

The terms of use of financial products and services offered by financial institutions are based on transaction ceilings, which vary greatly from one institution to another, on the nature of the transaction (credit transfers, payment or withdrawal), both in terms of amount and frequency (per day/week/month), and frequently on the quality of the business relationship (legal entities or companies).

A few financial institutions are making adjustments to transaction thresholds depending on customer knowledge, the age or the duration of the business relationship or the destination of payment (specific limits for online games, reloading of prepaid cards, online sales).

In some cases, higher ceilings can be obtained by customers paying an additional charge, either per transaction or for a higher threshold of transactions (especially in the case of payment cards). This analysis is based on the higher ceilings reported, without taking into account the pricing policy of the financial institutions.

Some financial institutions also apply a global ceiling for all payment channels.

- Standard credit transfers

All financial institutions but one have high standard transfer thresholds. The thresholds applied are extremely different.

Some financial institutions reported that they have no limits on issuing credit transfers, some of which mentioned relying on a detection framework based on criteria other than amount thresholds.

Four of the financial institutions offering instant transfers, reported that the ceilings applied are generally lower than those for standard transfers. Some financial institutions are also lowering ceilings for vulnerable customers (underage, elderly). Some institutions are applying specific velocity rules for instant transfers over certain time periods and per day.

In the case of a transfer request to a new payee, some financial institutions are applying either a delay period for the transaction, or the display of an alert message or validation by text message.

- Payment cards

Credit card payment ceilings range from €1,500 to much higher ceilings per month. The highest ceilings, most often defined on a daily or weekly basis but with no monthly limit, are available to both private individuals and businesses. Some financial institutions supplement these thresholds with a maximum number of payments per month.

Withdrawals by credit card are subject to monthly ceilings ranging from €150 to much higher ceilings.

- Multiple accounts and virtual IBANs

The 650 case studies revealed that the business relationships affected by the largest recall requests had on average three accounts. However, while three-quarters of affected customers have a single account, 8% have two, 8% have at least 10, and 4% have at least 20. The maximum number of accounts held by the same business relationship even reaches 68 for two legal person clients.

Multiple holding of accounts is observed mainly among a minority of financial institutions, with a very high number of accounts.

The use of virtual IBANs was indicated by a minority of financial institutions surveyed as covering 18 business relationships, mainly legal persons. However, the qualification of virtual IBANs is being discussed by some of the financial institutions.

7.4 Lessons learned by financial institutions that could reduce the laundering of scams and fraud

Financial institutions have identified risky practices, which makes it possible to detect products, services or terms of use presenting higher risks of laundering the proceeds of scams or fraud. Some financial institutions identified this specific risk in their **risk classification**. This is sometimes accompanied by an action plan monitored at a high level by governance bodies.

Several financial institutions identified **remote onboarding** as a risk factor increasing the risk of laundering the proceeds of scams or fraud.

Some practices aim to **limit the risk of identity fraud**. When onboarding, these practices are based in particular on:

- Methods ensuring that the person whose identity is being verified is the person requesting the opening of the account;
- A restrictive policy with regard to the sources of the account's first crediting transaction, used to confirm identity (excluding high-risk financial institutions, risky methods such as payment cards);
- Obtaining extracts from official registers directly.

The need **for quality in risk assessment** from the onboarding was stressed by some financial institutions. Verification measures (such as the 2D DOC) are sometimes taken to ensure that the supporting documents are not falsified, in terms of revenue, turnover or address.

Knowing **the customer** also requires a precise definition of the purpose of the business relationship, with precise expected profiles of account functioning. For example, this may include not only the total amount of expected transactions, but also its variation over a shorter period, the average transaction amount, the maximum amount of individual transactions, the average number of monthly transactions, the location of counterparties, etc. Some institutions reported that they check the transactions' record at the previous payment service provider (PSP).

Over the course of the business relationship, several financial institutions recommended that monitoring systems be set up (for example, with a consistency check between the beneficiary of wire transfers provided by the issuer and the account holder, or consistency between the place of connection to the PSP online services or locations of card payments that are inconsistent with customer knowledge, search for keywords in payment messages).

Product **design** seems to be an important risk management factor in some financial institutions, and may increase the success of recalls:

- Transaction limits that reflect the expected operating profile of the account and above which transactions are blocked;
- Allow for the possibility to delay outflows in the case of high-risk typologies, in order to make it possible to carry out enhanced due diligence and, where appropriate, to report to the French FIU Tracfin before carrying out the transaction.

Some financial institutions recognized the risks associated with new technologies and certain methods of payment (creation of multiple accounts / sub-accounts or virtual cards from the customer space, issuance of instant transfers, setting up of direct debits). For example, some financial institutions highlighted the risk that products that are freely accessible online could facilitate

fraudulent schemes or layering techniques. Others identified that accounts could be opened and then made available to third parties with or without the customer's consent, using remote access software.

Best practices identified include limiting access to certain products or services, such as limiting the number of virtual cards, setting ceilings on outgoing instant transfers without manual validation or enhanced review, and limiting the number of accounts per customer.

Several financial institutions also recommended the implementation of scenarios that trigger alerts or blocks, particularly in case of atypical changes in the technical data used to log in to the account (such as the login device, the IP address, login credentials, password failures or losses). Some financial institutions verify again the identity of the applicant when the customer accesses his account using a new connection device.

Participating financial institutions mentioned that the following features improve the effectiveness of due diligence:

- updating scam scenarios on a regular basis
- due diligence on all customer accounts / sub-accounts
- and ongoing monitoring of transactions. Several institutions considered that Machine Learning techniques offered by artificial intelligence can detect and block suspicious transactions more quickly and effectively. Some financial institutions favor more adaptive models with a broader scope over scenarios that are quickly obsolete because of the ability for money launderers to adapt. However, while one of the few institutions in the sample that uses AI has the lowest rate of fraud involving means of payment in the statistics collected by the Banque de France on the basis of victims' bank statements, others that also use AI are among those with the highest fraud rates.