Banfico | HERALD AVOCATS DEPUIS 1957

FNC-RF: A new shield against payment fraud in France

Table of Contents

Introduction

On May 7, France officially launched the Fichier National des Comptes signalés pour Risque de Fraude (FNC-RF), a centralised register of bank accounts flagged as potentially linked to fraudulent activities. Operated by the Banque de France and grounded in Law n° 2025-1058 of 6 November 2025 (known as the Labaronne law), the FNC-RF represents the most significant structural change to French payment security in a generation.

The law requires all in-scope payment service providers to report suspicious IBANs, to promptly handle alerts without delay and to share the result of its verification as soon as possible where they hold the flagged account, and to maintain the accuracy of what they contribute. For the first time, intelligence on potentially fraudulent accounts flows in near real time across every participating institution in France — making it considerably harder for fraudsters to migrate from one bank to another once identified.

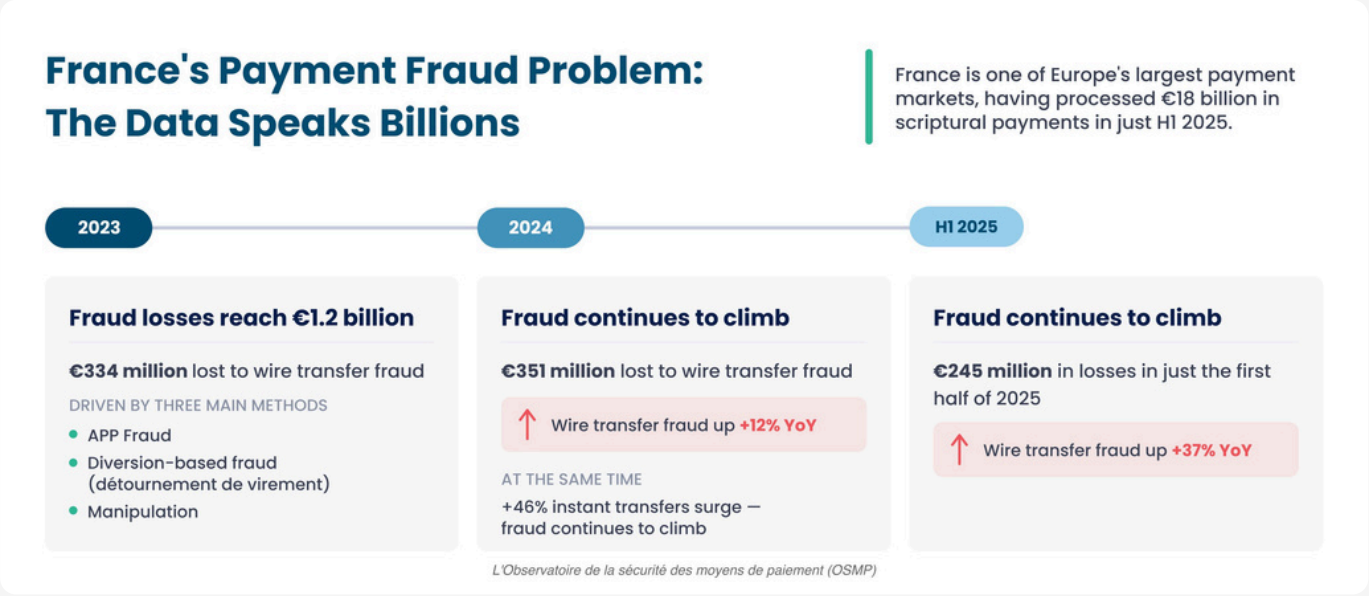
This whitepaper provides a comprehensive, practitioner-focused guide to the FNC-RF: the fraud context that gave rise to it, the regulatory journey that shaped it, what the law specifically requires, how the system works in practice, and the legal responsibilities and risks that now attach to every in-scope institution.

It draws on direct sources: officials at the Banque de France, Daniel Labaronne (the Member of Parliament who proposed the regulation), and legal and technical experts in the field.

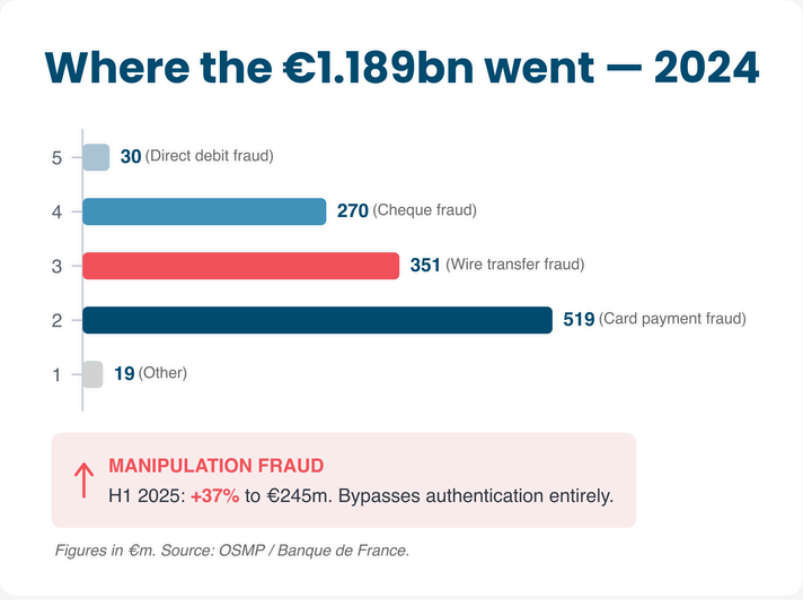
1. Context

1.1 The scale of payment fraud in France

France is one of the main payment markets in Europe, processing over €18 billion in scriptural payments in the first half of 2025 alone. Fraud losses have grown alongside that volume every year since 2023, driven by three recurring schemes: outright false wire transfers, diversion-based fraud (détournement de virement), and other manipulation methods.



Card payment fraud remains the largest single category by value, but it is also the one furthest along its decline — a point covered in Section 1.3. The instrument to watch is wire transfer fraud, and specifically the manipulation-based share of it: in the first half of 2025, the Observatoire de la sécurité des moyens de paiement (OSMP) recorded a 37% increase in manipulation-based fraud (€245 million), the only category still accelerating into 2025.

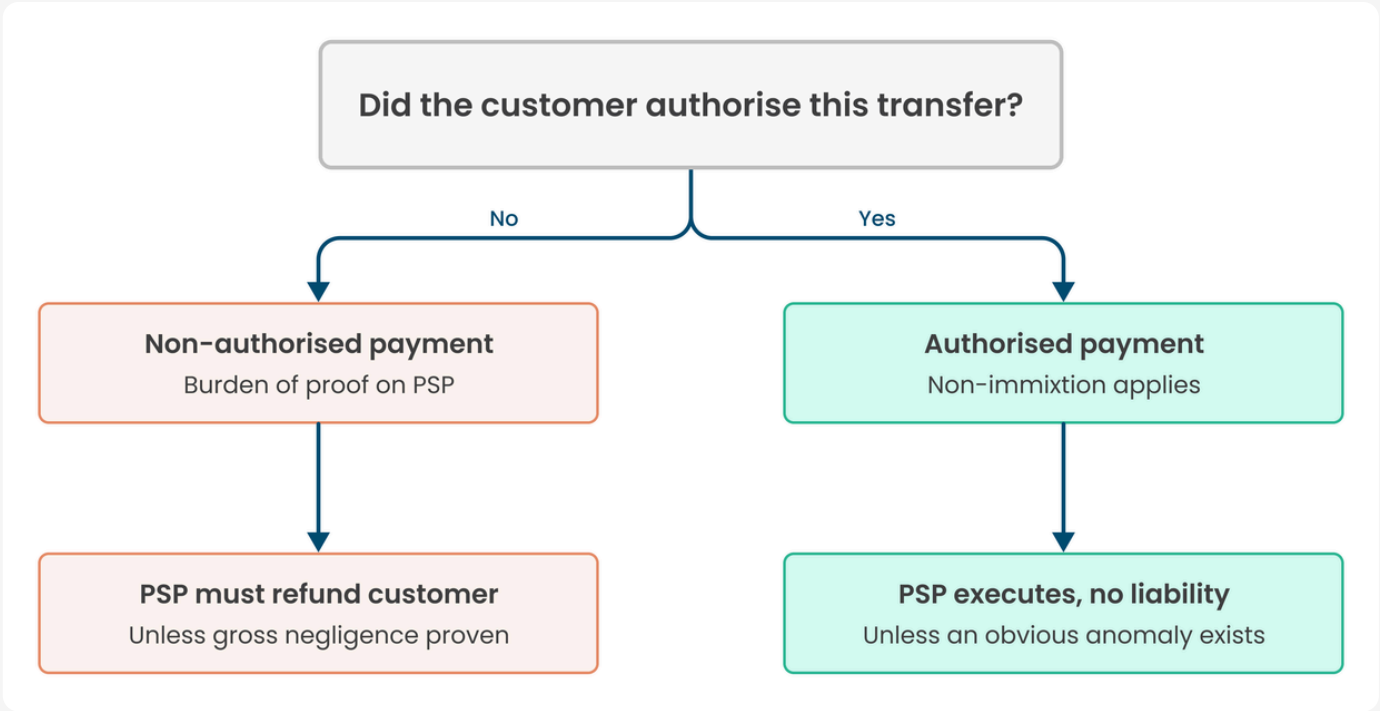


Card payment fraud remains the largest single category by value, but it is also the one furthest along its decline — a point covered in Section 1.3. The instrument to watch is wire transfer fraud, and specifically the manipulation-based share of it: in the first half of 2025, the Observatoire de la sécurité des moyens de paiement (OSMP) recorded a 37% increase in manipulation-based fraud (€245 million), the only category still accelerating into 2025.

That acceleration coincides with a second structural shift: instant transfers have gone from a minority option to the default, up 46% in volume in 2024 alone. The combination of the two trends — manipulation fraud rising, and transfers settling instantly — is what makes this fraud materially harder to stop than the fraud types that preceded it.

A standard bank transfer does not, by law, grant a general right to cancellation after the payment service provider (PSP) receives the order; however, operational intervention may still be possible until the order has been executed. Instant bank transfers, executed in a few seconds, significantly reduce this window. That time compression, more than the raw loss figures, is the reason technical defences alone can no longer carry the weight on their own (Section 1.3), and the reason a shared, real-time register like the FNC-RF became necessary rather than optional.

1.2 The structural problem: authorised versus non-authorised fraud



A non-authorised payment is one to which the account holder did not consent. This may occur where a criminal gains access to banking credentials and executes a transfer without the customer's knowledge, but also in more complex fraud scenarios where the customer denies having authorised the specific payment transaction. Under PSD2 (Revised Payment Services Directive), as transposed into French law, a payment transaction is authorised where the payer has given consent to its execution (Article L. 133-6 CMF). Where the user denies having authorised the transaction, Articles L. 133-18 to L. 133-24 CMF provide the specific refund and liability regime applicable to non-authorised payment transactions. The burden of proof is on the bank: it must first demonstrate that the operation was correctly authenticated, registered, and executed without technical failure before it can invoke gross negligence by the customer, and must characterise that negligence precisely and with full factual context (Cass. com., 30 April 2025, n° 24-10.149; 12 June 2025, n° 24-13.777).

An authorised payment is different. Here, the victim is manipulated into instructing the transfer themselves — through impersonation of a bank agent, a false invoice substituted into a legitimate email thread (FOVI fraud), a convincing scam call, or other forms of social engineering. In principle, the bank must execute a valid order and refrain from interfering in its client's affairs. However, its liability is not ruled out as a general matter: it may be held liable when apparent irregularities (easily detectable by a reasonably diligent professional) should have prompted verification of the order's validity. (notably, see Cass. com., 25 March 2026, n° 24-18.093).

High-value, numerous, international, or closely spaced transfers do not necessarily, in isolation, constitute an apparent anomaly; the analysis remains contextual. Thus, a combination of indicators—relating notably to the unusual nature of the amounts, the repetition of orders, their timing, the beneficiaries, and the geographical area—may necessitate verification (Cass. com., October 2, 2024, No. 23-13.282), whereas other scenarios do not give rise to bank liability (Cass. com., June 12, 2025; January 14, 2026). Furthermore, a payment service provider (PSP) is not, solely by virtue of executing transfers intended for investment in crypto-assets, subject to a duty to provide investment advice (Cass. com., March 25, 2026, No. 25-10.353).

Crucially, courts have also confirmed that Anti Money Laundering vigilance obligations — under Articles L. 561-4-1 to L. 561-14-2 CMF — exist solely for the purpose of combating money laundering and terrorist financing. A fraud victim therefore cannot rely on a bank's failure to meet its AML obligations as the basis for a civil damages claim (Com., 4 March 2026, n° 24-19.588).

> All of these difficulties constitute a liability gap, the structural vulnerability that fraudsters exploit. The FNC-RF does not close it (The future European Payment Services Regulation (PSR), if adopted in the currently available compromise version, will more directly alter the rules regarding supervision and liability.). What FNC-RF does, however, is give PSPs the intelligence to intervene before a manipulated payment reaches a known fraudulent account, and to build a documented record showing they acted based on that intelligence.

1.3 Why technical defences alone are no longer sufficient

The OSMP's H1 2025 statistics tell a precise story about the limits of authentication-only defences. Card fraud (where 3-D Secure and strong authentication have been most effectively deployed) fell 9.8% to a historic low fraud rate of 0.048%. Cheque fraud declined 16%. These are genuine successes.

Yet, manipulation-based fraud, which can bypass authentication entirely by exploiting human psychology, rose 37%. Fraudsters have adapted their toolset accordingly: having lost the ability to spoof bank phone numbers (the MAN mechanism, an authentication system to prevent fraudsters from displaying a bank's genuine phone number, curbed this), they now use ordinary mobile numbers ("06" and "07" prefixes) or instant messaging application calls to approach victims, impersonating bank staff and instructing customers to "secure" their funds by transferring them.

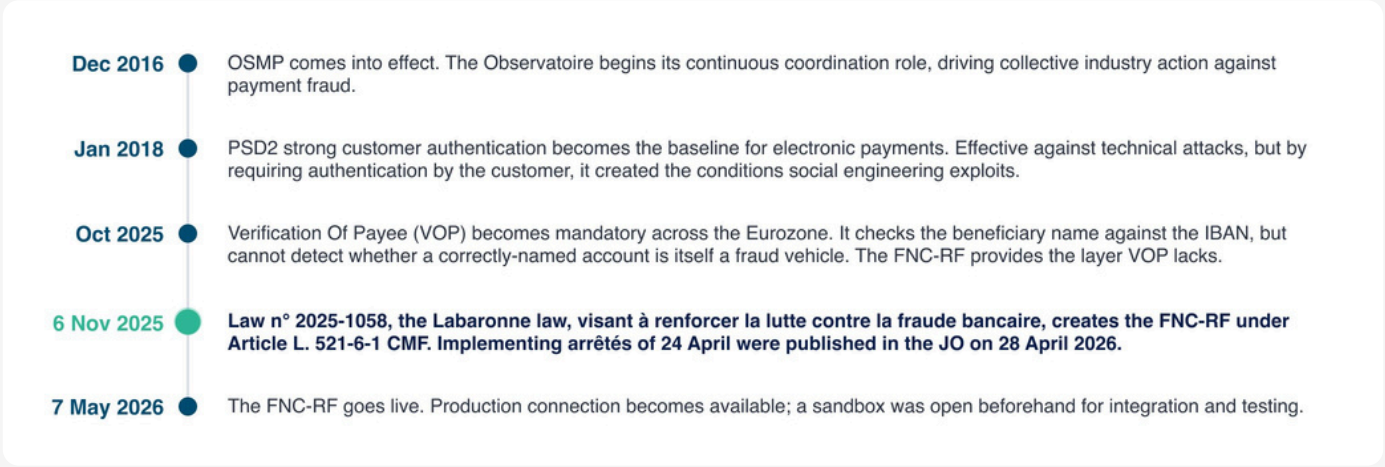
The economic incentive has also changed. Instant wire transfers grew by 46% in volume during 2024 and 70% in H1 2025 (following the January 2025 fee equalisation with standard transfers). This means that when fraud occurs, it occurs in seconds. The window for detection and intervention is narrowing down.

Against this background, any purely technical solution, however well-designed, faced a structural ceiling. What was missing was collective intelligence: the ability for one bank's discovery of a fraudulent account to benefit every other bank immediately. The FNC-RF fills that gap by enabling the sharing of information.

2. The Regulatory Background

2.1 The regulatory journey: from PSD2 to the Labaronne law

The FNC-RF did not emerge in isolation. It is the latest in a sequence of regulatory measures, French and European, designed to contain payment fraud as the threat landscape evolved.



PSD2 established strong customer authentication as a central element in the security of electronic payments, introducing the step-up authentication, transaction risk analysis, and liability frameworks still in force today. It was effective against technical attacks — but by requiring the customer to authenticate the transfer rather than the bank, it inadvertently built the exact condition social engineering exploits: once a fraudster talks a customer into authenticating, that authentication record then works against the victim, not for them, in any subsequent dispute.

The OSMP's coordinating role, running continuously since 2016, has followed the same closing-the-gap logic: its June 2024 action plan on remote card payments without 3-D Secure produced a sharp drop in card fraud, and its deployment of the MAN mechanism closed the bank-phone-number spoofing route fraudsters had been using. That role now extends to the FNC-RF too — going forward, the OSMP's own performance indicators will incorporate FNC-RF data.

Verification of Payee (VOP) is a narrower fix than it looks, and its rollout itself is staged: mandatory across the Eurozone from October 2025, but not until July 2027 for non-Eurozone SEPA countries. Mechanically, it checks whether the beneficiary's name matches the IBAN entered at payment initiation, generating a warning — not a block — on any mismatch. That stops one specific manipulation, a substituted IBAN in correspondence, but verifies identity, not intent: a correctly-named account can still be a money mule's account, and VOP has no way to know that. That's precisely the gap the FNC-RF is built to close, and why the two are designed to work together rather than as alternatives.

2.2 The Labaronne law and its legislative context

Proposed by Daniel Labaronne, Member of Parliament for Indre-Et-Loire, Law n° 2025-1058 of 6 November 2025 visant à renforcer la lutte contre la fraude bancaire creates the FNC-RF as a new instrument under Article L 521-6-1 of the Code monétaire et financier. The law has been refined over the course of its legislative passage, with over a thousand amendments introduced by April 2026; the implementing arrêtés of 24 April were published in the Journal Officiel on 28 April 2026.

Beyond the FNC-RF itself, the Labaronne law also strengthens the existing Fichier National des Chèques Irréguliers (FNCI): Article 3 reinforces the obligation for the drawee bank to report forged or counterfeit cheques, while Article 4 expressly allows the banker to consult the FNCI when a cheque is presented for payment in order to verify the regularity of its issuance. In practice, banks will be able to query the FNCI via a new specific access.

The FNC-RF is consciously designed to bridge to the coming European regulatory architecture. It anticipates the fraud intelligence sharing provisions of the Payment Services Regulation (PSR, Article 83a), which will become mandatory across the SEPA zone once PSD3/PSR is finalised and enforced, and is architecturally compatible with the European Payments Council's FRIDA (Fraud Information Distribution Arrangement) framework, which envisages a "network of networks" structure for SEPA-wide intelligence sharing.

2.3 The coming European layer: PSD3, PSR, and FRIDA

PSD3 and the accompanying Payment Services Regulation are expected to be finalised in 2026 and to enter into force within 18 months of publication. The PSR (Article 83a) will introduce a binding obligation on PSPs across the SEPA zone to share fraud intelligence, with FRIDA as the likely technical vehicle. A trilogue agreement was reached in November 2025, with ongoing technical discussions.

The FNC-RF is expected to act as France's connection point ("FIP" status) into that European layer, with an indicative effective FRIDA start around summer 2028 — 21 months after promulgation of the PSR. This is more precise than earlier public guidance, which referred only to "around 2028."

The future European framework is expected to broaden the scope of data shared beyond IBANs alone, potentially including payer behavioural data, IP addresses, and other environmental signals. It also envisages extending intelligence sharing to direct debits (ICS/prélèvements).

This extension is not settled, however the Banque de France noted that declaring creditor IBANs linked to direct debits and fraudulent trade instruments (effets de commerce) "seems of limited use to some PSPs," and the topic has been deferred to a later date for confirmation by market specialists. Similarly, the idea of also declaring IBANs linked to fraudulent cheques within the FNC-RF has been definitively abandoned, since the existing FNCI (Fichier national des chèques irréguliers) already serves that need.

Foreign IBANs cannot currently be classified as fraudulent within the FNC-RF. The French law does require that suspected fraud be reported regardless of the origin of the IBAN (whether French, Eurozone, or outside the SEPA zone) but the classification of those foreign IBANs as fraudulent will only be possible once the system is extended to the European level, expected around 2028. In the meantime, the FNC-RF's Malware Information Sharing Platform (MISP) architecture is explicitly designed for eventual interoperability with the EPC's FRIDA platform.

PSD3 is also expected to go further than PSD2 in clarifying liability in social engineering scenarios, potentially shifting greater responsibility onto PSPs. Institutions should anticipate that their FNC-RF integration and documentation will form part of the evidence base when demonstrating that they discharged their duty of care in a disputed authorised payment.

3. What the Law Requires

3.1 Who must participate

Two important scope clarifications have since been confirmed. First, URSSAF (the social security contributions collection body) was initially included as a reporting entity under the social security fraud law. That law has now been adopted by Parliament: Article 9 formally abrogates URSSAF's Article L. 521-6-1 (III) reporting access, since URSSAF is not subject to the same ACPR supervisory framework as PSPs. In its place, the same Article 9 adds a new Article VIII to L. 521-6-1, granting read-only consultation access to financing companies (sociétés de financement) and certain administrations, for financing-related purposes — covering an estimated 151 entities listed in the Banque de France's REGAFI register.

Separately, the technical arrêté confirms that foreign PSPs — those without a French or passported presence — cannot connect to the FNC-RF or obtain communication of its contents, and in particular cannot "qualify" fraud events concerning their own customers, since the Banque de France will not add foreign BIC codes to its central referential. In practice, this creates a real operational friction for merchant clients and false-positive disputes originating from foreign PSPs: the Banque de France has said it will collect a dedicated contact point (mailbox) at each French PSP to relay clarification and access requests it receives from foreign PSPs on their behalf.

Second, and more significantly for the market: institutions benefiting from a European passport to operate in France are no longer within the scope of connection to the database. French law cannot impose obligations on these participants without approval from European authorities, which has not been granted. A confirming decree was anticipated at the end of May 2026. Passported institutions should monitor this development closely, as their inclusion may follow once the European PSR framework is in place.

3.2 The reporting obligation: "as soon as possible"

The obligation to report is mandatory and must be fulfilled as quickly as possible. The wording "dans les plus bref délais", rendered in English as "as soon as possible", was the subject of extensive legislative debate. It was ultimately aligned with the standard already used in French anti-terrorism legislation, setting a precedent and closing the debate. The practical target, endorsed by the Banque de France, is that a fraudulent account should remain active for no more than 24 to 48 hours after being identified by the reporting institution.

The Banque de France cannot impose a hard deadline because it does not have access to the triggering event that gives rise to the obligation. Instead, it will monitor the quality and frequency of each institution's reporting through performance indicators, and the ACPR may sanction institutions that fail to meet the spirit of the obligation.

3.3 The three roles: Reporting PSP, Account-Holder PSP, Participant PSP

The obligations under the FNC-RF differ materially, depending on a PSP's role in relation to any given fraud event. There are three distinct roles.

Reporting PSP	The institution that detects a suspected fraud event and creates the report in the register. It must submit all required data fields, correct or withdraw the report if new information changes the picture, and ensure each fraud event generates exactly one declaration.
Account-Holder PSP	The institution that holds the account identified in a fraud report. It bears the most demanding operational obligation: it must indicate without delay that it is taking charge of the investigation, conduct verification of the account's fraudulent character, and share its qualification outcome back into the register. It must also report any identity theft (as defined in Article 226-4-1 of the Penal Code) it detects.
Participant PSP	Any other in-scope PSP that receives the intelligence feed. It may optionally record its own assessment of an event's fraudulent character (a "sighting") or flag it as a false positive, contributing to the collective quality of the register.

This three-role architecture is important for compliance planning. Most PSPs will simultaneously occupy all three roles depending on the fraud event: they will be the reporting institution for frauds they detect, the account-holder institution for alerts raised by others concerning their customers, and a participant for the broader intelligence feed they consume.

→ 3.4 What type of data is shared

The Labaronne law partially lifts banking secrecy to enable the FNC-RF, but the scope of data shared is deliberately narrow. The register does not share individual identities. For each fraud event, the following fields are declared:

- The account identifier: IBAN or BBAN, plus the BIC of the institution holding the account
- Detection date and last update date
- Fraud category (the type of fraud among the known major categories)
- Fraud source: elements concerning the method used by the fraudster (optional field)
- Transaction type: the payment instrument or customer action that was the subject of the fraud
- Transaction channel: the channel through which the transaction originated (optional field)
- Whether a complaint or claim for identity theft has been filed by the payment service user
- The reporting institution and a unique event UUID
- Qualification by the account-holder PSP and qualification by participant PSPs

Foreign IBANs must be reported where suspected fraud is identified, regardless of origin, but cannot be classified as fraudulent within the register until the European extension of the system. Multiple fraud events may relate to the same beneficiary account, creating multiple distinct MISP objects; deduplication is the responsibility of each PSP operating locally.

→ 3.5 The prohibition on blacklisting

One of the most important limitations of the FNC-RF is also one of its defining features: the register is explicitly not a blacklist. The law prohibits the automatic blocking of transactions to an IBAN simply because it appears in the database. PSPs are required to conduct an independent analysis before taking any action.

Inclusion in the FNC-RF does not in itself give grounds to terminate a banking relationship, freeze a customer account, or block legitimate transactions. The register is structured as an instrument of vigilance and intelligence, not of automatic sanction. An institution that acts on the basis of register inclusion alone, without conducting its own analysis, risks breaching both the letter of the law and the rights of its customers.

> The FNC-RF is a tool for informed decision-making, not automated blocking. Institutions must build internal processes that use the register's intelligence appropriately (enriching risk assessments and triggering investigations), while preserving the rights of account holders.

3.5a Manipulated and mule accounts: the "compte régularisé" qualification

The prohibition on blacklisting is reinforced by a specific qualification value introduced through the Règles d'usage to handle a recurring edge case: accounts used without their holder's knowledge (account takeover) or after the holder was manipulated (e.g. romance scams), and — at the margin — accounts used with the holder's consent but where the account-holder PSP assesses there is no risk of recurrence.

Left unaddressed, this creates a lose-lose qualification problem: qualifying such an account as “fraudulent” overstates the risk and causes other participants to block legitimate transfers to it, while qualifying it as “legitimate” wrongly records a genuine fraud event as a false positive. The Banque de France's solution is a third qualification value, “compte régularisé” (REGUL), which the account-holder PSP may apply at its own discretion to indicate the account may resume receiving transfers despite the past fraud occurrence. Participants must not treat a REGUL-tagged account as risky on the strength of its FNC-RF presence alone, and the Banque de France excludes REGUL accounts from its false-positive statistics. As a safeguard against misuse, participants are expected to raise their internal risk assessment of a REGUL account if it reappears in a new fraud event, and the Banque de France tracks usage of this value through its KPI programme.

3.5b Vigilance on virtual IBANs

The Règles d'usage also flag a related evasion technique: rather than reusing the same IBAN, a fraudster may generate a new virtual IBAN for each fraud event specifically to avoid being caught by FNC-RF sharing. The recommended practice (not a binding rule) is that where a declared IBAN turns out to be a virtual IBAN, the PSP holding the underlying master account should apply heightened vigilance to any further virtual IBANs created by the same customer. This sits alongside, and does not replace, the account-holder PSP's ordinary qualification obligations.

→ 3.6 Retention and correction obligations

Data entered in the register is subject to a 13-month retention period from the date of declaration, in the absence of earlier removal. Institutions are under a strict obligation to submit corrective declarations “without delay” whenever they hold new or contradictory information relative to what was initially reported. This includes withdrawing a report if the basis for suspicion is no longer founded.

Operationally, this correction obligation is implemented through an “event to delete” tag, which the Règles d'usage split into two categories: (1) false positive, where the suspected fraud is not substantiated, and (2) any other deletion motive, in particular technical duplicates. Participants must apply this tag as soon as they identify grounds for deletion, and must remove the event from their own local system at the earliest opportunity once tagged.

The Banque de France maintains the central platform but is not responsible for the accuracy of individual entries. Each reporting PSP is responsible for the quality, timeliness, and accuracy of what it contributes.

4. How the FNC-RF Works in Practice

→ 4.1 The technical architecture

The FNC-RF is built on MISP, an open-source threat intelligence platform originally developed for cybersecurity but adapted here for payment fraud. The Banque de France operates the central MISP hub, which serves as the trusted third party and single source of truth for the national register.

Each fraud event is represented as a MISP object (“Compte douteux”) with the data fields described above. When multiple fraud events are created for the same beneficiary account, there will be as many MISP objects as there are events — the central platform does not consolidate or deduplicate across objects. Local deduplication and consolidation are the responsibility of each PSP.

The system returns a binary response to queries: yes or no — has this IBAN been reported as suspicious? The architecture is designed for near-real-time dissemination, with the stated goal of ensuring that a fraudulent account cannot remain active across multiple institutions for more than 24 to 48 hours after being flagged. Pilot tests with banking groups have already validated this: reductions in fraudulent activity following the flagging of an account were measured in days.

→ 4.2 Connectivity options

The FNC-RF accommodates the varying technical capabilities of PSPs through three connection modes:

MISP Hub Sync	PSPs that run their own MISP instance synchronise their local database with the central Banque de France (BdF) hub. This requires maintaining a local MISP installation and managing synchronisation schedules, but gives maximum control over local data processing.
Direct API	PSPs interact with the central or local data hubs via API calls, either per transaction or as scheduled batch synchronisations. This is technically simpler than running a full MISP instance but offers less local processing flexibility.
TSP Integration	PSPs may engage a Technical Service Provider (TSP) that is itself directly connected to the Banque de France platform, and interact with the FNC-RF through that intermediary. This is the lowest-complexity option for institutions without dedicated technical infrastructure.

Regardless of connectivity mode, access to the platform requires a certified digital certificate: either one issued by the Banque de France's own certification authority (IGC Banque de France), an RGS **/*** qualified certificate, or a certificate from a qualified certification authority under the eIDAS regulation. The recommended approach is an RGS **/*** authentication certificate, though software-based authentication certificates are also permitted provided the private key is appropriately secured. The list of certification authorities accepted by the Banque de France for the FNC-RF is available in the dedicated FAQ on the Banque de France website.

PSPs must submit a formal connection request before gaining access. For the homologation (testing) phase, contacts at the Banque de France are: FNC-RF@banque-france.fr for the business connection request and Mohamed.BOULOUZ@banque-france.fr for technical connectivity and test monitoring.

→ 4.3 Go-live timeline and run-in period

Production connection has been available from 7 May 2026 onwards. A sandbox environment for integration and testing was available before that date. The Banque de France recommends a run-in period of one to three months before full operational exploitation, during which institutions can validate their reporting flows in production conditions with initial customers. PSPs must maintain a synchronised local copy of the central FNC-RF dataset to meet their operational and compliance requirements.

→ 4.4 The operational lifecycle of a fraud event

Understanding how a fraud event flows through the system is essential for building compliant internal processes. The lifecycle has distinct phases depending on the institution's role.

→ For the Reporting PSP (outbound reporting)

- Internal fraud detection identifies a suspicious beneficiary IBAN based on internal analytics or a customer complaint.
- A fraud event declaration is submitted to the Banque de France MISP with all required fields correctly mapped to the FNC-RF specification. Each identified fraud event generates exactly one declaration.
- The alert is ingested by the Banque de France and becomes live on the network, immediately available to all participants.
- The reporting institution monitors the subsequent qualification outcome from the account-holder PSP.
- If new or contradictory information emerges, a corrective declaration is submitted without delay.

→ For the Account-Holder PSP (qualification obligation)

- An inbound alert is received matching an IBAN belonging to the institution's customer base.
- The institution sets the qualification value to "EN COURS" as soon as it becomes aware of the declaration through local synchronisation, unless a definitive qualification is already available.
- The institution must indicate in the register "without delay" that it is taking charge of the investigation (to allow the reporting PSP to track the declaration).
- A due-diligence investigation is conducted to assess whether the account is genuinely fraudulent.
- The qualification outcome (confirming or refuting the fraudulent character of the account) is recorded back into the register.
- Optionally, a false-positive notification may be submitted to the Banque de France if the institution concludes the initial report was unfounded.

→ For all Participant PSPs (consuming the feed)

- The FNC-RF feed is synchronised regularly (the Banque de France platform allows synchronisation approximately four times a day, with manual refresh available at any time).
- Before executing a wire transfer, institutions can query the register to determine whether the destination IBAN has been flagged as suspicious.
- If a match is found, the institution's fraud risk process is triggered. This does not mandate automatic blocking but requires analysis. Typically, this results in a customer alert (see Section 4.5).
- Participant PSPs may log their own assessment of individual events as sightings or false positives, contributing to collective intelligence quality.

4.5 Integration with VOP and the customer alert use case

The most significant near-term operational use case is the enrichment of the VOP process with FNC-RF intelligence. When a customer initiates a wire transfer, the existing VOP check already verifies that the beneficiary's name matches the account. The FNC-RF adds a second layer: if the destination IBAN is present in the register, the institution can alert the customer at the point of payment initiation.

A typical customer-facing alert might read: "Warning: this IBAN has been flagged as suspicious by other financial institutions. It may be associated with fraudulent activity. Do you wish to proceed?" The decision remains with the customer (as the law does not permit automatic blocking), but the institution has discharged its duty of care and created a record of having done so.

This alert mechanism is legally significant. In the context of an authorised payment dispute, an institution that can demonstrate it warned the customer before the transfer was executed (and that the customer chose to proceed) is in a substantially stronger position than one that had no mechanism for doing so. PSD3's expected clarification of liability in social engineering scenarios will make this documentation even more important.
The specific operational parameters for how institutions use FNC-RF data in their internal systems (what thresholds trigger alerts, what internal processes follow a match) are left to institutional discretion. The law defines the intelligence-sharing obligation; it does not prescribe how institutions act on that intelligence.

5. Jurisprudence: The Duty of Vigilance in Practice

The FNC-RF does not exist in a legal vacuum. Courts have been actively developing the liability framework applicable to authorised and non-authorised transactions within which the FNC-RF operates. The following case law, drawn from recent Cour de cassation decisions, defines the current state of play and illustrates why the FNC-RF's documentation and alert capabilities matter operationally.

→ 5.1 Non-authorised payments: burden of proof and gross negligence

For non-authorised payments, the statutory regime under Articles L. 133-18 to L. 133-24 CMF places the burden squarely on the PSP. The bank must first prove that the operation was correctly authenticated, recorded, and executed without technical failure. Only then can it invoke gross negligence by the customer (and it must characterise that negligence with precision and supporting factual context). Two requirements from the customer side also apply:

- The customer must report the disputed transaction "without delay" from the moment they become aware of it. Failure to do so through gross negligence can strip them of refund rights, independently of the 13-month deadline (Cass. com., 14 January 2026, n° 22-14.822).
- Failure to establish the date of notification to the bank is fatal to the refund claim — the court of appeal's refusal was upheld on this ground alone (Cass. com., 4 February 2026, n° 22-22.609).

→ 5.2 Authorised payments: the non-immixtion principle and its limits

For authorised payments, the doctrine of non-immixtion defines the boundaries of bank liability. Recent decisions illustrate its application:

Case	Payment Type	Key Holding
Cass. com. June 12, 2025 ; n° 24-10.168 ;January 14, 2026, n° 24-19.102	Authorised	Wire transfers that are merely high-value, numerous, or cross-border do not alone engage bank liability. A contextual bundle-of-clues analysis is required.
Cass. com. January 14, 2026 n° 24-19.102	Authorised	The receiving bank is not required to verify the origin or size of credited funds, nor to question its customer about large movements, absent an obvious and easily detectable anomaly.
Cass. com. March 25, 2026 n° 24-18.093	Authorised	The account-holding bank's duty is limited to verifying the regularity of the payment order. Absent obvious anomalies detectable by a normally diligent professional, it must execute promptly and cannot interfere.
Cass. com., 25 March 2026, n° 25-10.353	Authorised	A bank receiving a transfer order for the purpose of investing in crypto-assets acts strictly in the capacity of a payment service provider (PSP). It is under no obligation to provide advice or warnings regarding investment risks, even where there are multiple large transfers to a foreign bank. The Court of Cassation overturned the Court of Appeal's decision.
Com. March 4, 2026 n° 24-19.588	Authorised	AML vigilance obligations (Arts. L. 561-4-1 to L. 561-14-2 CMF) exist solely for anti-money-laundering purposes. A fraud victim cannot invoke a bank's AML failures as the basis for a civil damages claim.

→ 5.3 What this means for FNC-RF compliance

Read as a whole this case law reinforces threeepp conclusions for PSPs building their FNC-RF posture.
First, in the case of an authorised payment, the mere presence of the destination IBAN in the FNC-RF does not automatically constitute an "obvious anomaly", nor does it automatically justify blocking the transaction. It is, however, an additional factual indicator that may become relevant in a subsequent dispute. The PSP should therefore be able to show whether it queried the register, whether the alert had been qualified, whether the customer was warned, whether the payment was suspended or executed, and how that decision was justified.

Second, the account-holding PSP's own response may also become relevant. Where it receives a signal concerning one of its customers, the timing and quality of its investigation, its qualification of the account and any corrective declaration will form part of the operational record. FNC-RF compliance should therefore be designed not merely as a reporting obligation, but as a process in which each institution must be capable of demonstrating how it reacted to the information it had.

Third, FNC-RF and AML/CFT procedures should remain legally distinct. An FNC-RF alert may also justify an AML escalation, particularly where an account appears to be used to receive or transfer criminal proceeds. However, the two regimes pursue different purposes, impose different obligations and have different consequences for civil liability. Internal procedures and responses to customer complaints should therefore identify clearly which regime is being applied.

5.4 The proposed PSR framework

The proposed Payment Services Regulation is in line with current French law provisions. It preserves the distinction between authorised and non-authorised transactions and extends the transaction monitoring obligation to the receiving PSP. It also includes provisions regarding manipulation fraud, transaction monitoring and suspension of payment orders. The most important change would lie in the implementation of fraud-information sharing agreements, as it may require the French framework to be reviewed in relation to the categories of information exchanged, security and confidentiality measures, governance arrangements, data protection impact assessment, and cross-border interoperability.

As a reminder, under current French law provisions, a payment transaction is authorised where the payer has consented to its execution. Non-authorised payment transactions are subject to the reimbursement regime set out in Articles L. 133-18 to L. 133-24 CMF. Where the user denies having authorised a transaction, the PSP must prove that it was authenticated, duly recorded and entered in the accounts, and was not affected by a technical or other deficiency.

French case law applies this regime to spoofing cases where the customer has carried out authentication or security-related steps because instructed by the fraudster to do so, but has not consented to the specific payments executed. In such circumstances, the transactions will usually be treated as non-authorised, and the PSP must reimburse them unless it establishes fraud or gross negligence by the customer.

For quick reference, the five operative PSR articles are summarised below; the detailed mechanics of each follow in the paragraphs beneath the table.

Article	Who it binds	Core obligation	Consequence of non-compliance
Art. 59	Payer's PSP	Refund fraudulent authorised payments where a third party impersonated the PSP itself, using communication channels attributed to that PSP	Must refund within 15 business days unless it proves consumer fraud or gross negligence
Art. 65	Payer's PSP	Suspend execution on justified suspicion; recontact payer; decide whether to execute or refuse	Payer does not bear the loss if the PSP failed to suspend despite justified suspicion (unless payer acted fraudulently)
Art. 69	Payer's PSP	May withhold funds on ordinary suspicion; must withhold and return where reasons are clear and incontrovertible	Payer does not bear the loss if the payee's PSP failed to withhold as required (unless payer acted fraudulently)
Art. 83	Both payer's and payee's PSP	Maintain transaction monitoring before execution (payer side) and before release of funds (payee side)	Liable PSP must refund the payer if it cannot evidence monitoring was carried out (unless payer acted fraudulently)
Art. 83a	All participating PSPs	Share fraud intelligence via an information-sharing arrangement (the FNC-RF's likely role), excluding normal-use behavioural/environmental data	Joint DPIA required; five-year maximum retention; no account action on shared data alone without independent PSP assessment

Article 59

The PSR would retain a specific regime for non-authorised payment transactions, similar to the current French regime. Article 59 would establish a reimbursement regime for certain fraudulent authorised payment transactions. It would apply where a consumer has been manipulated by a third party pretending to be the consumer's PSP, using communication channels attributed to that PSP, and that manipulation has resulted in a fraudulent authorised payment transaction.

The consumer would be required to notify the PSP without undue delay after becoming aware of the fraud and to report the fraud to the police. Within 15 business days of receiving the notification and police report, the PSP would be required either to refund the transaction or to provide reasons for refusing reimbursement. Reimbursement would not be required where the consumer acted fraudulently or with gross negligence. As with French law, the burden of proving fraud or gross negligence would lie with the consumer's PSP.

Article 83

The PSR would also introduce express transaction monitoring obligations. Under Article 83, PSPs would be required to maintain transaction monitoring mechanisms to support strong customer authentication and to prevent and detect potentially fraudulent payment transactions. The payer's PSP would be required to carry out monitoring before execution of the transaction, while the payee's PSP would be required to carry out monitoring before making the funds available to the payee.

Where a PSP fails to carry out the required monitoring and the payer suffers financial damage, that PSP would bear liability. Where the payer's PSP cannot provide evidence that the monitoring was carried out by both the payer's PSP and the payee's PSP, it would be required to refund the payer. Except where the payer acted fraudulently, the payer would not bear the financial consequences of the transaction. The burden of proving compliance would rest on the PSP concerned.

Article 65

The aforementioned article must be read in conjunction with article 65, which sets the liability regime applicable to authorised transactions. Similarly to the French regime, where there would be reasons, arising either from transaction monitoring or other relevant information available to the PSP to suspect fraud, the PSP would be required to suspend execution of the transaction.

Following suspension, the PSP would be required, where possible, to contact the payer and assess whether the reasons for suspicion remain justified. It would then decide whether to execute or refuse the payment order. Where the PSP had objectively justified reasons to suspect fraud but failed to suspend the transaction, the payer would not bear the resulting financial loss, except where the payer acted fraudulently. The burden of proving compliance would lie with the PSP.

Article 69

Article 69 would provide corresponding rules for the payee's PSP. Where transaction monitoring or other relevant information gives the payee's PSP objectively justified reasons to suspect that a transaction credited or to be credited to the payee's account is fraudulent, it may decide not to make the funds available and to return them to the payer's PSP. Where the reasons for suspicion are clear and incontrovertible, the payee's PSP would be required to withhold and return the funds.

If the payee's PSP failed to comply with that mandatory obligation, the payer would not bear the financial loss, except where the payer acted fraudulently. The burden of proving compliance would lie with the payee's PSP.

Article 83a

Finally, article 83a would require PSPs to participate in information-sharing arrangements with other PSPs and to exchange data where they have objectively justified reasons to suspect fraudulent behaviour by a payment service user. The information exchanged would be used for the purposes of the transaction-monitoring obligations set out in Article 83.

The information shared would be limited to the categories identified in Article 83, the objectively justified reasons giving rise to the suspicion and, where relevant, notifications made to hosting service providers. Environmental and behavioural characteristics typical of the payer's normal use of personalised security credentials would not be shared under Article 83a.

Additional notes

Participating PSPs would be required to implement appropriate technical and organisational measures to ensure the security and confidentiality of the information exchanged, including measures permitting pseudonymisation. The information-sharing arrangement would have to define its conditions of participation and operational arrangements, including any dedicated IT platform used for the exchange.

Before entering into the arrangement, participating PSPs would jointly carry out a data protection impact assessment and, where required, consult the competent data protection authority.

Information received through the arrangement could not be retained for longer than necessary for transaction-monitoring purposes and, in any event, for more than five years after the suspected fraudulent transaction. PSPs would also be prohibited from terminating a contractual relationship, affecting future onboarding or taking another decision affecting the customer relationship solely on the basis of information received from another PSP without first carrying out their own assessment.

The FNC-RF already operates as a French national information-sharing arrangement concerning accounts suspected of being used for payment fraud. It also applies a comparable principle of independent assessment: inclusion of an account in the register does not, by itself, prohibit payment transactions or justify termination of the relevant account or payment-services relationship.

Article 83a does not require the creation of a single central EU database or the replacement of existing national arrangements. The FNC-RF could therefore continue to operate as the French information-sharing mechanism, provided that its legal, technical and operational framework complies with Article 83a.

This may require the French framework to be reviewed in relation to the categories of information exchanged, security and confidentiality measures, governance arrangements, data protection impact assessment and cross-border interoperability. The five-year period in Article 83a is a maximum retention period and would not, by itself, require the current 13-month FNC-RF retention period to be extended.

Participation in the FNC-RF would not necessarily be sufficient on its own to satisfy Article 83a where the required information sharing extends beyond the French perimeter. The FNC-RF may therefore operate as the French component of the future European information-sharing framework, subject to any adaptations required when the PSR is formally adopted and becomes applicable.

6. Compliance, Monitoring, and Legal Obligations

6.1 The reporting obligation as a legal requirement

Connecting to the FNC-RF, reporting suspected fraud events, and qualifying alerts relating to held accounts are statutory obligations under the Labaronne law, not best practices. A PSP that fails to report a suspected fraud, fails to update an alert when circumstances change, or fails to take charge of the alert without delay and to share the result of its verification as soon as possible is not merely falling short of good practice — it is in breach of its legal obligations.

The Autorité de Contrôle Prudentiel et de Résolution (ACPR) monitors compliance and may impose sanctions on institutions that do not meet their obligations. The Banque de France will implement performance indicators to track reporting quality and frequency across all participants, feeding the results into the OSMP's annual report. Four categories of KPI are in scope:

- Data-sharing contribution: whether participants are fulfilling their reporting obligations and engaging with the platform as the regulatory and usage framework requires.
- Technical compliance: whether data submitted meets the technical standards set by the Banque de France.
- Data-sharing effectiveness: measurement of fraud prevented and false-positive rates, assessing the real-world impact of the register.
- Fraud analysis: statistical reporting on fraud types, sources, and typologies feeding into the OSMP's annual report and broader market intelligence.

6.2 Wrongful listing: the obligation to correct

The flip side of the obligation to report is an equally strict obligation to correct. PSPs must submit corrective declarations without delay whenever they hold new or contradictory information. No account may be maintained in the register once the basis for suspicion has changed or been resolved.

Institutions bear responsibility for deduplicating flagged accounts locally and maintaining the accuracy of their contributions.

An institution that allows a stale or incorrect entry to remain in the register (through inaction or inadequate internal processes) is exposed to both regulatory and civil liability toward the wrongly listed account holder.

The FNC-RF is not a blacklist, and must not be treated as one. Any institution that uses register inclusion as the sole basis for closing an account, refusing a transaction, or terminating a banking relationship risks breaching both the Labaronne law and its obligations to its customers under the Code monétaire et financier.

6.3 GDPR compliance obligations for PSPs

The Arrêté of 24 April 2026 creates explicit GDPR obligations for PSPs. The Banque de France FAQ of 26 May 2026 provides practical guidance on their implementation. The following analysis draws on that FAQ and post-event guidance prepared following the event of 28 May 2026. It is a practical interpretation, not a legal opinion; institutions should seek their own advice.

Obligation	What the law requires	Action required
T&C update (Art. 5 Arrêté / Arts. 12–14 GDPR / FAQ D.8)	PSPs must inform account holders that their data (account identifier, BIC, detection date, fraud category and type, transaction type, existence of identity theft claim) may be reported to the FNC-RF in cases of suspected fraud, and must explain how to exercise their data rights.	Add a specific FNC-RF clause to your General Account Terms and Conditions.
Access requests (Art. 8 Arrêté / Art. 15 GDPR / FAQ D.7)	The account-holder PSP is the exclusive point of contact for data subjects. When a customer requests access, you must tell them whether their account is in the register and for which fraud event(s).	Build an internal process to query the FNC-RF (via portal or API) in response to access requests, within the GDPR one-month deadline.
Rectification & limitation (Art. 8 Arrêté / Arts. 16 & 18 GDPR / FAQ C.9)	You must investigate the fraudulent character of the account without delay, update your qualification in the register, and where warranted ask the declaring PSP to submit a corrective or removal declaration.	Build an investigation and escalation workflow. Important: if the declaring PSP refuses to withdraw despite your contrary qualification, the entry stays in the register. BdF does not reconcile conflicting positions. Your obligation is to document all steps taken.
Data controllership (Art. 8 Arrêté / FAQ D.4)	Banque de France is the data controller for the central platform. Each PSP is the data controller for its own internal FNC-RF processes. There is no joint controllership between PSPs.	Document this processing activity in your Records of Processing Activities (RPA): legal basis Art. 6(1)(c) GDPR, 13-month retention period (from declaration or last corrective declaration, whichever is later), data subjects' rights and internal processes.
Right to erasure (Art. 17 GDPR)	Art. 17 is not cited in Art. 8 of the Arrêté — the omission is likely intentional, as Art. 17(3)(b) GDPR excludes erasure when processing serves a public interest mission. However, the Arrêté does not state this explicitly.	If you are the declaring PSP: you may request removal from BdF under Art. 4 of the Arrêté once the basis for suspicion has disappeared. If another PSP declared the event: you have no direct means to satisfy an erasure request. In both cases, document the reason for refusal or impossibility, inform the customer in writing, and remind them of their right to escalate to the CNIL.

Retention nuance: the 13-month period runs from the date of declaration or the date of the last corrective declaration, whichever is later. For contested or repeatedly updated events, effective retention can therefore significantly exceed 13 months from the original declaration. This must be reflected in your RPA documentation.

6.4 Liability and the duty of care

The FNC-RF does not resolve the authorised payment liability gap. Where a customer is manipulated into instructing a fraudulent transfer, and the bank executes it as instructed, the existing legal framework (as confirmed by the Court of Cassation) does not automatically hold the bank liable.

What the FNC-RF does is change the evidentiary position of PSPs in such disputes. By alerting a customer that a destination IBAN has been flagged as suspicious before the transfer is executed, and by documenting that alert and the customer's decision to proceed, an institution can demonstrate that it discharged its duty of care. In the absence of such a system — and such documentation — the institution's position in a future dispute is considerably weaker.

PSD3 is expected to go further by clarifying liability allocations in social engineering scenarios, potentially imposing greater responsibility on PSPs who can be shown to have had intelligence and failed to act on it. Institutions should treat their FNC-RF integration not merely as a regulatory compliance exercise but as the foundation of a defensible fraud risk management posture for the coming European regulatory cycle.

6.5 Costs: the system is entirely PSP-funded

The FNC-RF is entirely funded by participating PSPs. The Banque de France does not subsidise the operating costs of the platform. The CGU (Conditions Générales d'Utilisation) — the legal and contractual framework governing participation — covers the full billing and cost allocation structure, alongside connection and intermediation arrangements, data protection obligations, platform availability and support, and governance provisions. Institutions should obtain and review the CGU documentation from the Banque de France's FNC-RF portal before finalising their budgets.

7. Additional Legal Dimensions

7.1 The proposed internal fraud database

Separate from the FNC-RF, a specific bill is now before Parliament on this issue: Proposition de loi n° 3032, deposited at the Assemblée Nationale on 7 July 2026 by Daniel Labaronne — the same MP behind the original Labaronne law — and referred to the Commission des finances. It would create an automated national file recording individuals who committed serious breaches of integrity at a bank or financial institution, aimed at preventing fraud networks from placing complicit insiders in sensitive roles. Labaronne cites approximately 500 such breaches recorded in 2024, for an estimated €40 million in damage, drawn from major banking-network data. The bill is at first reading and has not yet been examined in the chamber; its design — feeding conditions, contestation procedures, access and rectification rights, and opposition rights — remains to be settled, and its ultimate adoption will depend on how those employee-protection questions are resolved. Institutions should monitor its progress, as it would create parallel reporting and data governance obligations alongside the FNC-RF.

7.2 The broader Labaronne law

The FNC-RF is the most visible component of Law n° 2025-1058 but not its only provision. The law also strengthens the FNCI (cheque register), codifies reporting obligations for forged cheque detection, and extends consultation rights at the point of cheque presentation. Institutions affected by both cheque and wire transfer fraud should review the full text of the law rather than treating the FNC-RF as its only operative part.

7.3 Interaction with AML and other French-law obligations

The FNC-RF sits alongside France's existing anti-money laundering (AML) framework rather than replacing any element of it. The suspicious account intelligence gathered through the FNC-RF may, in many cases, also trigger obligations under the AML regime, particularly where fraud patterns suggest that accounts are being used for layering of criminal proceeds. Compliance teams should ensure their internal processes connect FNC-RF matches to existing AML escalation workflows rather than treating them as separate streams.

ANNEX: A Practical Compliance Checklist for PSPs

This checklist summarises the key steps an in-scope institution must complete to achieve FNC-RF compliance. It is intended as a practical guide for project teams, not a substitute for legal advice on specific institutional circumstances.

1 Step 1 — Legal and Administrative

- [ ] Review the CGU (Conditions Générales d'Utilisation) from the Banque de France FNC-RF portal: https://www.banque-france.fr/fr/FNCRF, and complete the relevant bulletin d'adhésion, including acceptance of applicable billing terms (system is entirely PSP-funded; tariffs set by ministerial arrêté).
- [ ] Designate internal contacts: a business contact, a technical contact, and an internal point of contact for customer data rights requests relating to FNC-RF entries. Include your CIB number in the title of all communications to the Banque de France.
- [ ] Communicate to FNC-RF@banque-france.fr the email addresses and mobile numbers of all persons requiring access to the Banque de France (BdF) secure sharebox.
- [ ] Update General Account Terms and Conditions to include FNC-RF notification clause.
- [ ] Update the institution's Records of Processing Activities (RPA) with the FNC-RF processing activity, specifying Article 6(1)(c) GDPR as the legal basis and the 13-month retention period.
- [ ] Brief the DPO and CNIL define escalation pathway.
- [ ] Assign ownership of FNC-RF compliance within the compliance or fraud risk function

2 Step 2 — Technical Prerequisites (at least 15 days before testing)

- [ ] Confirm connectivity mode: MISP hub synchronisation, direct API, or TSP integration.
- [ ] Procure a qualifying digital certificate from an authorised certification authority: Banque de France IGC, RGS **/*** (recommended), or eIDAS-qualified. If using a software-based certificate, ensure the private key is appropriately secured.
- [ ] If using MISP: install the current Banque de France–specified MISP version. As of the May 2026 Production Note this was version 2.5.16; a further upgrade to 2.5.36 (patching known vulnerabilities and adding a "first publication" field) was scheduled for homologation on 18 June and production around 16 July 2026. Confirm the current requirement with the Banque de France before installing rather than relying on a fixed version number.
- [ ] Complete the connection form (formulaire de raccordement) and, for account-holder PSPs, the BIC register form (référentiel des BIC).
- [ ] Submit both forms and your test certificate (.cer file) to the BdF secure sharebox at least 15 days before the desired test start date.
- [ ] Obtain or confirm the institution's API key from the Banque de France.

3 Step 3 — Homologation (mandatory before production access)

- [ ] Run the unit test plan independently: connection, authentication, positive and negative test cases, using the client test plan provided by the Banque de France.

- [ ] Execute end-to-end business tests in bilateral pairs with another PSP (binôme) across all four test sheets:
  - Fiche 01: Declaration
  - Fiche 02: Account-Holder PSP Qualification
  - Fiche 03: Participant PSP Qualification
  - Fiche 04: Modification

- [ ] Complete the technical connection sequence (see Step 2 - C for full actor/action table).

- [ ] Submit the self-certification Procès-Verbal (PV) de recette to the BdF sharebox, accompanied by screenshots confirming successful completion of all test cases.

- [ ] Await BdF validation of the PV — this is the mandatory gateway to production connection.

- [ ] Go live in production (available from 7 May 2026); observe the recommended 1–3 month run-in period before full operational exploitation.

4 Step 4 — Ongoing Operations

Reporting workflows

- [ ] Build or configure internal tooling to generate compliant FNC-RF fraud event declarations, with all mandatory fields correctly mapped to the BdF specification. Target: declaration within 24–48 hours of internal fraud detection.

- [ ] Establish the internal process for submitting corrective declarations without delay when new or contradictory information emerges.

- [ ] Implement local deduplication of MISP objects and purge local instances after 13 months calculated from the declaration, and if applicable, from the last corrective declaration, (as per article 6 of the arrêté)

Account-holder qualification workflow

- [ ] Build an inbound alert management process: detection of alerts where flagged IBANs belong to the institution's own customers.

- [ ] Apply the “EN COURS” qualification value immediately on becoming aware of a declaration via local sync, ahead of the definitive qualification.

- [ ] Define SLAs for acknowledging receipt of inbound alerts and completing due-diligence investigations. Implement the qualification submission process back to the register, including false-positive notifications where warranted.

- [ ] Build a decision path for manipulated/mule accounts using the “compte régularisé” (REGUL) qualification, with a rule to escalate risk scoring if a REGUL-tagged account reappears in a later fraud event.

- [ ] Establish notification triggers (email and/or webhook) for inbound alerts requiring action.

4 Step 4 — Ongoing Operations

Customer-facing integration

- [ ] Integrate FNC-RF IBAN lookup into the wire transfer initiation flow to enable suspicious IBAN alerts at the point of payment.
- [ ] Define customer alert wording in line with the VOP alert framework already in operation.
- [ ] Ensure the alert and the customer's decision are logged to create an audit trail.

GDPR and legal

- [ ] Handle customer data rights requests within the GDPR one-month deadline.

Governance and monitoring

- [ ] Establish internal reporting on FNC-RF KPIs (reporting frequency, qualification timeliness, false-positive rate) aligned with Banque de France monitoring.
- [ ] Schedule periodic review of FNC-RF legislative developments, including the forthcoming European passport decree, PSD3/PSR implementation, and FRIDA.

Conclusion

The FNC-RF is a structural shift in how France addresses payment fraud. For the first time, a fraudulent account flagged by one bank becomes a shared intelligence signal that every in-scope institution can act on — within hours, not days. For PSPs, this creates both opportunity and obligation.

The opportunity is significant: institutions that integrate the FNC-RF effectively will protect their customers, reduce fraud losses, and build a defensible audit trail that will matter increasingly as PSD3 shifts liability expectations. Those that treat compliance as a minimum connectivity exercise (connected but not operationally engaged) will neither benefit from the intelligence nor have the documentation to support their position in fraud disputes.

The obligation is clear and enforced: the ACPR monitors compliance; the Banque de France tracks reporting quality; and the law itself imposes correction obligations that are legally distinct from the initial reporting duty. This is not optional participation in a voluntary scheme. It is a statutory regime with supervisory oversight.

France has positioned the FNC-RF explicitly as the national precursor to the SEPA-wide fraud intelligence sharing that PSD3 and FRIDA will make mandatory. Institutions that build robust participation now will be ahead of the curve when the European framework arrives, rather than facing it as a second implementation cycle.

The window for preparation is open. The time to act is now.

How Banfico Can Help

Banfico is the trusted technical partner for payment service providers connecting to the FNC-RF. With global presence, Banfico builds regulatory compliance infrastructure for the European payments ecosystem, specialising in Verification Of Payee and fraud intelligence solutions. Banfico holds ISO 27001 certification and provides 24/7 operational support.

Running MISP directly has real advantages worth acknowledging: no licensing cost, full control over where data sits, native correlation across events, and genuine synergy for institutions already using MISP for other threat-intelligence sharing. The trade-off is the operational burden below: the FNC-RF-specific workflow, ongoing platform maintenance, and administrative overhead that a self-hosted or API-only setup leaves entirely to the institution. Banfico exists to absorb that burden while your team keeps full visibility and control.

What's needed	Own MISP	Direct API	With Banfico
Alert interface tailored to FNC-RF qualification (EN COURS, REGUL, etc.)	Generic MISP UI only — built for threat-intel analysts, not fraud caseworkers	None — a raw API response, with no UI at all unless you build one	Purpose-built dashboard for the FNC-RF qualification workflow
Own-account/IBAN matching against your customer book	Requires custom development — MISP has no knowledge of which BICs/IBANs are yours	Requires custom development — same gap	Automatic detection on ingestion
FNC-RF field validation & one-event-per-account dedup rule	Not enforced by MISP itself; easy to submit malformed or duplicate declarations	Not enforced by the API itself; same risk	Built in, including group-entity edge cases
Bulk handling of qualifications	Manual, one event at a time unless custom-scripted	Manual, one call at a time unless custom-scripted	Bulk qualification supported natively
Notifications on inbound alerts	Native MISP email notifications only; no webhook triggers without custom development	None — you must poll for new events yourself	Email and webhook notifications, configurable per user
User access control	Single shared instance login model; granular per-user permissions require custom configuration	No native user layer at all — access control is whatever you build around the API key	Granular team management, with view-only and edit permission levels per user
Your own systems' access to the data	N/A — MISP is the system	Native, since this is the API itself	API integration available to the bank, alongside the portal
Certificate procurement & lifecycle (QWAC and others)	Manual acquisition and tracking; external CA lead times can run to several months	Same requirement and lead times — connectivity mode doesn't change this	Banfico can procure a dedicated QWAC certificate on your behalf, and tracks renewal dates ahead of expiry

What's needed	Own MISP	Direct API	With Banfico
Tracking and applying the Banque de France's mandatory MISP version upgrades	Your team's ongoing responsibility, on BdF's schedule (e.g. 2.5.16 → 2.5.36, homologation 18 June / production 16 July 2026 — and every future one)	Not applicable — no local MISP instance to maintain	Tracked and applied on your behalf
Consolidated view for banking groups with multiple declaring entities*	Manual reconciliation across entities; risk of the same account being double-counted as "reused"	Same manual reconciliation risk	Single consolidated view across group entities
Monitoring changes to the Règles d'usage and COPIL decisions	Your team's responsibility to watch BdF communications for rule changes	Same monitoring burden	Monitored and flagged as they're published
BdF-mandated reporting (KPIs, fraud/qualification statistics)	Your team builds and formats these internally against the BdF spec	Same requirement	Generated automatically in the format the Banque de France requires

**Group-consolidation and dedup benefits scale with the number of legal entities and declaring organisations involved — most relevant for banking groups; a single-entity PSP will see less benefit from this row specifically.*

Two further scheduling considerations, handled by Banfico as part of ongoing account management: institutions connecting from June 2026 onward only receive a four-week historical backfill on first connection, and once IP allow-listing is live for your connection mode, any change to your outbound server infrastructure requires updating your registered IPs with the Banque de France or risking silent connectivity loss.

Outbound reporting

Banfico's guided submission form maps every required field to the Banque de France specification, eliminating manual formatting errors and rejected submissions. Every submission is timestamped and captured in a full audit trail from day one.

Inbound feed and IBAN lookup

The feed synchronises automatically approximately four times a day, with manual refresh available at any time. IBAN lookup returns results in under 100ms. Banfico's own-account detection layer automatically flags alerts where the reported IBAN belongs to your institution's own customer base — the alerts requiring your legal qualification obligation.

Investigation workflow

When an inbound alert matches your IBAN universe, it is immediately highlighted and prioritised. Banfico provides a structured investigation workflow: threaded notes with author and timestamp, mandatory qualification codes, resolution descriptions, and optional false-positive notifications back to the Banque de France. Every step is recorded.

Team access and notifications

Institutions manage their own team structure within Banfico's dedicated portal: granular, per-user permissions distinguish view-only access from edit/qualification rights, so front-line staff and supervisors can be scoped appropriately. Email and webhook notifications are configurable per user, ensuring the right person is alerted without noise for the rest of the team.

Reporting and audit

The full audit trail including every action, every actor, every timestamp, before/after field values, is exportable as CSV or formatted Excel report, with a minimum five-year retention period configurable per institution. Banfico also generates the periodic reports the Banque de France requires from participants (KPIs and fraud/qualification statistics), in the correct format, ready for submission.

Going live

Banfico handles the full connectivity to the Banque de France FNC-RF network. You provide your API key (issued by the Banque de France for your institution) and your QWAC certificate for mTLS authentication. Banfico handles the MISP integration and protocol layer, feed synchronisation and ingestion, field mapping to the FNC-RF spec, error handling and retry logic, and ongoing connectivity.

Contact Banfico

Banfico Europe GmbH
Platz d. Einheit 2, TechQuartier, 60327
Frankfurt am Main, Germany

+44 207 993 4810

paulo.barbosa@banfico.com

www.banfico.com

How Herald Avocats Can Help

Herald Avocats is a French multidisciplinary law firm founded in 1957, possessing deep expertise in banking and financial law, regulatory compliance, and commercial litigation.

Comprehensive expertise in banking and financial law

Banking and financial regulation

Herald assists credit institutions, payment institutions, electronic money institutions, finance companies, foreign branches, and fintechs with all their regulatory matters. The firm advises on licensing and European passporting, governance, internal control, payment services, AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism), outsourcing, and operational resilience, as well as on anticipating European regulatory developments.

Financing and credit transactions

Herald advises lenders, borrowers, sponsors, and investors on the structuring, negotiation, and implementation of domestic and international financing: corporate, real estate, acquisition, project, and asset financing, as well as syndicated loans, refinancings, and debt restructurings. The firm drafts and negotiates financing documentation, intercreditor agreements, guarantees and security interests, conditions precedent, and legal opinions. It also acts in debt rescheduling, default situations, and the enforcement of security interests.

Structuring of activities, products, and partnerships

Herald assists clients in creating and evolving their banking and payment offerings, as well as in securing their contractual relationships. The firm drafts and negotiates general terms and conditions, service agreements, outsourcing contracts, and agreements with technology providers. It also supports transformation projects involving the adaptation of internal processes, governance, and regulatory documentation.

Audits, regulatory proceedings, and banking litigation

Herald handles ACPR (French Prudential Supervision and Resolution Authority) audits—whether conducted off-site or on-site—from the preparation stage through to the follow-up on remediation measures. The firm also defends institutions before the ACPR's Sanctions Committee and, where applicable, before the Council of State. Its litigation team further represents banking and financial entities in disputes with clients, partners, or service providers, particularly regarding banking liability, payment services, and the performance of financing contracts.

Specialised support regarding FNC-RF and payment fraud

GDPR and data governance

Herald assists Payment Service Providers (PSPs) with informing data subjects, documenting processing activities, determining data retention periods, and managing requests for access, rectification, restriction, or erasure. The firm also analyses the allocation of responsibilities between PSPs and the Banque de France, prepares data protection impact assessments, and handles data breach management as well as interactions or proceedings involving the CNIL.

Liability analysis and dispute management

Herald advises Payment Service Providers (PSPs) on handling claims regarding authorized or unauthorized payments and on compiling comprehensive evidentiary files—including authentication logs, transaction monitoring records, customer alerts, VoP and FNC-RF data, customer correspondence, and the rationale behind decisions made.

The firm primarily represents PSPs in the defense of litigation related to payment fraud, particularly cases involving fraud through manipulation, identity theft, transaction disputes, or alleged breaches of the duty of vigilance.

Herald acts from the pre-litigation stage—handling mediations and amicable negotiations—through to proceedings before courts of first instance and appellate courts. The firm also assists PSPs in pursuing claims against other parties in the payment chain.

Regulatory advice and compliance

Herald assists Payment Service Providers (PSPs) in analysing the scope of the FNC-RF (Fichier National des Comptes signalés pour Risque de Fraude), defining reporting and qualification workflows, and drafting and updating internal policies and procedures. The firm focuses on distinguishing between obligations subject to statutory deadlines and operational objectives set by the institution, while also establishing guidelines for the use of registry data in decisions regarding the suspension or refusal of services or the management of customer relationships.

Herald also supports institutions during ACPR off-site and on-site inspections, covering inspection preparation, document review, responses to the Authority's requests, interview support, and the definition of remediation measures. In the event of disciplinary proceedings, the firm represents the institution before the ACPR's Sanctions Committee and, where applicable, the Council of State.

Training and operational procedures

Herald trains fraud, compliance, legal, and operations teams on the FNC-RF framework, alert and complaint handling, and case law related to payment fraud. The firm drafts and updates escalation matrices, decision trees, reporting and qualification procedures, correction and deletion procedures, customer communication models and audit trail protocols.

These procedures can also be tested through file reviews or mock control exercises, and subsequently updated to reflect regulatory changes, case law developments, and the expectations of the authorities.

Contact Herald Avocats

Herald Avocats
Avocats depuis 1957

Christophe Jacomin
Avocat associé

+33(0)153431515