Banfico | HERALD AVOCATS DEPUIS 1957

FNC-RF : Un nouveau rempart contre la fraude aux paiements en France

Sommaire

Introduction

Le 7 mai 2026, la France a officiellement lancé le Fichier National des Comptes signalés pour Risque de Fraude (FNC-RF), un registre centralisé des comptes bancaires signalés comme potentiellement liés à des activités frauduleuses. Géré par la Banque de France et créé par la loi n° 2025-1058 du 6 novembre 2025 (dite loi Labaronne), le FNC-RF représente une évolution majeure dans les pratiques de sécurité des paiements en France.

La loi impose à chaque Prestataire de Services de Paiement (PSP) concerné de signaler sans délai les IBAN bénéficiaires suspects. Lorsqu'un PSP détient le compte signalé, il doit prendre immédiatement en charge l'alerte et communiquer les résultats de son enquête dans les meilleurs délais. Tous les participants sont tenus de garantir l'exactitude et la mise à jour des informations qu'ils fournissent.

Pour la première fois, les informations sur les comptes potentiellement frauduleux circulent en temps quasi réel entre tous les établissements participants en France, ce qui complique considérablement la tâche des fraudeurs qui souhaitent passer d'une banque à l'autre une fois identifiés.

Ce livre blanc offre un guide complet et pratique du FNC-RF : le contexte de fraude qui l'a engendré, l'évolution réglementaire qui l'a façonné, les exigences légales spécifiques, le fonctionnement concret du système et les responsabilités et risques juridiques qui incombent désormais à chaque établissement concerné.

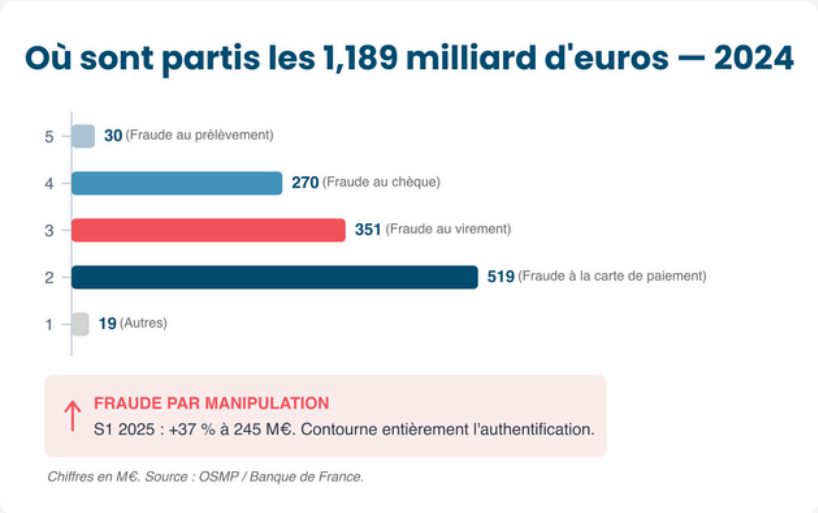
Il s'appuie sur les textes législatifs publiés par la Banque de France, les arrêtés d'exécution, les CGU et les règles d'usage, ainsi que sur les comptes rendus du comité de pilotage (COPIL), et sur la jurisprudence relative à la responsabilité des PSP et au contexte, présentée lors de l'événement sectoriel que nous avons organisé et auquel M. Labaronne a participé. Il a été entièrement mis à jour afin de refléter les orientations opérationnelles publiées par la Banque de France depuis son entrée en vigueur.

1. Contexte

1.1 L'ampleur de la fraude aux paiements en France

La France est l'un des principaux marchés de paiement d'Europe, avec plus de 18 000 milliards d'euros de paiements scripturaux traités au seul premier semestre 2025. Le volume ainsi que les pertes liées à la fraude ont augmenté chaque année depuis 2023, sous l'effet de trois schémas récurrents : les virements bancaires frauduleux, la fraude par détournement de virement et d'autres méthodes de manipulation.

La tendance au cours de ces trois périodes n'est pas simplement une croissance : c'est un changement de nature. Les fraudes par carte et par chèque, les deux catégories les plus exposées aux défenses basées sur l'authentification, sont en baisse. Tout ce qui dépend de la manipulation d'une personne augmente fortement, et ce plus rapidement chaque année.



Cette accélération coïncide avec un second changement structurel : les virements instantanés, autrefois minoritaires, sont devenus la norme, avec une augmentation de 46 % de leur volume rien qu'en 2024. La combinaison de ces deux tendances – la hausse des fraudes par manipulation et le règlement instantané des virements – rend cette fraude bien plus difficile à endiguer que les précédentes

Un virement classique n'ouvre pas, en droit, un droit général à l'annulation après réception de l'ordre par le PSP ; une intervention opérationnelle peut néanmoins rester possible tant que l'ordre n'a pas été exécuté. Le virement instantané, exécuté en quelques secondes, réduit considérablement cette fenêtre. Cette compression du temps, plus encore que le montant brut des pertes, explique pourquoi les seules mesures techniques de protection ne suffisent plus (article 1.3) et pourquoi un registre partagé et mis à jour en temps réel, tel que le FNC-RF, est devenu indispensable.

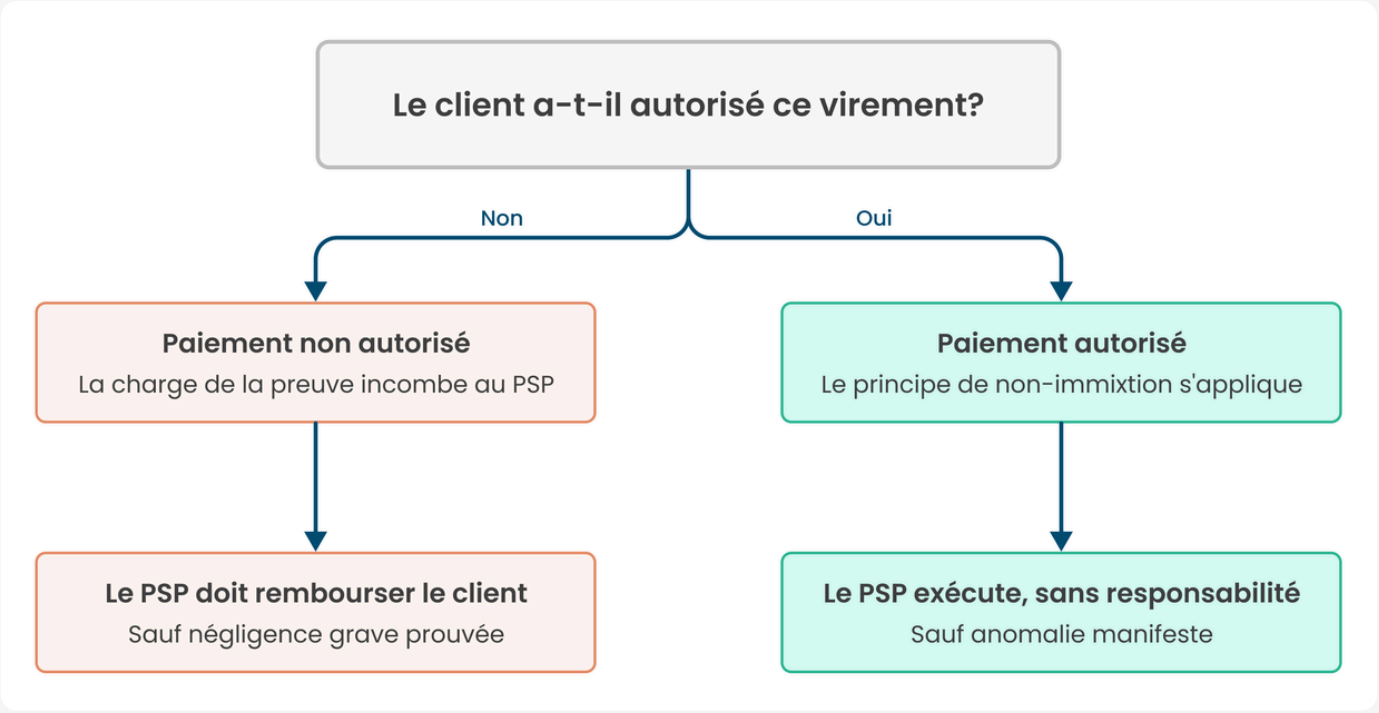
1.2 Le problème structurel : fraude autorisée versus fraude non autorisée

Pour comprendre pourquoi le FNC-RF était nécessaire, il est essentiel de saisir une distinction juridique qui se trouve au cœur du problème de la fraude et qui structure désormais l'ensemble du paysage contentieux pour les PSP : la différence entre paiements non autorisés et paiements autorisés.

Un paiement non autorisé est un paiement auquel le titulaire du compte n'a pas consenti. Cela peut se produire lorsqu'un criminel accède aux identifiants bancaires et exécute un virement à l'insu du client, mais également dans des scénarios de fraude plus complexes où le client nie avoir autorisé l'opération de paiement spécifique. En vertu de la DSP2 (deuxième directive sur les services de paiement), telle que transposée en droit français, une opération de paiement est autorisée lorsque le payeur a consenti à son exécution (article L. 133-6 CMF). Lorsque l'utilisateur nie avoir autorisé l'opération, les articles L. 133-18 à L. 133-24 CMF prévoient le régime spécifique de remboursement et de responsabilité applicable aux opérations de paiement non autorisées. La charge de la preuve pèse sur la banque : celle-ci doit d'abord démontrer que l'opération a été correctement authentifiée, enregistrée et exécutée sans défaillance technique avant de pouvoir invoquer la négligence grave du client, et doit caractériser cette négligence avec précision et dans son contexte factuel complet (Cass. com., 30 avril 2025, n° 24-10.149 ; 12 juin 2025, n° 24-13.777).

Un paiement autorisé est différent. Ici, la victime est manipulée pour ordonner elle-même le virement — par l'usurpation de l'identité d'un agent bancaire, une fausse facture substituée dans un échange de courriels légitime (fraude FOVI), un appel frauduleux convaincant, ou une autre technique d'ingénierie sociale. En principe, la banque doit exécuter un ordre régulier et ne pas s'immiscer dans les affaires de son client. Sa responsabilité n'est cependant pas exclue de manière générale : elle peut être engagée lorsque des anomalies apparentes, aisément décelables par un professionnel normalement diligent, auraient dû conduire à vérifier la validité de l'ordre (voir notamment Cass. com., 25 mars 2026, n° 24-18.093).

Des virements élevés, nombreux, internationaux ou rapprochés ne suffisent pas nécessairement, pris isolément, à caractériser une anomalie apparente. L'analyse demeure contextuelle. Ainsi, un faisceau d'indices tenant notamment au caractère inhabituel des montants, à la répétition des ordres, à leur période, aux bénéficiaires et à la zone géographique peut imposer une vérification (Cass. com., 2 octobre 2024, n° 23-13.282), tandis que d'autres configurations n'engagent pas la responsabilité de la banque (Cass. com., 12 juin 2025 ; 14 janvier 2026). Par ailleurs, le PSP n'est pas, du seul fait de l'exécution de virements destinés à un investissement en crypto-actifs, tenu d'un devoir de conseil sur l'investissement (Cass. com., 25 mars 2026, n° 25-10.353).



De manière déterminante, les tribunaux ont également confirmé que les obligations de vigilance en matière de lutte contre le blanchiment — au titre des articles L. 561-4-1 à L. 561-14-2 CMF — existent uniquement aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Une victime de fraude ne peut donc pas invoquer le manquement d'une banque à ses obligations LCB-FT comme fondement d'une action civile en dommages-intérêts (Com., 4 mars 2026, nº 24-19.588).

> L'ensemble de ces difficultés révèle une vulnérabilité structurelle que les fraudeurs exploitent. Le FNC-RF ne la comble pas (Le futur règlement européen sur les services de paiement (PSR), s'il est adopté dans la version de compromis disponible, modifiera plus directement les règles de surveillance et de responsabilité). Ce que fait le FNC-RF, en revanche, c'est donner aux PSP le renseignement nécessaire pour intervenir avant qu'un paiement obtenu par manipulation n'atteigne un compte frauduleux connu, et pour constituer un dossier documenté démontrant qu'ils ont agi sur la base de ce renseignement.

1.3 Pourquoi les défenses techniques seules ne suffisent plus

Les statistiques de l'OSMP pour le S1 2025 racontent une histoire précise sur les limites des défenses fondées uniquement sur l'authentification. La fraude à la carte (là où 3-D Secure et l'authentification forte ont été déployés le plus efficacement) a chuté de 9,8 % pour atteindre un taux de fraude historiquement bas de 0,048 %. La fraude au chèque a reculé de 16 %. Ce sont de véritables succès.

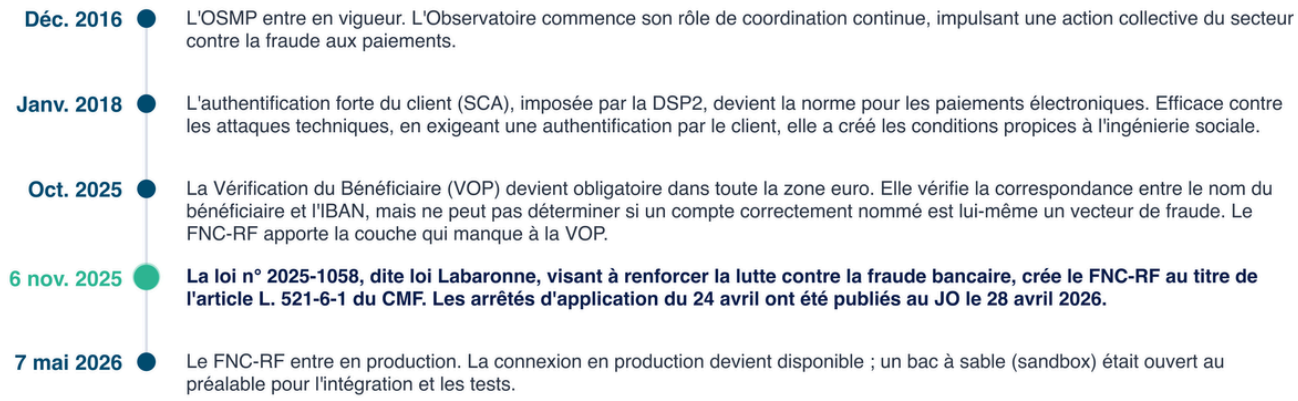
Pourtant, la fraude par manipulation, qui peut contourner l'authentification en exploitant la psychologie humaine, a augmenté de 37 %. Les fraudeurs ont adapté leur arsenal en conséquence : ayant perdu la capacité d'usurper les numéros de téléphone des banques (le mécanisme MAN, un système d'authentification empêchant les fraudeurs d'afficher le véritable numéro de téléphone d'une banque, y a mis un frein), ils utilisent désormais des numéros de mobile ordinaires (préfixes « 06 » et « 07 ») ou des appels via des applications de messagerie instantanée pour approcher les victimes, en se faisant passer pour des employés de banque et en demandant aux clients de « sécuriser » leurs fonds en les transférant.

L'incitation économique a également changé. Les virements instantanés ont progressé de 46 % en volume en 2024 et de 70 % au S1 2025 (à la suite de l'alignement tarifaire de janvier 2025 sur les virements standards). Cela signifie que lorsque la fraude survient, elle se produit en quelques secondes. La fenêtre de détection et d'intervention se réduit.

Dans ce contexte, toute solution purement technique, aussi bien conçue soit-elle, se heurtait à un plafond structurel. Ce qui manquait, c'était l'intelligence collective : la capacité pour la découverte d'un compte frauduleux par une banque de bénéficier immédiatement à toutes les autres. Le FNC-RF comble cette lacune en permettant la mutualisation des informations.

2. Le contexte réglementaire

2.1 Le parcours réglementaire : de la DSP2 à la loi Labaronne



La DSP2 a fait de l'authentification forte un élément central de la sécurité des paiements électroniques, en introduisant des cadres d'authentification renforcée, d'analyse des risques de transaction et de responsabilité toujours en vigueur aujourd'hui. Elle s'est avérée efficace contre les attaques techniques, mais en exigeant que le client authentifie le transfert plutôt que la banque, il a créé par inadvertance la condition exacte exploitée par l'ingénierie sociale : une fois qu'un fraudeur a convaincu un client de s'authentifier, cet enregistrement d'authentification joue alors contre la victime, et non pour elle, dans tout litige ultérieur.

Le rôle de coordination de l'OSMP, en cours depuis 2016, s'inscrit dans la même logique de rapprochement : son plan d'action de juin 2024 sur les paiements par carte à distance sans 3-D Secure a permis une forte baisse de la fraude à la carte, et le déploiement du mécanisme MAN a fermé la voie de l'usurpation de numéro de téléphone bancaire utilisée par les fraudeurs. Ce rôle s'étend désormais également au FNC-RF : à l'avenir, les propres indicateurs de performance de l'OSMP intégreront les données du FNC-RF.

La vérification du bénéficiaire (Verification of Payee – VOP) est une solution plus étroite qu'il n'y paraît, et son déploiement lui-même est échelonné : obligatoire dans toute la zone euro à partir d'octobre 2025, mais pas avant juillet 2027 pour les pays SEPA hors zone euro.

Mécaniquement, il vérifie si le nom du bénéficiaire correspond à l'IBAN saisi lors de l'initiation du paiement, générant un avertissement (et non un blocage) en cas de non-concordance. Cela arrête une manipulation spécifique, un IBAN substitué dans la correspondance, mais vérifie l'identité, pas l'intention : un compte correctement nommé peut toujours être le compte d'une mule bancaire, et la VOP ne permet pas de le savoir. C'est précisément l'écart que le FNC-RF est censé combler, et pourquoi les deux sont conçus pour fonctionner ensemble plutôt que comme des alternatives.

2.2 La loi Labaronne et son contexte législatif

Proposée par Daniel Labaronne, député d'Indre-et-Loire, la loi n° 2025-1058 du 6 novembre 2025 visant à renforcer la lutte contre la fraude bancaire crée le FNC-RF en tant que nouvel instrument prévu à l'article L. 521-6-1 du Code monétaire et financier. La loi a été affinée au cours de son parcours législatif, avec plus d'un millier d'amendements déposés jusqu'en avril 2026 ; les arrêtés d'application du 24 avril ont été publiés au Journal officiel le 28 avril 2026.

Au-delà du FNC-RF lui-même, la loi Labaronne renforce également le Fichier National des Chèques Irréguliers (FNCI) existant : l'article 3 renforce l'obligation pour la banque tirée de déclarer les chèques falsifiés ou contrefaits, tandis que l'article 4 autorise expressément le banquier à consulter le FNCI lorsqu'un chèque est présenté au paiement afin de vérifier la régularité de son émission. En pratique, les banques pourront interroger le FNCI via un nouvel accès dédié.

Le FNC-RF est délibérément conçu pour faire le pont avec l'architecture réglementaire européenne à venir. Il anticipe les dispositions de partage du renseignement sur la fraude du règlement sur les services de paiement (PSR, article 83a), qui deviendront obligatoires dans toute la zone SEPA une fois la DSP3/le PSR finalisés et appliqués, et il est architecturalement compatible avec le cadre FRIDA (Fraud Information Distribution Arrangement) du Conseil européen des paiements (EPC), qui envisage une structure en « réseau de réseaux » pour le partage du renseignement à l'échelle SEPA.

2.3 Le futur cadre européen : DSP3, PSR et FRIDA

La DSP3 et le règlement sur les services de paiement qui l'accompagne devraient être finalisés en 2026 et entrer en vigueur dans les 18 mois suivant leur publication. Le PSR (article 83a) introduira une obligation contraignante pour les PSP de toute la zone SEPA de partager le renseignement sur la fraude, FRIDA étant le véhicule technique probable. Un accord en trilogue a été trouvé en novembre 2025, avec des discussions techniques en cours.
Le FNC-RF devrait servir de point de connexion (statut « FIP ») à la France au sein de ce système européen, avec un démarrage effectif indicatif du dispositif FRIDA autour de l'été 2028, soit 21 mois après la promulgation du PSR. Cette estimation est plus précise que les précédentes indications publiques, qui mentionnaient seulement « aux alentours de 2028 ».

Le futur cadre européen devrait élargir le périmètre des données partagées au-delà des seuls IBAN, en incluant potentiellement des données comportementales du payeur, des adresses IP et d'autres signaux environnementaux. Il envisage également d'étendre le partage du renseignement aux prélèvements (ICS/prélèvements).

Cette extension n'est pas encore définitive. La Banque de France a toutefois indiqué que la déclaration des IBAN des créanciers liés aux prélèvements automatiques et aux effets de commerce « semble présenter un intérêt limité pour certains prestataires de services de paiement » et a reporté la question à une date ultérieure pour confirmation par les spécialistes du marché. De même, l'idée de déclarer également les IBAN liés aux chèques frauduleux au sein du FNC-RF a été définitivement abandonnée, le FNCI (Fichier national des chèques irréguliers) existant répondant déjà à ce besoin.

Les IBAN étrangers ne peuvent actuellement pas être qualifiés de frauduleux au sein du FNC-RF. La loi française exige bien que la fraude suspectée soit déclarée quelle que soit l'origine de l'IBAN (français, zone euro ou hors zone SEPA), mais la qualification de ces IBAN étrangers comme frauduleux ne sera possible qu'une fois le système étendu au niveau européen, ce qui est attendu vers 2028. Dans l'intervalle, l'architecture MISP (Malware Information Sharing Platform) du FNC-RF est explicitement conçue pour une interopérabilité future avec la plateforme FRIDA de l'EPC.

La DSP3 devrait également aller plus loin que la DSP2 en clarifiant la responsabilité dans les scénarios d'ingénierie sociale, en transférant potentiellement une plus grande part de responsabilité aux PSP. Les établissements doivent anticiper que leur intégration au FNC-RF et leur documentation feront partie des éléments de preuve lorsqu'il s'agira de démontrer qu'ils ont satisfait à leur devoir de vigilance dans un litige portant sur un paiement autorisé.

3. Ce que la loi exige

→ 3.1 Qui doit participer

Deux clarifications importantes concernant le champ d'application ont été confirmées depuis. Premièrement, l'URSSAF (organisme chargé du recouvrement des cotisations de sécurité sociale) figurait initialement parmi les entités déclarantes au titre de la loi relative à la fraude à la sécurité sociale. Cette loi ayant été adoptée par le Parlement, son article 9 abroge formellement l'accès aux données de l'URSSAF prévu par l'article L. 521-6-1 (III), l'URSSAF n'étant pas soumise au même cadre de surveillance de l'ACPR que les prestataires de services de paiement (PSP). En remplacement, ce même article 9 ajoute un nouvel article VIII à la loi L. 521-6-1, accordant un accès en lecture seule aux sociétés de financement et à certaines administrations, à des fins liées au financement – ce qui concerne environ 151 entités inscrites au registre REGAFI de la Banque de France.

Par ailleurs, l'arrêté technique confirme que les PSP étrangers – c'est-à-dire ceux qui ne disposent pas d'une présence en France ou d'un passeport européen – ne peuvent se connecter au FNC-RF ni obtenir communication de son contenu, et notamment ne peuvent pas « qualifier » les cas de fraude concernant leurs propres clients, la Banque de France n'intégrant pas les codes BIC étrangers à son référentiel central. En pratique, cela engendre de réelles difficultés opérationnelles pour les commerçants et des litiges liés à des faux positifs émanant de prestataires de services de paiement (PSP) étrangers. La Banque de France a annoncé la mise en place d'un point de contact dédié (boîte mail) auprès de chaque PSP français afin de relayer les demandes de clarification et d'accès qu'elle reçoit en leur nom de la part des PSP étrangers.

Deuxièmement, et plus important encore pour le marché : les établissements bénéficiant d'un passeport européen pour opérer en France ne sont plus concernés par l'intégration à la base de données. Le droit français ne peut imposer d'obligations à ces participants sans l'approbation des autorités européennes, laquelle n'a pas encore été accordée. Un décret de confirmation était attendu fin mai 2026. Les établissements titulaires d'un passeport européen doivent suivre de près cette évolution, car leur intégration pourrait intervenir une fois le cadre européen du système de règlement des services de paiement (PSR) mis en place.

→ 3.2 L'obligation de déclaration : « sans délai »

L'obligation de déclarer est impérative et doit être remplie le plus rapidement possible. La formulation « sans délai », a fait l'objet d'un débat législatif approfondi. Elle a finalement été alignée sur le standard déjà utilisé dans la législation antiterroriste française, créant un précédent et clôturant le débat. L'objectif pratique, approuvé par la Banque de France, est qu'un compte frauduleux ne reste pas actif plus de 24 à 48 heures après son identification par l'établissement déclarant.

La Banque de France ne peut imposer d'échéance ferme, car elle n'a pas accès à l'événement déclencheur qui fait naître l'obligation. Elle surveillera en revanche la qualité et la fréquence des déclarations de chaque établissement au moyen d'indicateurs de performance, et l'ACPR pourra sanctionner les établissements qui ne respectent pas l'esprit de l'obligation.

3.3 Les trois rôles : PSP déclarant, PSP teneur de compte, PSP participant

Les obligations au titre du FNC-RF diffèrent sensiblement selon le rôle d'un PSP par rapport à un événement de fraude donné. Il existe trois rôles distincts.

PSP déclarant	L'établissement qui détecte un événement de fraude suspecté et crée la déclaration dans le registre. Il doit soumettre tous les champs de données requis, corriger ou retirer la déclaration si de nouvelles informations modifient la situation, et veiller à ce que chaque événement de fraude génère exactement une déclaration.
PSP teneur de compte	L'établissement qui détient le compte identifié dans une déclaration de fraude. Il supporte l'obligation opérationnelle la plus exigeante : il doit indiquer sans délai qu'il prend en charge l'investigation, mener la vérification du caractère frauduleux du compte et partager le résultat de sa qualification dans le registre. Il doit également déclarer toute usurpation d'identité (au sens de l'article 226-4-1 du Code pénal) qu'il détecte.
PSP participant	Tout autre PSP dans le périmètre qui reçoit le flux de renseignement. Il peut, de manière facultative, consigner sa propre évaluation du caractère frauduleux d'un événement (un « sighting ») ou le signaler comme faux-positif, contribuant ainsi à la qualité collective du registre.

Cette architecture à trois rôles est importante pour la planification de la conformité. La plupart des PSP occuperont simultanément les trois rôles selon l'événement de fraude : ils seront l'établissement déclarant pour les fraudes qu'ils détectent, l'établissement teneur de compte pour les alertes émises par d'autres concernant leurs clients, et participant pour le flux de renseignement plus large qu'ils consomment.

3.4 Quel type de données est partagé

La loi Labaronne lève partiellement le secret bancaire pour permettre le FNC-RF d'opérer, mais le périmètre des données partagées est délibérément restreint. Le registre ne partage pas les identités individuelles. Pour chaque événement de fraude, les champs suivants sont déclarés :

- L'identifiant du compte : IBAN ou BBAN, ainsi que le BIC de l'établissement détenant le compte
- La date de détection et la date de dernière mise à jour
- La catégorie de fraude (le type de fraude parmi les grandes catégories connues)
- La source de la fraude : éléments concernant la méthode utilisée par le fraudeur (champ facultatif)
- Le type de transaction : l'instrument de paiement ou l'action du client ayant fait l'objet de la fraude
- Le canal de la transaction : le canal par lequel la transaction a été initiée (champ facultatif)
- L'existence ou non d'une plainte ou d'une réclamation pour usurpation d'identité déposée par l'utilisateur de services de paiement
- L'établissement déclarant et un UUID unique d'événement
- La qualification par le PSP teneur de compte et la qualification par les PSP participants

Les IBAN étrangers doivent être déclarés en cas de fraude suspectée, quelle que soit leur origine, mais ne peuvent être qualifiés de frauduleux dans le registre avant l'extension européenne du système. Plusieurs événements de fraude peuvent concerner le même compte bénéficiaire, créant plusieurs objets MISP distincts ; la déduplication relève de la responsabilité de chaque PSP au niveau local.

→ 3.5 L'interdiction de la liste noire

L'une des limitations les plus importantes du FNC-RF est aussi l'un de ses traits caractéristiques : le registre n'est explicitement pas une liste noire. La loi interdit le blocage automatique des transactions vers un IBAN au seul motif qu'il figure dans la base de données. Les PSP sont tenus de mener une analyse indépendante avant toute action.

L'inscription au FNC-RF ne constitue pas en soi un motif de rupture d'une relation bancaire, de gel d'un compte client ou de blocage de transactions légitimes. Le registre est structuré comme un instrument de vigilance et de renseignement, non de sanction automatique. Un établissement qui agirait sur la seule base de l'inscription au registre, sans mener sa propre analyse, risque de violer à la fois la loi et les droits de ses clients.

> Le FNC-RF est un outil d'aide à la décision éclairée, non de blocage automatisé. Les établissements doivent construire des processus internes utilisant le renseignement du registre de manière appropriée (en enrichissant les évaluations de risque et en déclenchant des investigations), tout en préservant les droits des titulaires de comptes.

3.5a Comptes manipulés et comptes de mules : la qualification « compte régularisé »

L'interdiction de la mise sur liste noire est renforcée par une qualification spécifique introduite par les Règles d'usage afin de gérer un cas particulier récurrent : les comptes utilisés à l'insu de leur titulaire (prise de contrôle de compte) ou après manipulation de ce dernier (par exemple, escroqueries sentimentales), et – plus marginalement – les comptes utilisés avec le consentement du titulaire mais pour lesquels le prestataire de services de paiement (PSP) du titulaire estime qu'il n'existe aucun risque de récidive.

En l'absence de traitement, ce problème de qualification est insoluble: qualifier un tel compte de « frauduleux » surestime le risque et incite les autres participants à bloquer les virements légitimes vers ce compte, tandis que le qualifier de « légitime » revient à enregistrer à tort une fraude réelle comme un faux-positif. La solution de la Banque de France est une troisième qualification, « compte régularisé » (REGUL), que le PSP du titulaire peut appliquer à sa discrétion pour indiquer que le compte peut à nouveau recevoir des virements malgré un incident de fraude antérieur. Les participants ne doivent pas considérer un compte marqué REGUL comme risqué sur la seule base de sa présence dans la base de données FNC-RF, et la Banque de France exclut les comptes REGUL de ses statistiques de faux positifs. Afin de prévenir tout abus, les participants sont tenus de revoir à la hausse leur évaluation interne du risque associé à un compte REGUL s'il réapparaît dans une nouvelle affaire de fraude. La Banque de France suit l'utilisation de cette valeur via son programme d'indicateurs clés de performance (KPI).

3.5b Vigilance sur les IBAN virtuels

Les règles d'usage signalent également une technique d'évasion connexe : plutôt que de réutiliser le même IBAN, un fraudeur peut générer un nouvel IBAN virtuel pour chaque fraude, afin d'échapper au partage des données FNC-RF. Il est recommandé (sans obligation) que, lorsqu'un IBAN déclaré s'avère être un IBAN virtuel, le prestataire de services de paiement (PSP) détenant le compte principal sous-jacent applique une vigilance accrue à l'égard de tout autre IBAN virtuel créé par le même client. Cette pratique s'ajoute aux obligations de qualification habituelles du PSP titulaire du compte et ne les remplace pas.

3.6 Obligations de conservation et de correction

Les données inscrites au registre sont soumises à une durée de conservation de 13 mois à compter de la date de déclaration, en l'absence de suppression anticipée. Les établissements ont l'obligation stricte de soumettre des déclarations rectificatives « sans délai » dès lors qu'ils détiennent des informations nouvelles ou contradictoires par rapport à ce qui a été initialement déclaré. Cela inclut le retrait d'une déclaration si le fondement du soupçon n'est plus établi.

Sur le plan opérationnel, cette obligation de correction se traduit par un tag « événement à supprimer », que les Règles d'usage distinguent en deux catégories : (1) faux positif, lorsque la fraude présumée n'est pas avérée, et (2) tout autre motif de suppression, notamment les doublons techniques. Les participants doivent apposer ce tag dès qu'ils identifient un motif de suppression et supprimer l'événement de leur système local dans les meilleurs délais après son apposition.

La Banque de France maintient la plateforme centrale mais n'est pas responsable de l'exactitude des inscriptions individuelles. Chaque PSP déclarant est responsable de la qualité, de la ponctualité et de l'exactitude de ses contributions.

4. Le fonctionnement du FNC-RF en pratique

4.1 L'architecture technique

Le FNC-RF repose sur MISP, une plateforme open source de renseignement sur les menaces initialement développée pour la cybersécurité, mais adaptée ici à la fraude aux paiements. La Banque de France opère le hub MISP central, qui sert de tiers de confiance et de source unique de vérité pour le registre national.

Chaque événement de fraude est représenté sous la forme d'un objet MISP (« Compte douteux ») avec les champs de données décrits ci-dessus. Lorsque plusieurs événements de fraude sont créés pour le même compte bénéficiaire, il y aura autant d'objets MISP que d'événements — la plateforme centrale ne consolide pas et ne déduplique pas les objets entre eux. La déduplication et la consolidation locales relèvent de la responsabilité de chaque PSP.

Le système renvoie une réponse binaire aux requêtes : oui ou non — cet IBAN a-t-il été signalé comme suspect ? L'architecture est conçue pour une diffusion en quasi temps réel, avec pour objectif affiché qu'un compte frauduleux ne puisse rester actif dans plusieurs établissements plus de 24 à 48 heures après son signalement. Des tests pilotes menés avec des groupes bancaires l'ont déjà validé : les réductions de l'activité frauduleuse après le signalement d'un compte se sont mesurées en jours.

4.2 Options de connectivité

Le FNC-RF s'adapte aux capacités techniques variées des PSP grâce à trois modes de connexion :

Synchronisation avec le hub MISP	Les PSP qui exploitent leur propre instance MISP synchronisent leur base de données locale avec le hub central de la Banque de France (BdF). Cela impose de maintenir une installation MISP locale et de gérer les calendriers de synchronisation, mais offre un contrôle maximal sur le traitement local des données.
API directe	Les PSP interagissent avec le hub de données central via des appels API. C'est techniquement plus simple que d'exploiter une instance MISP complète, mais cela offre moins de flexibilité de traitement local.
Intégration via Prestataire Technique	Les PSP peuvent recourir à un prestataire de services techniques lui-même directement connecté à la plateforme de la Banque de France, et interagir avec le FNC-RF par l'intermédiaire de celui-ci. C'est l'option la moins complexe pour les établissements dépourvus d'infrastructure technique dédiée.

Quel que soit le mode de connectivité, l'accès à la plateforme requiert un certificat d'authentification accepté: soit un certificat délivré par l'autorité de certification propre de la Banque de France (IGC Banque de France), soit un certificat qualifié RGS **/***, soit un certificat d'une autorité de certification qualifiée au sens du règlement eIDAS. L'approche recommandée est un certificat d'authentification RGS **/*** , bien que les certificats d'authentification logiciels soient également admis à condition que la clé privée soit sécurisée de manière appropriée. La liste des autorités de certification acceptées par la Banque de France pour le FNC-RF est disponible dans la FAQ dédiée sur le site de la Banque de France.

Les PSP doivent soumettre une demande formelle de raccordement avant d'obtenir l'accès. Pour la phase d'homologation (tests), les contacts à la Banque de France sont : FNC-RF@banque-france.fr pour la demande de raccordement métier, et Mohamed.BOULOUZ@banque-france.fr pour la connectivité technique et le suivi des tests.

4.3 Calendrier de mise en production et période de rodage

La connexion en production est disponible depuis le 7 mai 2026. Un environnement d'homologation (sandbox) et de test était disponible avant cette date et l'est toujours. La Banque de France recommande une période de rodage d'un à trois mois avant l'exploitation opérationnelle complète, durant laquelle les établissements peuvent valider leurs flux de déclaration en conditions de production. Les PSP doivent maintenir une copie locale synchronisée du jeu de données central du FNC-RF pour satisfaire à leurs exigences opérationnelles et de conformité.

4.4 Le cycle de vie opérationnel d'un événement de fraude

Comprendre comment un événement de fraude circule dans le système est essentiel pour bâtir des processus internes conformes. Le cycle de vie comporte des phases distinctes selon le rôle de l'établissement.

→ Pour le PSP déclarant (déclaration sortante)

- La détection interne de la fraude identifie un IBAN bénéficiaire suspect sur la base d'analyses internes ou d'une réclamation client.
- Une déclaration d'événement de fraude est soumise au MISP de la Banque de France avec tous les champs requis correctement mappés à la spécification FNC-RF. Chaque événement de fraude identifié génère exactement une déclaration.
- L'alerte est ingérée par la Banque de France et devient active sur le réseau, immédiatement disponible pour tous les participants.
- L'établissement déclarant suit le résultat de qualification ultérieur du PSP teneur de compte.
- Si des informations nouvelles ou contradictoires apparaissent, une déclaration rectificative est soumise sans délai.

→ Pour le PSP teneur de compte (obligation de qualification)

- Une alerte entrante est reçue, correspondant à un IBAN appartenant à la clientèle de l'établissement.
- L'établissement attribue la valeur de qualification « EN COURS » dès qu'il prend connaissance de la déclaration par le biais de la synchronisation locale, à moins qu'une qualification définitive ne soit déjà disponible.
- L'établissement doit indiquer dans le registre « sans délai » qu'il prend en charge l'investigation (pour permettre au PSP déclarant de suivre la déclaration).
- Une investigation est menée pour évaluer si le compte est réellement frauduleux.
- Le résultat de la qualification (confirmant ou infirmant le caractère frauduleux du compte) est consigné dans le registre.
- De manière facultative, une notification de faux positif peut être soumise à la Banque de France si l'établissement conclut que la déclaration initiale était infondée.

→ Pour tous les PSP participants (consommation du flux)

- Le flux FNC-RF doit être synchronisé régulièrement (la plateforme de la Banque de France permet une synchronisation environ quatre fois par jour, avec une actualisation manuelle possible à tout moment.)
- Avant d'exécuter un virement, les établissements peuvent interroger le registre pour déterminer si l'IBAN de destination a été signalé comme suspect.
- En cas de correspondance, le processus de risque de fraude de l'établissement est déclenché. Cela n'impose pas de blocage automatique mais exige une analyse. En général, cela aboutit à une alerte client (voir section 4.5).
- Les PSP participants peuvent consigner leur propre évaluation d'événements individuels sous forme de « sightings » ou de faux positifs, contribuant à la qualité du renseignement collectif.

4.5 Intégration avec la VOP et le cas d'usage de l'alerte client

Le cas d'usage opérationnel le plus significatif à court terme est l'enrichissement du processus VOP par le renseignement du FNC-RF. Lorsqu'un client initie un virement, le contrôle VOP existant vérifie déjà que le nom du bénéficiaire correspond au compte. Le FNC-RF ajoute une seconde couche : si l'IBAN de destination figure dans le registre, l'établissement peut alerter le client au moment de l'initiation du paiement.

Une alerte type destinée au client pourrait être libellée ainsi : « Attention : cet IBAN a été signalé comme suspect par d'autres établissements financiers. Il pourrait être associé à une activité frauduleuse. Souhaitez-vous poursuivre ? » La décision revient au client (la loi n'autorisant pas le blocage automatique), mais l'établissement a satisfait à son devoir de vigilance et en a conservé la preuve.

Ce mécanisme d'alerte est juridiquement significatif. Dans le cadre d'un litige portant sur un paiement autorisé, un établissement capable de démontrer qu'il a averti le client avant l'exécution du virement (et que le client a choisi de poursuivre) se trouve dans une position sensiblement plus solide qu'un établissement dépourvu d'un tel mécanisme. La clarification attendue de la DSP3 sur la responsabilité dans les scénarios d'ingénierie sociale rendra cette documentation encore plus importante.

Les paramètres opérationnels spécifiques de l'utilisation des données du FNC-RF dans les systèmes internes des établissements (seuils de déclenchement des alertes, processus internes consécutifs à une correspondance) sont laissés à la discrétion de chaque établissement. La loi définit l'obligation de partage du renseignement ; elle ne prescrit pas la manière dont les établissements agissent sur la base de ce renseignement.

5. Jurisprudence : le devoir de vigilance en pratique

Le FNC-RF n'existe pas dans un vide juridique. Les tribunaux développent activement le cadre de responsabilité applicable aux opérations autorisées et non autorisées dans lequel le FNC-RF s'inscrit. La jurisprudence suivante, tirée d'arrêts récents de la Cour de cassation, définit l'état actuel du droit et illustre pourquoi les capacités de documentation et d'alerte du FNC-RF ont une portée opérationnelle.

→ 5.1 Paiements non autorisés : charge de la preuve et négligence grave

Pour les paiements non autorisés, le régime légal des articles L. 133-18 à L. 133-24 CMF fait peser la charge de la preuve directement sur le PSP. La banque doit d'abord prouver que l'opération a été correctement authentifiée, enregistrée et exécutée sans défaillance technique. Ce n'est qu'ensuite qu'elle peut invoquer la négligence grave du client (qu'elle doit caractériser avec précision et à l'appui d'éléments factuels). Deux exigences pèsent également côté client :

- Le client doit signaler l'opération contestée « sans tarder » à compter du moment où il en a connaissance. Un défaut de signalement constitutif d'une négligence grave peut le priver de son droit à remboursement, indépendamment du délai de 13 mois (Cass. com., 14 janvier 2026, n° 22-14.822).
- L'absence de preuve de la date de notification à la banque est fatale à la demande de remboursement — le refus de la cour d'appel a été confirmé sur ce seul fondement (Cass. com., 4 février 2026, n° 22-22.609).

→ 5.2 Paiements autorisés : le principe de non-immixtion et ses limites

Pour les paiements autorisés, la doctrine de la non-immixtion définit les limites de la responsabilité bancaire. Des décisions récentes en illustrent l'application:

Affaire	Type de paiement	Élément clé
Cass. com., 12 juin 2025, n° 24-10.168 ; 14 janv. 2026, n° 24-19.102	Autorisé	Des virements simplement d'un montant élevé, nombreux ou transfrontaliers n'engagent pas à eux seuls la responsabilité de la banque. Une analyse contextuelle par faisceau d'indices est requise.
Cass. com., 14 janv. 2026, n° 24-19.102	Autorisé	La banque réceptrice n'est pas tenue de vérifier l'origine ou le montant des fonds crédités, ni d'interroger son client sur des mouvements importants, en l'absence d'anomalie apparente et aisément décelable.
Cass. com., 25 mars 2026, n° 24-18.093	Autorisé	Le devoir de la banque teneuse de compte se limite à vérifier la régularité de l'ordre de paiement. En l'absence d'anomalies apparentes décelables par un professionnel normalement diligent, elle doit exécuter promptement et ne peut s'immiscer.
Cass. com., 25 mars 2026, n° 25-10.353	Autorisé	Une banque recevant un ordre de virement en vue d'un investissement en crypto-actifs agit strictement en qualité de PSP. Elle n'est tenue d'aucune obligation de conseil ou de mise en garde quant aux risques de l'investissement, même en présence de multiples virements importants vers une banque étrangère. La Cour de cassation a censuré la cour d'appel.
Com., 4 mars 2026, n° 24-19.588	Autorisé	Les obligations de vigilance LCB-FT (art. L. 561-4-1 à L. 561-14-2 CMF) existent uniquement à des fins de lutte contre le blanchiment. Une victime de fraude ne peut invoquer les manquements LCB-FT d'une banque comme fondement d'une action civile en dommages-intérêts.

→ 5.3 Ce que cela signifie pour la conformité FNC-RF

Prise dans son ensemble, cette jurisprudence renforce trois conclusions pour les PSP qui construisent leur dispositif FNC-RF.

Premièrement, dans le cas d'un paiement autorisé, la simple présence de l'IBAN de destination dans le FNC-RF ne constitue pas automatiquement une « anomalie apparente », et ne justifie pas non plus automatiquement le blocage de la transaction. Elle constitue en revanche un indice factuel supplémentaire susceptible de devenir pertinent dans un litige ultérieur. Le PSP doit donc être en mesure de démontrer s'il a interrogé le registre, si l'alerte avait été qualifiée, si le client a été averti, si le paiement a été suspendu ou exécuté, et comment cette décision a été justifiée.

Deuxièmement, la propre réaction du PSP teneur de compte peut également devenir pertinente. Lorsqu'il reçoit un signalement concernant l'un de ses clients, le calendrier et la qualité de son investigation, sa qualification du compte et toute déclaration rectificative feront partie du dossier opérationnel. La conformité FNC-RF doit donc être conçue non pas simplement comme une obligation de déclaration, mais comme un processus dans lequel chaque établissement doit être capable de démontrer comment il a réagi aux informations dont il disposait.

Troisièmement, les procédures FNC-RF et LCB-FT doivent rester juridiquement distinctes. Une alerte FNC-RF peut également justifier une escalade LCB-FT, notamment lorsqu'un compte semble utilisé pour recevoir ou transférer des produits d'origine criminelle. Toutefois, les deux régimes poursuivent des finalités différentes, imposent des obligations différentes et emportent des conséquences différentes en matière de responsabilité civile. Les procédures internes et les réponses aux réclamations des clients doivent donc identifier clairement quel régime est appliqué.

5.4 Le cadre proposé du PSR

Le projet de règlement sur les services de paiement (PSR) s'inscrit dans la ligne des dispositions actuelles du droit français. Il préserve la distinction entre opérations autorisées et non autorisées et étend l'obligation de surveillance des transactions au PSP récepteur. Il comporte également des dispositions relatives à la fraude par manipulation, à la surveillance des transactions et à la suspension des ordres de paiement. Le changement le plus important résiderait dans la mise en œuvre d'accords de partage d'informations sur la fraude, qui pourrait imposer une révision du cadre français en ce qui concerne les catégories d'informations échangées, les mesures de sécurité et de confidentialité, les dispositifs de gouvernance, l'analyse d'impact relative à la protection des données et l'interopérabilité transfrontalière.

Pour rappel, en vertu des dispositions actuelles du droit français, une opération de paiement est autorisée lorsque le payeur a consenti à son exécution. Les opérations de paiement non autorisées sont soumises au régime de remboursement prévu aux articles L. 133-18 à L. 133-24 CMF. Lorsque l'utilisateur nie avoir autorisé une opération, le PSP doit prouver qu'elle a été authentifiée, dûment enregistrée et comptabilisée, et qu'elle n'a été affectée d'aucune déficience technique ou autre.

La jurisprudence française applique ce régime aux cas de spoofing dans lesquels le client a effectué des étapes d'authentification ou de sécurité sur instruction du fraudeur, mais n'a pas consenti aux paiements spécifiques exécutés. Dans de telles circonstances, les opérations seront généralement traitées comme non autorisées, et le PSP doit les rembourser, sauf s'il établit la fraude ou la négligence grave du client.

Le PSR, une fois approuvé, conservera un régime spécifique pour les opérations de paiement non autorisées, similaire au régime français actuel.

Pour référence, les cinq articles opérationnels du PSR (Payment Services Regulation) sont résumés ci-dessous ; le détail du fonctionnement de chacun est présenté dans les paragraphes qui suivent le tableau.

Article	Qui est concerné?	Obligation principale	Conséquence en cas de non-conformité
Art. 59	PSP du payeur	Rembourser les paiements autorisés frauduleux lorsqu'un tiers a usurpé l'identité du PSP lui-même, en utilisant des canaux de communication attribués à ce PSP	Doit rembourser sous 15 jours ouvrés, sauf s'il prouve une fraude du consommateur ou une négligence grave
Art. 65	PSP du payeur	Suspendre l'exécution en cas de suspicion justifiée ; recontacter le payeur ; décider d'exécuter ou de refuser	Le payeur ne supporte pas la perte si le PSP n'a pas suspendu malgré une suspicion justifiée (sauf fraude du payeur)
Art. 69	PSP du bénéficiaire	Peut retenir les fonds en cas de suspicion ordinaire ; doit les retenir et les restituer lorsque les motifs sont clairs et incontestables	Le payeur ne supporte pas la perte si le PSP du bénéficiaire n'a pas retenu les fonds comme requis (sauf fraude du payeur)
Art. 83	PSP du payeur et du bénéficiaire	Maintenir une surveillance des transactions avant exécution (côté payeur) et avant libération des fonds (côté bénéficiaire)	Le PSP responsable doit rembourser le payeur s'il ne peut prouver que la surveillance a été effectuée (sauf fraude du payeur)
Art. 83a	Tous les PSP participants	Partager les renseignements sur la fraude via un dispositif de partage d'informations (rôle probable du FNC-RF), à l'exclusion des données comportementales/environnementales d'usage normal	Une AIPD conjointe est requise ; conservation maximale de cinq ans ; aucune action sur un compte ne peut être fondée sur les seules données partagées, sans évaluation indépendante du PSP

L'article 59

Le PSR conserverait un régime spécifique pour les opérations de paiement non autorisées, similaire au régime français actuel. L'article 59 établirait un régime de remboursement pour certaines opérations de paiement autorisées frauduleuses. Il s'appliquerait lorsqu'un consommateur a été manipulé par un tiers se faisant passer pour le PSP du consommateur, en utilisant des canaux de communication attribués à ce PSP, et que cette manipulation a abouti à une opération de paiement autorisée frauduleuse.

Le consommateur serait tenu de notifier le PSP sans délai injustifié après avoir eu connaissance de la fraude et l'avoir signalé à la police. Dans les 15 jours ouvrables suivant la réception de la notification et du dépôt de plainte, le PSP serait tenu soit de rembourser l'opération, soit de motiver son refus de remboursement. Le remboursement ne serait pas dû lorsque le consommateur a agi frauduleusement ou avec une négligence grave. Comme en droit français, la charge de la preuve de la fraude ou de la négligence grave incomberait au PSP du consommateur.

L'article 83

Le PSR introduirait également des obligations de surveillance des transactions. En vertu de l'article 83, les PSP seraient tenus de maintenir des mécanismes de surveillance des transactions destinés à appuyer l'authentification forte du client et à prévenir et détecter les opérations de paiement potentiellement frauduleuses. Le PSP du payeur serait tenu d'effectuer la surveillance avant l'exécution de l'opération, tandis que le PSP du bénéficiaire serait tenu de l'effectuer avant de mettre les fonds à la disposition du bénéficiaire.

Lorsqu'un PSP omet d'effectuer la surveillance requise et que le payeur subit un préjudice financier, ce PSP en supporterait la responsabilité. Lorsque le PSP du payeur ne peut apporter la preuve que la surveillance a été effectuée tant par le PSP du payeur que par le PSP du bénéficiaire, il serait tenu de rembourser le payeur. Sauf si le payeur a agi frauduleusement, celui-ci ne supporterait pas les conséquences financières de l'opération.

L'article 65

L'article précité doit être lu en combinaison avec l'article 65, qui fixe le régime de responsabilité applicable aux opérations autorisées. De manière similaire au régime français, lorsqu'il existerait des raisons, découlant soit de la surveillance des transactions, soit d'autres informations pertinentes à la disposition du PSP, de suspecter une fraude, le PSP serait tenu de suspendre l'exécution de l'opération.

À la suite de la suspension, le PSP serait tenu, dans la mesure du possible, de contacter le payeur et d'évaluer si les raisons du soupçon demeurent justifiées. Il déciderait ensuite d'exécuter ou de refuser l'ordre de paiement. Lorsque le PSP disposerait de raisons objectivement justifiées de suspecter une fraude mais a omis de suspendre l'opération, le payeur ne supporterait pas la perte financière en résultant, sauf s'il a agi frauduleusement. La charge de la preuve de la conformité incomberait au PSP.

L'article 69

L'article 69 prévoirait des règles correspondantes pour le PSP du bénéficiaire. Lorsque la surveillance des transactions ou d'autres informations pertinentes donnent au PSP du bénéficiaire des raisons objectivement justifiées de suspecter qu'une opération créditée ou devant être créditée sur le compte du bénéficiaire est frauduleuse, il peut décider de ne pas mettre les fonds à disposition et de les restituer au PSP du payeur. Lorsque les raisons du soupçon sont claires et incontestables, le PSP du bénéficiaire serait tenu de retenir et de restituer les fonds.

Si le PSP du bénéficiaire manquait à cette obligation impérative, le payeur ne supporterait pas la perte financière, sauf s'il a agi frauduleusement. La charge de la preuve de la conformité incomberait au PSP du bénéficiaire.

Article 83a

Enfin, l'article 83a imposerait aux PSP de participer à des dispositifs de partage d'informations avec d'autres PSP et d'échanger des données lorsqu'ils disposent de raisons objectivement justifiées de suspecter un comportement frauduleux de la part d'un utilisateur de services de paiement. Les informations échangées seraient utilisées aux fins des obligations de surveillance des transactions prévues à l'article 83.

Les informations partagées seraient limitées aux catégories identifiées à l'article 83, aux raisons objectivement justifiées à l'origine du soupçon et, le cas échéant, aux notifications adressées aux fournisseurs de services d'hébergement. Les caractéristiques environnementales et comportementales typiques de l'utilisation normale par le payeur de ses données de sécurité personnalisées ne seraient pas partagées au titre de l'article 83a.

Notes additionnelles

Les PSP participants seraient tenus de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité et la confidentialité des informations échangées, y compris des mesures permettant la pseudonymisation. Le dispositif de partage d'informations devrait définir ses conditions de participation et ses modalités opérationnelles, y compris toute plateforme informatique dédiée utilisée pour l'échange.

Avant de conclure le dispositif, les PSP participants réaliseraient conjointement une analyse d'impact relative à la protection des données et, le cas échéant, consulteraient l'autorité de protection des données compétente. Les informations reçues dans le cadre du dispositif ne pourraient être conservées plus longtemps que nécessaire aux fins de la surveillance des transactions et, en tout état de cause, pas plus de cinq ans après l'opération frauduleuse suspectée. Il serait également interdit aux PSP de résilier une relation contractuelle, d'affecter une entrée en relation future ou de prendre toute autre décision affectant la relation client sur la seule base d'informations reçues d'un autre PSP sans avoir procédé au préalable à leur propre évaluation.

Le FNC-RF fonctionne déjà comme un dispositif national français de partage d'informations concernant les comptes suspectés d'être utilisés pour la fraude aux paiements. Il applique également un principe comparable d'évaluation indépendante : l'inscription d'un compte au registre n'interdit pas, en soi, les opérations de paiement et ne justifie pas la résiliation du compte ou de la relation de services de paiement concernée.

L'article 83a n'exige pas la création d'une base de données centrale unique au niveau de l'UE ni le remplacement des dispositifs nationaux existants. Le FNC-RF pourrait donc continuer à fonctionner comme le mécanisme français de partage d'informations, sous réserve que son cadre juridique, technique et opérationnel soit conforme à l'article 83a.

Cela pourrait nécessiter une révision du cadre français en ce qui concerne les catégories d'informations échangées, les mesures de sécurité et de confidentialité, les dispositifs de gouvernance, l'analyse d'impact relative à la protection des données et l'interopérabilité transfrontalière. La période de cinq ans prévue à l'article 83a est une durée maximale de conservation et n'imposerait pas, à elle seule, d'allonger la durée actuelle de conservation de 13 mois du FNC-RF.

La participation au FNC-RF ne suffirait pas nécessairement, à elle seule, à satisfaire l'article 83a lorsque le partage d'informations requis dépasse le périmètre français. Le FNC-RF pourrait donc fonctionner comme la composante française du futur cadre européen de partage d'informations, sous réserve des adaptations requises lorsque le PSR sera formellement adopté et deviendra applicable.

6. Conformité, surveillance et obligations légales

→ 6.1 L'obligation de déclaration en tant qu'exigence légale

Se connecter au FNC-RF, déclarer les événements de fraude suspectée et qualifier les alertes relatives aux comptes détenus sont des obligations légales au titre de la loi Labaronne, et non de simples bonnes pratiques. Un PSP qui omet de déclarer une fraude suspectée, de mettre à jour une alerte lorsque les circonstances changent, ou de prendre en charge l'alerte sans délai et de partager le résultat de sa vérification dans les meilleurs délais, ne se contente pas de s'écarter des bonnes pratiques — il est en violation de ses obligations légales.

L'Autorité de Contrôle Prudentiel et de Résolution (ACPR) surveille la conformité et peut prononcer des sanctions à l'encontre des établissements qui ne respectent pas leurs obligations. La Banque de France mettra en place des indicateurs de performance pour suivre la qualité et la fréquence des déclarations de l'ensemble des participants, dont les résultats alimenteront le rapport annuel de l'OSMP. Quatre catégories de KPI sont prévues :

- Contribution au partage de données : les participants remplissent-ils leurs obligations de déclaration et utilisent-ils la plateforme conformément au cadre réglementaire et d'usage
- Conformité technique : les données soumises respectent-elles les normes techniques fixées par la Banque de France
- Efficacité du partage de données : mesure de la fraude évitée et des taux de faux positifs, évaluant l'impact réel du registre
- Analyse de la fraude : reporting statistique sur les types, sources et typologies de fraude alimentant le rapport annuel de l'OSMP et le renseignement de marché au sens large

→ 6.2 Inscription injustifiée : l'obligation de correction

Le pendant de l'obligation de déclaration est une obligation de correction tout aussi stricte. Les PSP doivent soumettre des déclarations rectificatives sans délai dès lors qu'ils détiennent des informations nouvelles ou contradictoires. Aucun compte ne peut être maintenu au registre une fois que le fondement du soupçon a changé ou a été levé.

Les établissements sont responsables de la déduplication locale des comptes signalés et du maintien de l'exactitude de leurs contributions.

Un établissement qui laisse une inscription obsolète ou erronée subsister dans le registre (par inaction ou du fait de processus internes inadéquats) s'expose à une responsabilité à la fois réglementaire et civile vis-à-vis du titulaire de compte injustement inscrit.

Le FNC-RF n'est pas une liste noire et ne doit pas être traité comme telle. Tout établissement qui utiliserait l'inscription au registre comme seul fondement pour clôturer un compte, refuser une transaction ou mettre fin à une relation bancaire risque de violer à la fois la loi Labaronne et ses obligations envers ses clients au titre du Code monétaire et financier.

→ 6.3 Obligations de conformité RGPD pour les PSP

L'arrêté du 24 avril 2026 crée des obligations RGPD explicites pour les PSP. La FAQ de la Banque de France du 26 mai 2026 fournit des orientations pratiques pour leur mise en œuvre. L'analyse qui suit s'appuie sur cette FAQ et sur les orientations préparées à la suite de l'événement du 28 mai 2026. Il s'agit d'une interprétation pratique, non d'un avis juridique ; les établissements doivent solliciter leur propre conseil.

Obligation	Ce que la loi exige	Action requise
Mise à jour des CGV/CG (art. 5 de l'arrêté / art. 12–14 RGPD / FAQ D.8)	Les PSP doivent informer les titulaires de comptes que leurs données (identifiant de compte, BIC, date de détection, catégorie et type de fraude, type de transaction, existence d'une plainte pour usurpation d'identité) peuvent être déclarées au FNC-RF en cas de fraude suspectée, et doivent expliquer comment exercer leurs droits sur leurs données.	Ajouter une clause spécifique FNC-RF à vos conditions générales de compte.
Demandes d'accès (art. 8 de l'arrêté / art. 15 RGPD / FAQ D.7)	Le PSP teneur de compte est le point de contact exclusif pour les personnes concernées. Lorsqu'un client demande l'accès, vous devez lui indiquer si son compte figure au registre et pour quel(s) événement(s) de fraude.	Mettre en place un processus interne d'interrogation du FNC-RF (via portail ou API) en réponse aux demandes d'accès, dans le délai d'un mois prévu par le RGPD.
Rectification et limitation (art. 8 de l'arrêté / art. 16 et 18 RGPD / FAQ C.9)	Vous devez investiguer sans délai le caractère frauduleux du compte, mettre à jour votre qualification dans le registre et, le cas échéant, demander au PSP déclarant de soumettre une déclaration rectificative ou de retrait.	Mettre en place un flux d'investigation et d'escalade. Important : si le PSP déclarant refuse de retirer sa déclaration malgré votre qualification contraire, l'inscription demeure au registre. La BdF n'arbitre pas les positions divergentes. Votre obligation est de documenter toutes les démarches entreprises.
Responsabilité de traitement (art. 8 de l'arrêté / FAQ D.4)	La Banque de France est responsable de traitement pour la plateforme centrale. Chaque PSP est responsable de traitement pour ses propres processus internes liés au FNC-RF. Il n'existe pas de responsabilité conjointe entre PSP.	Documenter cette activité de traitement dans votre registre des activités de traitement : base légale art. 6(1)(c) RGPD, durée de conservation de 13 mois (à compter de la déclaration ou de la dernière déclaration rectificative, la plus récente des deux), droits des personnes concernées et processus internes.
Droit à l'effacement (art. 17 RGPD)	L'art. 17 n'est pas visé par l'art. 8 de l'arrêté — l'omission est vraisemblablement intentionnelle, l'art. 17(3)(b) RGPD excluant l'effacement lorsque le traitement répond à une mission d'intérêt public. L'arrêté ne le précise toutefois pas explicitement.	Si vous êtes le PSP déclarant : vous pouvez demander la radiation à la BdF au titre de l'art. 4 de l'arrêté dès lors que le fondement du soupçon a disparu. Si un autre PSP a déclaré l'événement : vous ne disposez d'aucun moyen direct de satisfaire une demande d'effacement. Dans les deux cas, documentez le motif du refus ou de l'impossibilité, informez le client par écrit et rappelez-lui son droit de saisir la CNIL.

Nuance sur la conservation : la période de 13 mois court à compter de la date de déclaration ou de la date de la dernière déclaration rectificative, la plus récente des deux. Pour les événements contestés ou mis à jour de manière répétée, la durée effective de conservation peut donc dépasser sensiblement 13 mois à compter de la déclaration initiale. Cela doit être reflété dans la documentation de votre registre des activités de traitement.

→ 6.4 Responsabilité et devoir de vigilance

Le FNC-RF ne résout pas la lacune de responsabilité relative aux paiements autorisés. Lorsqu'un client est manipulé pour ordonner un virement frauduleux et que la banque l'exécute conformément aux instructions, le cadre juridique existant (tel que confirmé par la Cour de cassation) n'engage pas automatiquement la responsabilité de la banque.

Ce que fait le FNC-RF, c'est modifier la position probatoire des PSP dans de tels litiges. En alertant un client que l'IBAN de destination a été signalé comme suspect avant l'exécution du virement, et en documentant cette alerte ainsi que la décision du client de poursuivre, un établissement peut démontrer qu'il a satisfait à son devoir de vigilance. En l'absence d'un tel système — et d'une telle documentation — la position de l'établissement dans un litige futur est considérablement affaiblie.

La DSP3 devrait aller plus loin en clarifiant la répartition des responsabilités dans les scénarios d'ingénierie sociale, en imposant potentiellement une responsabilité accrue aux PSP dont il peut être démontré qu'ils disposaient du renseignement et n'ont pas agi en conséquence. Les établissements doivent considérer leur intégration au FNC-RF non pas simplement comme un exercice de conformité réglementaire, mais comme le socle d'une gestion du risque de fraude défendable pour le prochain cycle réglementaire européen.

→ 6.5 Coûts : un système entièrement financé par les PSP

Le FNC-RF est entièrement financé par les PSP participants. La Banque de France ne subventionne pas les coûts d'exploitation de la plateforme. Les CGU (Conditions Générales d'Utilisation) — le cadre juridique et contractuel régissant la participation — couvrent l'ensemble de la structure de facturation et de répartition des coûts, ainsi que les modalités de raccordement et d'intermédiation, les obligations de protection des données, la disponibilité de la plateforme et le support, et les dispositions de gouvernance. Les établissements doivent obtenir et examiner la documentation des CGU sur le portail FNCRF de la Banque de France avant de finaliser leurs budgets.

7. Dimensions juridiques complémentaires

→ 7.1 Le projet de base de données sur la fraude interne

Indépendamment du FNC-RF, une proposition de loi spécifique est actuellement examinée par le Parlement sur ce sujet : la proposition de loi n° 3032, déposée à l'Assemblée nationale le 7 juillet 2026 par Daniel Labaronne – le même député à l'origine de la loi Labaronne – et renvoyée à la Commission des finances. Elle vise à créer un fichier national automatisé recensant les personnes ayant commis des manquements graves à l'intégrité au sein d'une banque ou d'un établissement financier, afin d'empêcher les réseaux de fraude de placer des complices internes à des postes sensibles. M. Labaronne cite environ 500 manquements de ce type enregistrés en 2024, pour un préjudice estimé à 40 millions d'euros, d'après les données des principaux réseaux bancaires. Le projet de loi est en première lecture et n'a pas encore été examiné en séance plénière ; ses modalités – conditions d'alimentation du fichier, procédures de contestation, droits d'accès et de rectification, et droits d'opposition – restent à définir, et son adoption définitive dépendra de la manière dont seront résolues les questions de protection des salariés. Les établissements sont invités à suivre son évolution, car il créerait des obligations parallèles de déclaration et de gouvernance des données, en complément de celles du FNC-RF.

→ 7.2 La loi Labaronne au sens large

Le FNC-RF est la composante la plus visible de la loi n° 2025-1058, mais non sa seule disposition. La loi renforce également le FNCI (fichier des chèques), codifie les obligations de déclaration en matière de détection de chèques falsifiés et étend les droits de consultation au moment de la présentation d'un chèque. Les établissements concernés à la fois par la fraude au chèque et la fraude au virement doivent examiner le texte intégral de la loi plutôt que de considérer le FNC-RF comme sa seule partie opérante.

→ 7.3 Interaction avec la LCB-FT et les autres obligations de droit français

Le FNC-RF s'ajoute au cadre français existant de lutte contre le blanchiment de capitaux (LCB-FT) sans en remplacer aucun élément. Le renseignement sur les comptes suspects recueilli via le FNC-RF peut, dans de nombreux cas, également déclencher des obligations au titre du régime LCB-FT, en particulier lorsque les schémas de fraude suggèrent que des comptes sont utilisés pour l'empilement de produits d'origine criminelle. Les équipes conformité doivent veiller à ce que leurs processus internes relient les correspondances FNC-RF aux flux d'escalade LCB-FT existants plutôt que de les traiter comme des filières distinctes.

ANNEXE : Liste de contrôle pratique de conformité pour les PSP

Cette liste de contrôle résume les étapes clés qu'un établissement dans le périmètre doit accomplir pour atteindre la conformité FNC-RF. Elle est conçue comme un guide pratique pour les équipes projet, non comme un substitut au conseil juridique adapté aux circonstances propres à chaque établissement.

1 Phase 1 — Juridique et administrative

- [ ] Examiner les CGU (Conditions Générales d'Utilisation) sur le portail FNC-RF de la Banque de France : https://www.banque-france.fr/fr/FNCRF, et compléter le bulletin d'adhésion correspondant, y compris l'acceptation des conditions de facturation applicables (système entièrement financé par les PSP ; tarifs fixés par arrêté ministériel).
- [ ] Désigner les contacts internes : un contact métier, un contact technique et un point de contact interne pour les demandes d'exercice des droits des clients relatives aux inscriptions au FNC-RF. Inclure votre numéro CIB dans l'objet de toutes les communications adressées à la Banque de France.
- [ ] Communiquer à FNC-RF@banque-france.fr les adresses électroniques et numéros de mobile de toutes les personnes nécessitant un accès à la sharebox sécurisée de la Banque de France (BdF).
- [ ] Mettre à jour les conditions générales de compte pour y inclure la clause d'information relative au FNC-RF.
- [ ] Mettre à jour le registre des activités de traitement de l'établissement avec l'activité de traitement FNC-RF, en précisant l'article 6(1)(c) du RGPD comme base légale et la durée de conservation de 13 mois.
- [ ] Informer le DPO et définir la voie d'escalade vers la CNIL.
- [ ] Attribuer la responsabilité de la conformité FNC-RF au sein de la fonction conformité ou risque de fraude.

2 Phase 2 — Prérequis techniques (au moins 15 jours avant les tests)

- [ ] Confirmer le mode de connectivité : synchronisation avec le hub MISP, API directe ou intégration via TSP.
- [ ] Se procurer un certificat numérique qualifiant auprès d'une autorité de certification agréée : IGC Banque de France, RGS **/*** (recommandé) ou qualifié eIDAS. En cas d'utilisation d'un certificat logiciel, s'assurer que la clé privée est sécurisée de manière appropriée.
- [ ] Si vous utilisez MISP : installez la version MISP actuellement spécifiée par la Banque de France. Selon la note de production de mai 2026, il s'agissait de la version 2.5.16 ; une mise à jour ultérieure vers la version 2.5.36 (corrigeant les vulnérabilités connues et ajoutant un champ « première publication ») était prévue pour homologation le 18 juin et mise en production autour du 16 juillet 2026. Veuillez vérifier la version requise auprès de la Banque de France avant l'installation plutôt que de vous fier à un numéro de version fixe.
- [ ] Compléter le formulaire de raccordement et, pour les PSP teneurs de compte, le formulaire du référentiel des BIC.
- [ ] Soumettre les deux formulaires et votre certificat de test (fichier .cer) à la sharebox sécurisée de la BdF au moins 15 jours avant la date de début des tests souhaitée.
- [ ] Obtenir ou confirmer la clé API de l'établissement auprès de la Banque de France.

3 Phase 3 — Homologation (obligatoire avant l'accès à la production)

- [ ] Exécuter de manière autonome le plan de tests unitaires : connexion, authentification, cas de test positifs et négatifs, à l'aide du plan de tests client fourni par la Banque de France.

- [ ] Exécuter les tests métier de bout en bout en binôme avec un autre PSP, sur les quatre fiches de test :
  - Fiche 01 : Déclaration
  - Fiche 02 : Qualification par le PSP teneur de compte
  - Fiche 03 : Qualification par le PSP participant
  - Fiche 04 : Modification

- [ ] Accomplir la séquence de raccordement technique (voir Phase 2, étape C pour le tableau complet acteurs/actions).

- [ ] Soumettre le procès-verbal (PV) de recette en auto-certification à la sharebox de la BdF, accompagné de captures d'écran attestant de la réussite de tous les cas de test.

- [ ] Attendre la validation du PV par la BdF — c'est le passage obligé vers la connexion en production.

- [ ] Passer en production (disponible depuis le 7 mai 2026) ; observer la période de rodage recommandée de 1 à 3 mois avant l'exploitation opérationnelle complète.

4 Phase 4 — Exploitation courante

Flux de déclaration

- [ ] Construire ou configurer l'outillage interne pour générer des déclarations d'événements de fraude FNC-RF conformes, avec tous les champs obligatoires correctement mappés à la spécification de la BdF. Objectif : déclaration dans les 24 à 48 heures suivant la détection interne de la fraude.

- [ ] Établir le processus interne de soumission des déclarations rectificatives sans délai lorsque des informations nouvelles ou contradictoires apparaissent.

- [ ] Mettre en œuvre la déduplication locale des objets MISP et purger les instances locales après 13 mois, calculés à compter de la déclaration et, le cas échéant, de la dernière déclaration rectificative.

Flux de qualification du teneur de compte

- [ ] Construire un processus de gestion des alertes entrantes : détection des alertes dont les IBAN signalés appartiennent aux propres clients de l'établissement.

- [ ] Appliquer immédiatement la valeur de qualification « EN COURS » dès que l'on a connaissance d'une déclaration via la synchronisation locale, avant la qualification définitive.

- [ ] Définir des SLA pour l'accusé de réception des alertes entrantes et l'achèvement des investigations de diligence.

- [ ] Mettre en œuvre le processus de soumission de la qualification au registre, y compris les notifications de faux positifs le cas échéant.

- [ ] Mettre en place des déclencheurs de notification (courriel et/ou webhook) pour les alertes entrantes nécessitant une action.

Intégration côté client

- [ ] Intégrer la consultation d'IBAN du FNC-RF dans le parcours d'initiation de virement afin de permettre des alertes sur IBAN suspects au moment du paiement.
- [ ] Définir le libellé des alertes clients en cohérence avec le dispositif d'alerte VOP déjà en fonctionnement.
- [ ] Veiller à ce que l'alerte et la décision du client soient journalisées afin de constituer une piste d'audit.

RGPD et juridique

- [ ] Traiter les demandes d'exercice des droits des clients dans le délai d'un mois prévu par le RGPD.

Gouvernance et suivi

- [ ] Mettre en place un reporting interne sur les KPI du FNC-RF (fréquence de déclaration, délais de qualification, taux de faux positifs) aligné sur le suivi de la Banque de France.
- [ ] Planifier une revue périodique des évolutions législatives relatives au FNC-RF, notamment le décret à venir sur le passeport européen, la mise en œuvre de la DSP3/du PSR et FRIDA.

Conclusion

Le FNC-RF constitue un changement structurel dans la manière dont la France lutte contre la fraude aux paiements. Pour la première fois, un compte frauduleux signalé par une banque devient un signal de renseignement partagé sur lequel chaque établissement dans le périmètre peut agir — en quelques heures, et non en quelques jours. Pour les PSP, cela crée à la fois une opportunité et une obligation.

L'opportunité est significative : les établissements qui intègrent efficacement le FNC-RF protégeront leurs clients, réduiront leurs pertes liées à la fraude et constitueront une piste d'audit défendable dont l'importance ira croissant à mesure que la DSP3 fera évoluer les attentes en matière de responsabilité. Ceux qui traiteront la conformité comme un simple exercice de connectivité minimale (connectés mais non engagés opérationnellement) ne bénéficieront ni du renseignement, ni de la documentation nécessaire pour étayer leur position dans les litiges de fraude.

L'obligation est claire et sanctionnée : l'ACPR surveille la conformité ; la Banque de France suit la qualité des déclarations ; et la loi elle-même impose des obligations de correction juridiquement distinctes du devoir initial de déclaration. Il ne s'agit pas d'une participation facultative à un dispositif volontaire. C'est un régime légal assorti d'une supervision.

La France a explicitement positionné le FNC-RF comme le précurseur national du partage de renseignement sur la fraude à l'échelle SEPA que la DSP3 et FRIDA rendront obligatoire. Les établissements qui construisent dès maintenant une participation robuste auront une longueur d'avance lorsque le cadre européen arrivera, plutôt que d'y faire face comme à un second cycle de mise en œuvre.

La fenêtre de préparation est ouverte. Le moment d'agir, c'est maintenant.

Comment Banfico peut vous accompagner

Banfico est le partenaire technique de confiance des prestataires de services de paiement se connectant au FNC-RF. Présent à l'international, Banfico conçoit des solutions de conformité réglementaire pour l'écosystème des paiements européens, et se spécialise dans la vérification du bénéficiaire (VoP) et le partage d'événements de fraude (FNC-RF, FRIDA). Certifié ISO 27001, Banfico assure un support opérationnel 24h/24 et 7j/7.

L'utilisation directe de MISP présente des avantages indéniables : absence de frais de licence, contrôle total sur le stockage des données, corrélation native des événements et synergie réelle pour les institutions utilisant déjà MISP pour le partage d'informations sur les menaces. En contrepartie, cela engendre une charge opérationnelle plus importante : le flux de travail spécifique au FNC-RF, la maintenance continue de la plateforme et les frais administratifs qu'une configuration auto-hébergée ou basée uniquement sur une API laisse entièrement à la charge de l'institution. Banfico prend en charge ce travail, permettant ainsi à votre équipe de conserver une visibilité et un contrôle complets.

Ce qu'il faut	MISP local	API	Avec Banfico
Interface d'alerte adaptée à la qualification FNC-RF (EN COURS, REGUL, etc.)	Interface MISP générique uniquement — conçue pour les analystes threat-intel, pas pour les gestionnaires de dossiers de fraude	Aucune — une réponse API brute, sans interface utilisateur, à moins d'en construire une	Tableau de bord conçu spécifiquement pour le workflow de qualification FNC-RF
Rapprochement compte propre / IBAN avec votre base clients	Nécessite un développement sur mesure — MISP ne sait pas quels BIC/IBAN vous appartiennent	Nécessite un développement sur mesure — même lacune	Détection automatique dès l'ingestion
Validation des champs FNC-RF & règle de dédoublonnage « un évènement par compte »	Non imposée par MISP lui-même ; facile de soumettre des déclarations malformées ou en doublon	Non imposée par l'API elle-même ; même risque	Intégrée nativement, y compris pour les cas particuliers de groupes/entités
Traitement en masse des qualifications	Manuel, un évènement à la fois, sauf script personnalisé	Manuel, un appel à la fois, sauf script personnalisé	Qualification en masse prise en charge nativement
Notifications sur les alertes entrantes	Notifications email natives de MISP uniquement ; aucun déclencheur webhook sans développement sur mesure	Aucune — vous devez interroger l'API vous-même pour détecter les nouveaux évènements (polling)	Notifications email et webhook, configurables par utilisateur
Contrôle des accès utilisateurs	Modèle de connexion à instance unique partagée ; permissions granulaires par utilisateur	Aucune couche utilisateur native — le contrôle d'accès dépend entièrement de ce que vous construisez autour de la clé API	Gestion d'équipe granulaire, avec niveaux de permission lecture seule / modification par utilisateur
Accès de vos propres systèmes aux données	Sans objet — MISP est le système lui-même	Natif, puisque c'est l'API elle-même	Intégration API disponible pour la banque, en complément du portail
Acquisition et cycle de vie des certificats (QWAC et autres)	Acquisition et suivi manuels ; les délais des autorités de certification externes peuvent atteindre plusieurs mois	Même exigence et mêmes délais — le mode de connectivité ne change rien	Banfico peut se charger de l'acquisition d'un certificat QWAC dédié pour votre compte, et suit les dates de renouvellement avant échéance

Ce qu'il faut	MISP local	API	Avec Banfico
Suivi et application des mises à jour obligatoires de version MISP imposées par la Banque de France	Responsabilité continue de votre équipe, selon le calendrier de la BdF (ex. 2.5.16 → 2.5.36, homologation le 18 juin / mise en production le 16 juillet 2026 — et pour chaque future mise à jour)	Non applicable — aucune instance MISP locale à maintenir	Suivies et appliquées pour votre compte
Vue consolidée pour les groupes bancaires ayant plusieurs entités déclarantes*	Rapprochement manuel entre entités ; risque qu'un même compte soit compté deux fois comme « réutilisé »	Même risque de rapprochement manuel	Vue consolidée unique sur l'ensemble des entités du groupe
Suivi des évolutions des Règles d'usage et des décisions du COPIL	Responsabilité de votre équipe de surveiller les communications de la BdF pour détecter les changements de règles	Même charge de veille	Suivies et signalées dès leur publication
Reporting imposé par la BdF (KPI, statistiques de fraude/qualification)	Votre équipe construit et formate ces rapports en interne selon les spécifications de la BdF	Même exigence	Générés automatiquement dans le format requis par la Banque de France

**Les bénéfices de la consolidation de groupe et du dédoublonnage augmentent avec le nombre d'entités juridiques et d'organisations déclarantes concernées — surtout pertinent pour les groupes bancaires ; un PSP mono-entité en tirera moins d'avantage sur cette ligne spécifiquement.*

Deux autres points importants concernant la planification, gérés par Banfico dans le cadre de la gestion continue de votre compte : les établissements se connectant à partir de juin 2026 ne bénéficieront que d'un historique de quatre semaines lors de leur première connexion. De plus, une fois la liste blanche d'adresses IP activée pour votre mode de connexion, toute modification de votre infrastructure de serveur sortant nécessitera la mise à jour de vos adresses IP enregistrées auprès de la Banque de France, sous peine de risque de perte de connectivité.

Rapports sortants

Le formulaire de signalement de Banfico associe chaque champ obligatoire aux spécifications de la Banque de France, éliminant ainsi les erreurs de formatage manuel et les soumissions rejetées. Chaque soumission est horodatée et enregistrée dans un journal d'audit complet depuis le premier jour.

Flux entrant et recherche d'IBAN

Le flux se synchronise automatiquement quatre fois par jour, avec une possibilité d'actualisation manuelle à tout moment. La recherche d'IBAN renvoie des résultats en moins de 100 ms. Le système de détection des comptes propres de Banfico signale automatiquement les alertes lorsque l'IBAN déclaré appartient à la clientèle de votre établissement ; ces alertes vous soumettent à votre obligation légale de qualification.

Flux d'investigation

Lorsqu'une alerte entrante correspond à votre univers IBAN, elle est immédiatement mise en évidence et priorisée. Banfico propose un flux d'investigation structuré : horodatage, codes de qualification obligatoires, descriptions de résolution, qualification groupée pour les pics d'activité et notifications optionnelles de faux positifs à la Banque de France. Chaque étape est enregistrée.

Accès et notifications des équipes

Les établissements gèrent leur propre structure d'équipe via le portail dédié de Banfico : des permissions précises par utilisateur distinguent l'accès en lecture seule des droits de modification/qualification, permettant ainsi une gestion adaptée des accès pour les équipes opérationnelles et les superviseurs. Les notifications par e-mail et webhook sont configurables par utilisateur, garantissant que la bonne personne soit alertée sans perturber le reste de l'équipe.

Rapports et audit

L'historique complet des opérations, incluant chaque action, chaque acteur, chaque horodatage et les valeurs des champs avant/après, est exportable au format CSV ou Excel, avec une durée de conservation minimale de cinq ans configurables par établissement. Banfico génère également les rapports périodiques exigés par la Banque de France (indicateurs clés de performance et statistiques de fraude/qualification), au format requis et prêts à être soumis.

Mise en service

Banfico assure la connectivité complète au réseau FNC-RF de la Banque de France pour le compte de cette dernière. Banfico peut obtenir un certificat QWAC dédié pour l'authentification mTLS ou utiliser un certificat que vous possédez déjà. Banfico gère l'intégration et la couche protocolaire MISP, la synchronisation et l'ingestion des flux de données, le mappage des champs selon la spécification FNC-RF, la gestion des erreurs et la logique de nouvelle tentative, ainsi que la connectivité continue, y compris le suivi des mises à jour de la version MISP de la Banque de France afin de garantir la continuité de votre intégration. Les systèmes de la banque peuvent s'intégrer via API au portail, et un accès API complet est disponible pour les institutions souhaitant développer leur propre couche de connectivité par-dessus celle de Banfico.

Contacter Banfico

Banfico Europe GmbH
Platz d. Einheit 2, TechQuartier, 60327
Francfort-sur-le-Main, Allemagne

+44 207 993 4810

paulo.barbosa@banfico.com

www.banfico.com

Comment Herald Avocats peut vous accompagner

Herald Avocats est un cabinet d'avocats français pluridisciplinaire fondé en 1957, doté d'une expertise approfondie en droit bancaire et financier, en conformité réglementaire et en contentieux commercial.

Une expertise globale en droit bancaire et financier

Réglementation bancaire et financière

Herald accompagne les établissements de crédit, établissements de paiement, établissements de monnaie électronique, sociétés de financement, succursales étrangères et fintechs dans l'ensemble de leurs problématiques réglementaires. Le cabinet intervient notamment en matière d'agrément et de passeport européen, de gouvernance, de contrôle interne, de services de paiement, de LCB-FT, d'externalisation et de résilience opérationnelle, ainsi que dans l'anticipation des évolutions réglementaires européennes.

Financements et opérations de crédit

Herald conseille les prêteurs, emprunteurs, sponsors et investisseurs dans la structuration, la négociation et la mise en œuvre de financements domestiques et internationaux : financements corporate, immobiliers, d'acquisition, de projets et d'actifs, crédits syndiqués, refinancements et restructurations de dette. Le cabinet rédige et négocie la documentation de financement, les conventions intercréanciers, les garanties et sûretés, les conditions suspensives et les avis juridiques. Il intervient également lors des réaménagements de dette, des situations de défaut et de la réalisation des sûretés.

Structuration des activités, produits et partenariats

Herald assiste ses clients dans la création et l'évolution de leurs offres bancaires et de paiement, ainsi que dans la sécurisation de leurs relations contractuelles. Le cabinet rédige et négocie notamment les conditions générales, conventions de services, contrats d'externalisation et accords conclus avec les prestataires technologiques. Il accompagne également les projets de transformation impliquant l'adaptation des processus internes, de la gouvernance et de la documentation réglementaire.

Contrôles, procédures réglementaires et contentieux bancaire

Herald intervient lors des contrôles sur pièces ou sur place de l'ACPR, depuis leur préparation jusqu'au suivi des mesures de remédiation. Le cabinet assure également la défense des établissements devant la Commission des sanctions de l'ACPR et, le cas échéant, devant le Conseil d'État. Son équipe contentieuse représente par ailleurs les acteurs bancaires et financiers dans leurs différends avec leurs clients, partenaires ou prestataires, notamment en matière de responsabilité bancaire, de services de paiement et d'exécution des contrats de financement.

Un accompagnement spécifique en matière de FNC-RF et de fraude aux paiements

RGPD et gouvernance des données

Herald accompagne les PSP dans l'information des personnes concernées, la documentation du traitement, la définition des durées de conservation et la gestion des demandes d'accès, de rectification, de limitation ou d'effacement. Le cabinet analyse également la répartition des responsabilités entre les PSP et la Banque de France, prépare les analyses d'impact et intervient dans la gestion des violations de données ainsi que dans les échanges ou procédures devant la CNIL.

Analyse de responsabilité et gestion des litiges

Herald conseille les PSP dans le traitement des réclamations relatives aux paiements autorisés ou non autorisés et dans la constitution de dossiers probatoires complets : journaux d'authentification, surveillance des transactions, alertes adressées au client, données VoP et FNC-RF, échanges avec le client et motifs des décisions prises.

Le cabinet représente principalement les PSP en défense dans les contentieux liés aux fraudes aux paiements, notamment en cas de fraude par manipulation, d'usurpation d'identité, de contestation d'une opération ou de manquement allégué au devoir de vigilance.

Herald intervient dès la phase précontentieuse, dans le cadre des médiations et négociations amiables, puis devant les juridictions de première instance et d'appel. Le cabinet accompagne également les PSP dans leurs recours contre les autres acteurs de la chaîne de paiement.

Conseil réglementaire et conformité

Herald accompagne les PSP dans l'analyse du périmètre du FNC-RF, la définition des flux de déclaration et de qualification ainsi que la rédaction et la mise à jour des politiques et procédures internes. Le cabinet veille notamment à distinguer les obligations assorties d'un délai légal des objectifs opérationnels définis par l'établissement et à encadrer l'utilisation des informations du registre dans les décisions de suspension, de refus ou de gestion de la relation clientèle.

Herald assiste également les établissements lors des contrôles sur pièces ou sur place de l'ACPR : préparation du contrôle, revue des documents, réponses aux demandes de l'Autorité, assistance lors des entretiens et définition des mesures de remédiation. En cas de procédure disciplinaire, le cabinet assure leur défense devant la Commission des sanctions de l'ACPR et, le cas échéant, devant le Conseil d'État.

Formation et procédures opérationnelles

Herald forme les équipes fraude, conformité, juridique et opérations au cadre du FNC-RF, au traitement des alertes et des réclamations ainsi qu'à la jurisprudence relative aux fraudes aux paiements. Le cabinet rédige et met à jour les matrices d'escalade, arbres de décision, procédures de déclaration, de qualification, de correction et de radiation, modèles de communication client et protocoles de piste d'audit.

Ces procédures peuvent également être testées au moyen de revues de dossiers ou d'exercices de contrôle à blanc, puis actualisées en fonction des évolutions réglementaires, jurisprudentielles et des attentes des autorités.

Contact Herald Avocats

Herald Avocats
Avocats depuis 1957

Christophe Jacomin
Avocat associé

+33(0)153431515