Version du 22 juillet 2026

FOIRE AUX QUESTIONS sur le FNC-RF

A. Périmètre du FNC-RF		
N°	**Question**	**Réponse**
1	Cette réglementation concerne-t-elle uniquement les PSP établis en France ?	Les PSP établis en France tel que précisé au sein du L521-6-1 du code monétaire et financier (CMF). L'arrêté publié le 28 avril 2026 exclut du champ du dispositif Labaronne les établissements opérant en France en libre prestation de service (LPS). Les succursales françaises en libre établissement restent, elles, bien dans le champ d'application du dispositif français.
2	Tous les PSP français doivent-ils être reliés à la plateforme centrale pour le 7 mai ?	Le L521-6-1 du code monétaire et financier précise que son article premier entre en vigueur 6 mois après la promulgation de ladite loi. Les établissements sont invités à se rapprocher le plus rapidement possible de la Banque de France (BDF) pour indiquer leur date prévisionnelle de raccordement à l'aide du questionnaire d'interfaçage mis à disposition sur le site internet dédié.
3	La loi du 6 novembre 2025 interdit aux prestataires de services de paiement de remettre à quiconque copie des informations contenues dans le fichier. Est-ce que vous confirmez que cette interdiction n'empêche pas les PSP de confier à un prestataire tiers la consultation et l'alimentation du fichier dans le cadre d'une gestion externalisée, à l'instar de toute information couverte par le secret bancaire ?	L'arrêté technique publié le 28 avril par le Ministre de l'Économie, a confirmé dans son article 7 qu'un accès aux prestataires agissant pour le compte d'un PSP est bien possible.
4	Pouvez-vous définir exactement quels sont les établissements considérés comme PSP ?	Le L521-6-1 du code monétaire et financier fait explicitement référence au L 521-1 du même code, tout en excluant nommément les prestataires de services d'information sur les comptes, ainsi que les établissements de paiement fournissant exclusivement un service d'initiation de paiement.
5	Si un PSP français fournit à ses clients des IBAN virtuels FR alors que la tenue de compte est assurée par confrère étranger, comment s'opèrent les qualifications ?	Les CGU et les principes de fonctionnement du FNC-RF indiquent que c'est le PSP « propriétaire » du BIC FR associé à ces IBANs qui est responsable de leur qualification. Ce PSP doit donc prendre ses dispositions pour répondre aux exigences de la Loi Labaronne.

6	Qui, à part les PSP adhérents, pourront avoir accès aux données de la plateforme ?	Le L521-6-1 du CMF précise que seuls les PSP ont accès au FNC-RF en écriture (URSSAF retiré a posteriori). Le projet de loi (adopté le 30 mars 2026) portant sur la lutte contre les fraudes sociales et fiscales contient des amendements ouvrant l'accès au FNC-RF en consultation aux sociétés de financement, ainsi qu'à certaines administrations dont la liste reste à définir. Le titulaire d'un compte pourra en outre exercer un droit d'accès auprès de **son PSP** afin de savoir si son compte bancaire est enregistré au sein du FNC-RF.
7	Cette obligation s'applique-t-elle à une filiale monégasque d'une banque Française ?	L'article L. 521-6-1 du code monétaire et financier prévoit que les dispositions relatives au FNC-RF ne s'appliquent qu'aux établissements établis ou exerçant sur le territoire français. De plus, si les établissements monégasques sont contrôlés par l'ACPR, Monaco a son propre Code monétaire et financier et l'ACPR supervise ces établissements sur la base de textes européens tel que CRR et CRD et de leur transposition (article 11 de l'accord monétaire entre l'union européenne et la Principauté de Monaco). Les PSP monégasques ne sont donc a priori pas inclus dans le périmètre de la loi Labaronne.
8	Les prélèvements reçus sont-ils concernés ?	Le L521-6-1 du CMF permet de déclarer des évènements de fraude portant sur des opérations de prélèvement. Dans les faits, les cas d'usage envisagés par le groupe de travail de Place concernent principalement les virements, mais des ajustements techniques à venir permettront toutefois d'utiliser le FNC-RF dans le cadre de la lutte contre la fraude au prélèvement.
9	Les IBANs étrangers seront-ils déclarables ? Question induite pour les Succursales en France des groupes rattachés à ces IBANs étrangers : les succursales seront-elles responsables des « qualifications détenteurs » vis-à-vis de ces IBAN dans la base ?	Les comptes bancaires étrangers (IBAN ou BBAN) doivent faire l'objet d'une déclaration (évènement de fraude) au sein du FNC-RF, comme les IBAN français. Concernant le cas des groupes, la qualification détenteurs de comptes gérés par d'autres entités appartenant au même groupe paraît contrevenir au principe de non divulgation des données à des tiers, inscrit dans le L521-6-1.
10	Quelles sont les autres pays qui ont mis en place un dispositif similaire en avance de phase du dispositif européen ?	Les places italienne, suisse, autrichienne néerlandaise, britannique, polonaise et espagnole ont déjà mis en place des fichiers similaires, mais non gérés directement par leurs banques centrales comme en France.

11	Quelle typologie juridique de compte est déclarable ? les comptes de paiement ? .. autres ?	Les comptes de paiement et de dépôt comme précisé au sein du L 314-1 du CMF.
12	Bien que classé PSP par l'ACPR, je ne fournis pas de services de paiement à ma clientèle. Suis-je obligé de me raccorder au FNC-RF ?	Les services de paiement sont définis par l'article L314-1 du CMF. Les paiements associés à une ouverture de crédit y sont par exemple considérés comme un Service de Paiement, au contraire des paiements liés aux services de titres. Les services de l'ACPR confirment donc que les PSP réalisant exclusivement des opérations de paiement liées à des transactions sur des instruments financiers (ou autre opération mentionnée au III de l'article sus mentionné) ne sont pas assujettis au FNC-RF. Chaque PSP se trouvant dans ce contexte devra transmettre par courriel une demande formelle à l'Administrateur du FNC-RF. Celui-ci validera auprès de l'ACPR cette sortie du périmètre d'assujettissement.

B. Connexion au FNC-RF - certificats

N°	Question	Réponse
1	Quelles solutions sont privilégiées pour la connexion ? notamment pour les "petits" établissements	Les PSP peuvent se connecter via synchronisation, API ou par l'entremise d'un prestataire. Les petits PSP peuvent recourir à un prestataire externe s'ils souhaitent éviter d'engager des développements informatiques.
2	Est-ce que chaque PSP reçoit l'intégralité de la base tenue par la BdF ? Même s'il n'est pas teneur des comptes déclarés ?	OUI. La réception se fonde sur le principe de synchronisation au moins quotidienne entre les bases locale et centrale.
3	Quel est le processus d'adhésion ?	Le PSP passe en premier lieu par une phase d'homologation client, suivie de la signature de la documentation juridique (les CGU + formulaires), avant de pouvoir participer au dispositif en production.
4	Avez-vous des exemples de prestataires techniques?	La BDF reste neutre quant au choix des prestataires. Il est en revanche possible de la contacter afin d'obtenir la liste des prestataires qui se sont signalés auprès d'elle à ce jour, sachant qu'il n'y a aucun processus de certification de la part de la BDF.
5	Un PSP peut-il exporter les informations de la base centrale vers une base locale que le PSP va pouvoir interroger avant chaque virement ?	OUI, c'est un des principes de base du fonctionnement des plateformes MISP choisies pour la gestion du FNC-RF. Une interrogation directe du FNC-RF à chaque opération de virement doit en revanche être absolument évitée.
6	Quelles sont les autorités de certification admises par la BdF pour sécuriser la connexion au FNC-RF ? (en sus de l'IGCV3 produite par la BdF)	**Editeur / AC Racine** **GlobalSign (Belgique)** GlobalSign Root R6 **Sectigo (Espagne)** Sectigo Public Server Authentication Root E46 **Certinomis (France)** Certinomis Racine G3 Certinomis Racine G4 Certinomis Racine WEB **ChamberSign (France)** ChamberSign France CA3 Root **Certigna (France)** Certigna Client authentication Root CA Certigna Client authentication EU Root CA **DigiCert (Pays-Bas)** QuoVadis Root CA 1 G3 DigiCert High Assurance EV Root CA DigiCert Global Root G2 DigiCert Global Root CA Cert Europe Tinexta InfoCert SpA

7	Les certificats nécessaires pour la PROD et l'homologation sont-ils distincts ?	NON, un même certificat **peut** servir aux 2 environnements.
8	Dois-je compléter le formulaire de listage des BICs si je ne gère pas de compte bancaire pour ma clientèle ?	NON, ce formulaire sert à définir le périmètre de comptes bancaires que vous seriez amenés à « qualifier » en cas de déclaration de soupçon de fraude par un confrère (grâce au lien IBAN-BIC). Si vous n'êtes pas « détenteur » de comptes bancaires, vous n'avez pas à le remplir.
9	Quel type de certificat « client » ou « client-serveur » doit fournir un PSP ne faisant pas appel à l'AC BDF	Le PSP doit fournir **le .cer en base 64** du X509 d'un certificat de type : PSD2 eIDAS QWAC dont l'AC intermédiaire figure dans la liste de la question B6.
10	Quel est le processus de demande de certificat logiciel de l'AC BdF ?	- Les formulaires doivent être entièrement complétés, contrôlés et **accompagnés des documents demandés inscrits sur les formulaires**. - Il convient aux entreprises demandeuses de désigner un mandataire de certification qui signera la demande et sera responsable du certificat. - Les demandes doivent être envoyées par mail à notre BAL : FNC-RF@banque-france.fr (en attendant la dématérialisation de notre processus des demandes). Les modèles de formulaires sont disponibles sur la rubrique Certificats | Banque de France de notre page internet.
11	Un certificat BDF servant à interagir avec POBI le Portail Banque de France peut-il convenir pour le FNC-RF ?	NON
12	Quelles sont les adresses IP à déclarer sur le formulaire de raccordement ?	Il s'agit des @ nattées, donc publiques, des canaux de sortie du Participant sur le réseau internet. (Le canal MEXIC n'est pas utilisé par le FNC-RF)
13	Faut-il s'enregistrer au FNC-RF si on passe déjà par un prestataire pour nos interrogations BDF des fichiers d'incidents de paiement (FCC – FICP …)	OUI, ce sont des processus tout à fait distincts : les modalités d'interactions et les modes de fonctionnement sont totalement différents pour le FNC-RF par comparaison aux fichiers d'incidents de paiement (FCC, FICP…). Pour le Fichier de lutte contre la fraude, vous aurez à gérer, vous ou le prestataire choisi, une copie « locale » de la base de données, qui servira après retraitement à alimenter vos process internes (automatisés ou non).
14	Pouvons-nous référencer des plages IP dans la demande de raccordement plutôt qu'une liste unitaire ?	OUI
15	Comment obtenir la clé publique du certificat au format .CER si je n'ai qu'un fichier CRT ?	La commande pour passer de l'un à l'autre est : openssl x509 -in "_filename_.crt" -outform DER -out _filename.cer Ce sont les mêmes données, au bon format demandé par l'Administrateur du FNC-RF.
16	Toutes les Autorités de Certification RGS**/*** sont elles acceptées par la Banque de France ?	NON, la certification RGS**/*** est une condition nécessaire, mais non suffisante, pour être acceptée par les services de sécurité de la BdF.

C. Fonctionnement du FNC-RF		
N°	**Question**	**Réponse**
1	Le PSP détenteur doit il obligatoirement donner un avis ?	OUI. L'article 1er du 521-6-1 du CMF prévoit en effet que : « Lorsqu'un compte figure dans le fichier, le prestataire de services de paiement chargé de la tenue de ce compte effectue sans délai l'ensemble des diligences visant à évaluer son caractère frauduleux. »
2	Sous quel délai doit s'effectuer la qualification ?	La loi précise "sans délai", il est donc attendu que chaque établissement participant commence immédiatement à investiguer lorsqu'un de ses comptes est déclaré dans le fichier afin d'informer ses confrères le plus rapidement possible. Dans les faits, il n'y a pas de délai maximal fixe pour communiquer au FNC-RF le résultat des investigations. Un suivi statistique sera cependant réalisé par la Banque de France. Si le délai moyen d'investigation affiché par un établissement devait être très supérieur à la moyenne observée sur l'ensemble des participants, la Banque de France organiserait une réunion bilatérale afin de comprendre les raisons pouvant expliquer ces délais et voir comment y remédier en collaboration avec l'établissement concerné.
3	Si un IBAN est inscrit dans le fichier, les PSP ont-ils l'obligation de bloquer les opérations à destination de ce compte ?	NON, il n'y a pas d'obligation portant sur les PSP en matière de blocage des paiements. Le FNC-RF n'est pas une liste noire. La décision finale repose toujours sur l'analyse des équipes en charge de la fraude chez chacun des PSP.
4	Quels sont les critères qui permettent de considérer qu'un IBAN est douteux ?	La définition du caractère frauduleux ou non d'un compte est laissée à la responsabilité de chaque PSP. Pour aider les participants à se saisir de cette notion, des exemples sont fournis dans le tableau 1 en fin de ce document.
5	Y a-t-il une obligation de rapidité pour la déclaration dans la base afin que les informations soient les plus fraîches possibles pour l'efficacité du système ?	OUI, dans le but de limiter les cas de fraude.
6	Afin de tenir compte des IBAN virtuels, est-il envisagé d'imposer au PSP teneur du compte de notifier les autres IBAN rattachés au même compte, ou toute autre mesure visant à contourner l'utilisation de la base comme outil de contrôle collectif ?	NON, seul un IBAN identifié dans une fraude peut être déclaré au sein d'un évènement de fraude. Plus largement, les interrogations afférentes aux IBANs virtuels sont en cours d'analyse au sein de différentes instances de Place ou européennes.
8	Quel est le statut transitoire d'un compte sur la plateforme dans l'attente d'une confirmation de fraude par l'établissement teneur de compte ? Est-il catégorisé par défaut comme 'Frauduleux' ou existe-t-il un statut intermédiaire de suspicion ?	La notion de statut n'existe pas au niveau de l'évènement de fraude. A sa déclaration dans le FNC-RF, l'événement n'a pas de valeur de qualification. Lorsque le PSP détenteur (si celui est bien connecté au FNC-RF) prend en charge le dossier d'investigation, il appose une

		qualification « en cours / under investigation » le temps de son instruction. Cette qualification peut ensuite être enrichie d'autre valeurs en fonction du résultat de l'analyse du détenteur de compte (Frauduleux, Commerçant, Légitime, Régularisé, Clos, etc..), mais est toujours à la main du PSP détenteur. Les PSP exploitant les déclarations de soupçon de leurs confrères dans le FNC-RF doivent donc définir dans leurs modèles de scoring le niveau de risque à raisonnablement associer à chacune de ces valeurs (ou absence de valeur).
9	Comment vont se régler les divergences entre Établissement déclarant et Établissement teneur du compte (sur le retrait de la base naturellement) ?	Le PSP teneur du compte déclaré comme suspect devra qualifier ce compte (en précisant s'il est légitime ou non) Le PSP déclarant peut ensuite corriger sa propre déclaration, **ou non**. Si le déclarant opte finalement pour la suppression, cet événement sera ensuite supprimé dans les bases centrale et locales. La Banque de France n'aura pas pour rôle de réconcilier des visions potentiellement contradictoires entre participants.
10	Le délai de purge est-il prorogé si un second établissement déclare un évènement de fraude plusieurs mois après un 1er évènement ?	Toute nouvelle déclaration (événement de fraude) est gérée individuellement au sein de la plateforme ; cette nouvelle déclaration aura donc un cycle de vie qui lui sera propre. La purge de 13 mois est ainsi appliquée événement par événement.
11	Est qu'il y aura une sorte de "liste blanche" empêchant d'ajouter l'IBAN d'un organisme ayant un IBAN unique pour tous ses clients ?	NON, il n'y aura pas de liste blanche. Un IBAN légitime pourra être ainsi qualifié comme tel par le PSP détenteur de compte.
12	Que se passe-t-il si une banque déclare un cas, et qu'un client d'une banque émet un virement vers un IBAN de cette liste ? le virement est-il traité, l'établissement est-il alerté ?	Chaque PSP participant est responsable de la synchronisation de sa base de données locale avec le FNC-RF afin de récupérer au plus vite les évènements de fraude déclarés par la Place. Il est ensuite totalement maitre de la manière dont il utilise cette donnée au sein de ses outils de lutte contre la fraude.
13	Comment positionner la frontière entre la Qualification par un PSP participant à un 1er évènement de fraude VS déclarer un nouvel évènement sur le même IBAN ?	Le PSP doit déclarer un évènement de fraude au sein du FNC-RF lorsqu'il suspecte une fraude bénéficiant à un compte bancaire. Si ce compte est déjà présent dans le FNC-RF, le PSP est également invité à réagir sur les évènements existants par une qualification participant (= observations).
14	Est-ce que les commentaires de l'établissement teneur de compte seront tout de même mentionnés si le déclarant ne veut pas retirer sa déclaration ?	OUI. La qualification du compte par le détenteur de compte est primordiale.
15	Est-ce que l'historique complet des 13 derniers mois (selon les dernières modifications) sera accessible afin de permettre aux PSP des analyses à froid pour renforcer les dispositifs de détection de fraude ?	La totalité des données non purgées sera disponible au sein de la plateforme centrale.

16	Les KPI seront disponibles en temps réel ou via rapport OSMP ?	Il n'y aura pas de KPI en temps réel. Certains KPI permettant de juger de la performance du dispositif seront présentés au sein du rapport de l'OSMP. D'autres KPI seront utilisés par la Banque de France afin de s'assurer que les principes actés par le Comité de pilotage de Place sont bien respectés par les participants.
17	Est-il possible de partager les alertes fraude avec des clients commerçants ?	NON, les événements de fraude transmis à travers le FNC-RF ne peuvent être utilisés qu'en interne par les PSP pour leurs propres algorithmes et process internes de lutte contre la fraude.
18	Un même compte bancaire peut-il être associé à plusieurs événements distincts ? Les actions (qualification, observation, suppression…) s'appliquent elles bien à un événement et non directement au compte bancaire?	OUI aux 2 questions. C'est bien l'événement de fraude qui est l'élément pivot de la base de données du FNC-RF, et non l'identifiant du compte bancaire. Les premières semaine d'exploitation du dispositif montrent une proportion de 1 IBAN pour 4 événements de fraude.
19	Le planning du projet indique que le raccordement des PSP en production est prévu au plus tôt à partir du 7 mai 2026. Dans le cas de ces PSP « A » et « B » : • Etablissement bancaire « A » Déclarant (raccordé à MISP) • Etablissement bancaire « B » Teneur du compte déclaré (non encore raccordé à MISP) Est-ce qu'une notification de non atteignabilité de l'établissement bancaire « B » sera envoyée par BDF à l'établissement « A » ?	Le simple fait que la banque B ne « qualifie » pas l'événement de fraude est en soi une quasi notification de non atteignabilité. Cette situation d'absence de qualification sera toujours une possibilité, même bien après le démarrage du FNC-RF, en particulier pour les comptes tenus dans des banques étrangères (qui ne pourront pas participer au système français tant que l'interopérabilité européenne demandée par le R)SP (DSP3 ne sera pas mise en place.) Les algorithmes de lutte anti-fraude de chaque PSP doivent tenir compte de cette possibilité. Par ailleurs, dans le cadre du démarrage du FNC-RF, il a été prévu par le Comité de Place de mettre en place une phase de rodage et de montée en charge de 2 à 3 mois (jusque début septembre), avant que tous les nouveaux moyens de lutte contre la fraude ne soient activés.

D.Règlementation relative au FNC-RF		
N°	**Question**	**Réponse**
1	La loi du 6 novembre 2025 mentionne un décret. Savez-vous quand ce décret sera publié ?	Les arrêtés technique et tarifaire ont été publiés au JOE le 28 avril 2026.
2	Si un PSP français n'est pas connecté à la plateforme le 7 mai, que risque-t-il ?	La loi entre en vigueur 6 mois après sa promulgation le 6 novembre 2025. Passé ce délai, un PSP se retrouve de fait en non-conformité réglementaire s'il n'est pas connecté au fichier. Si des établissements rencontrent des difficultés dans le cadre de leur raccordement au dispositif, nous leur conseillons d'en informer la BDF dans les plus brefs délais.
3	Quid des comptes frauduleux dans le cadre AMLFT ? Le fait de "trahir" la confidentialité peut-il nous être opposé ?	Ces échanges d'information seront autorisés par la loi à partir du 7 mai.
4	Les banques sont-elles co-responsables de traitement au regard du GDPR ?	Selon les CGU du dispositif, la Banque de France est responsable de traitement au regard du RGPD pour ce qui a trait à la plateforme centrale. Chaque PSP est responsable de traitement au regard du RGPD pour ce qui concerne ses processus internes.
5	Quelles sont les sanctions en cas de non-déclaration ?	Les PSP sont tenus de déclarer au sein du FNC-RF les informations permettant d'identifier les comptes de paiement et les comptes de dépôt qu'ils estiment susceptibles d'être frauduleux en se fondant notamment sur les analyses réalisées dans le cadre de leurs dispositifs internes de lutte contre la fraude. En France, l'ACPR est l'autorité qui veille au respect et à la mise en œuvre de la règlementation à laquelle sont assujettis les PSP.
6	La déclaration d'un événement de fraude peut 1) justifier automatiquement une déclaration de soupçon à Tracfin ? ou 2) exempter une DS à Tracfin ?	Il n'existe pas de lien direct, les règles de déclaration sont distinctes (notamment les montants)
7	Un tiers pourrait-il saisir la CNIL pour avoir connaissance de la banque qui a généré l'alerte ?	Le titulaire d'un compte pourra exercer son droit d'information auprès de son PSP afin de savoir si son compte bancaire est enregistré au sein du FNC-RF et pour quel dossier. Pour mémoire, le FNC-RF n'enregistre pas l'identité du titulaire du compte déclaré suspect.
8	Quid des éventuelles modalités d'information des titulaires de comptes sur ce dispositif pour les PSP et sur la possible transmission de leurs coordonnées bancaires dans ce cadre ?	Une mention devra être ajoutée dans vos CG de tenue de compte (le FNC-RF est une contrainte règlementaire)

E. Facturation du FNC-RF		
N°	**Question**	**Réponse**
1	La facturation repose sur les établissements teneurs des comptes ou sur les établissements ayant fait les déclarations ?	La facturation comprend une part fixe d'un faible montant, à laquelle s'ajoute une part variable proportionnelle au nombre de comptes de paiement et de dépôt.
2	Les établissements digitaux investissent moins dans la lutte antifraude et sont beaucoup plus exposés... Plus logique que la part variable soit proportionnelle au nombre de comptes notifiés à risque de fraude ? Principe de l'hébergeur de fraudeur - payeur ?	Plusieurs méthodes de facturation ont été étudiées par le groupe de Place. Les principes définis à la question 1 ont été validés en comité de pilotage de Place. La variable « nombre de comptes de paiement et de dépôt » présente l'avantage d'être assez objective.
3	On parle bien de nombre de compte de dépôt et pas de nombre de clients ? Un client titulaire de plusieurs comptes de dépôt sera pris en compte plusieurs fois ?	OUI
4	Quand seront émises les refacturations des dépenses d'investissement de la BdF ?	Elles sont planifiées pour moitié sur 2 années : 2027 et 2028.
5	A quelle date seront émises les premières refacturations de fonctionnement de la BdF ?	Les factures liées au fonctionnement 2026 seront émises en sept 2027 pour les PSP raccordés au 31 dec 2026.

F. Phase d'Homologation		
N°	**Question**	**Réponse**
1	L'homologation est-elle bien possible après le 7 mai ?	OUI, ainsi que des tests libres, dans la limite des disponibilités des équipes techniques de la Banque de France.
2	Un certificat est-il nécessaire pour l'homologation ?	OUI. Attention, les délais d'obtention peuvent être très longs !
3	Comment compléter le BIC11 de l'établissement déclarant à renseigner dans un événement de fraude (page 24 des SEG V2.3)	Le BIC du déclarant • est une donnée facultative, ○ qui a été demandée par au moins un groupe bancaire qui, va y indiquer le BIC de l'entité à l'origine (et donc pas le chef de file) • est complété par le déclarant (donc pas par la plateforme centrale de la BDF) La BdF n'a pas de préconisation particulière à ce stade sur la manière de le compléter, puisque ce champ n'est pas exploité sur le fichier central. Le Déclarant est identifié par son organisation créé lors du raccordement au FNC-RF (OrgC de l'événement). Cette information est partagée à tous et notamment au teneur de compte qui qualifie.
4	Existe-t-il un niveau de distribution recommandé que l'un PSP devrait utiliser pour permettre la qualification correcte des évènements de fraude entre banques ?	Le niveau de distribution d'une Note de qualification détenteur de compte est fonction du mode d'interfaçage avec la Plateforme centrale MISP BDF. - En **mode API** : le niveau de distribution de la Note envoyée vers la Plateforme centrale (via le web service « /analystData/add ») doit être « **This community only** » - En **mode MISP** : le niveau de distribution de la Note créée via l'interface MISP locale doit être « **Connected communities** ». Les Notes créées en local (mode MISP) doivent être envoyées vers la Plateforme centrale via le mécanisme MISP « PUSH ALL ». Si la Note respecte les exigences (valeur, niveau de distribution, organisation créatrice), elle sera intégrée en central.

5	Comment devons-nous qualifier le "transaction type" dans le cas où nous identifions un IBAN destinataire potentiellement frauduleux tenu par un confrère ?	La logique de classification repose sur le type de transaction déclaré, pas sur la notion de flux entrant ou sortant. Vous devez donc bien déclarer un SCT dans votre alerte (s'il s'agit bien d'une opération de virement), même si votre établissement l'a émis et non reçu.
6	Nous identifions un compte tenu dans notre établissement comme frauduleux, à la suite de l'examen de l'historique d'activité de celui-ci. Comment devons-nous qualifier le "Transaction Type" dans ce cas précis ?	Logique identique au cas précédent : pourquoi vos équipes estiment-elles que le compte est frauduleux : Est-ce à l'occasion d'une opération de paiement, ou par recoupements en estimant que l'identité du titulaire du compte a été usurpée ou fabriquée ? La réponse donne le type de transaction à utiliser dans le FNC-RF.
7	Nous rencontrons des timeouts systématiques lors des interrogations en mode API. Quel est le problème ?	Nous préconisons fortement d'utiliser les paramètres « **limit** » et « **page** » (valeur du paramètre « page » à incrémenter jusqu'à ce que le résultat de la recherche soit vide) dans le corps de la requête du web service « /events/restSearch ». Un exemple de requête issu des SED : - Paramètres de l'URL : « /events/restSearch » - Corps de requête au format json : {"returnFormat": "json", "last": "2h", "includeAnalystData": true, "limit": 200, "page": 1} À noter qu'en Homologation comme en Production, le timeout du serveur API BDF est de 60 secondes. Nous suggérons d'utiliser une valeur comprise entre 200 et 500 pour le champ ***limit.***
8	Nous avons des problèmes de connexion à l'api, avec le message suivant : *The remote certificate is invalid because of errors in the certificate chain: UntrustedRoot*	Le service gérant l'API Management BDF comprend, à partir de vos messages, que vous devriez ajouter la chaine de certification IGCV3 de la BDF dans votre trustStore. Les problèmes seront identiques en Prod. La chaine de confiance de l'AC BdF à installer sur votre SI est disponible sur cette page : Certificats | Banque de France

9	Sur les Tags de façon générale, dont le Tag de suppression, il n'y a pas de date associée. Avez-vous des préconisations pour déterminer une date de suppression? C'est elle qui nous permettra de déterminer la fin du délai des 4 jours prévu par les CGU.	A la réception d'un Tag « EVENT_TO_DELETE_1 » ou « EVENT_TO_DELETE_2 » émis par le PSP déclarant sur un événement de fraude partagé en central, la date de modification de l'événement de fraude est automatiquement mise à jour par MISP. Toute nouvelle modification de l'événement par le PSP déclarant est interdite (des contrôles fonctionnels sont effectués par le MISP central) . C'est sur cette Date de modification de l'événement que s'appuie le traitement de suppression par l'Administrateur des événements tagués « à supprimer » (cf. SEG). **Il n'y a pas de date spécifique liée à l'association d'un Tag à un événement de fraude.**
10	Pour connaitre la Date de création de l'EVT par le PSP qui saisit l'EVT : Quelle est la donnée qui me permet de connaître cette information ?	Il n'y a pas à proprement parler de Date de création d'un événement. **En mode API :** Il est demandé aux PSP de ne pas renseigner la Date & heure de modification d'un événement (« timestamp ») lors de la déclaration d'un événement de fraude sur le MISP central : - Si le champ est bien absent du fichier json reçu, MISP renseignera en central la Date & heure de modification de l'événement (« timestamp »); - Par contre, si le champ est présent dans le fichier json reçu, MISP conservera la valeur renseignée dans ce fichier. **En mode MISP :** Lors de la synchronisation d'un nouvel événement créé en local avec le MISP central (en mode PUSH), la Date & heure de modification de l'événement (« timestamp ») en central correspond à celle en local.
11	Comment connaitre la Date de transmission initiale de l'EVT à la BdF	À la création d'un nouvel événement de fraude dans la base de données du MISP central, la Date & heure de publication de l'événement (« publish_timestamp ») va être renseignée en central avec la date & heure de traitement. À chaque modification d'un événement de fraude soit par le PSP déclarant (enrichissement du contexte de fraude, ajout d'une Qualification Détenteur ou d'une Qualification Participant, ajout d'un Tag « Événement à supprimer ») ou par un autre PSP (ajout d'une Qualification Détenteur ou d'une Qualification Participant), la Date & heure de publication de l'événement (« publish_timestamp ») va être mise à jour en central avec la date & heure de traitement.
12	Comment retrouver la date de 1ère récupération d'un EVT par un PSP	**En mode MISP :** Lors de la synchronisation d'un événement présent en central et absent en local (PULL) : - La Date & heure de publication de l'événement (« publish_timestamp ») en local va être renseignée avec la date & heure de traitement ; - La Date & heure de modification de l'événement (« timestamp ») en local correspondra à celle en central. **En mode API :**

		- Cf. réponse précédente pour la valorisation en central de la Date & heure de publication de l'événement (« publish_timestamp ») ; - La Date & heure de modification de l'événement (« timestamp ») en central correspond à celle sur le MISP local du Déclarant de l'événement de fraude.
13	Je constate que plusieurs évènements arrivent sur notre plateforme locale MISP avec la distribution « **Your organisation only** ». Je ne peux les qualifier.	Il n'y a pas à modifier la distribution de ces événements en local pour y ajouter des Notes. Il est rappelé que seul le PSP déclarant peut modifier son événement. Toute modification effectuée en local (via un user avec le rôle « admin ») par un PSP sur un événement dont il n'est pas le déclarant ne sera pas propagée en central (N.B. : les Notes & Sightings ne sont pas considérés comme une modification d'un événement : la date & heure de modification de l'événement reste inchangée lors de l'ajout d'une Note ou d'un Sighting).
14	Nos requêtes vers l'endpoint suivant échouent systématiquement avec une erreur **401 Unauthorized** : • **Endpoint :** /events/restSearch • **Détail de l'erreur :** API Gateway encountered an error. Error Message: Token specified is invalid or has expired.	Cette erreur « ***Token specified is invalid or has expired.*** » est documentée dans le document « **FNC-RF_Homologation_Authent_API_V1.1_20260225.pdf** » accessible depuis la ShareBox sous le répertoire racine ***« FNCRF- Spécifications ».*** Ce document précise comment accéder au service d'autorisation ***(/getAccessToken)*** En effet, pour appeler les services MISP (ici, events/restSearch), il faut présenter un token valide dans le header « ***Authorization*** » (cf. SFD). Pour récupérer un token valide, il faut accéder au service d'autorisation avec les crédenciales ***(Client ID et Client Secret)*** qui vous ont été communiqués. Chaque token a une durée de validité d'une heure (la durée de validité est précisée dans le retour du web service */getAccessToken*) : Après une heure, il faut récupérer un autre token valide.
15	Pourriez vous nous indiquer quelle est la longueur maximale autorisée pour le champ (**sus-acct-iban)** ?	Extrait des spécifications FNC-RF (§ 9.6) Un **IBAN** « ***International Bank Account Number*** » est un identifiant international d'un compte bancaire. Il est constitué au maximum de 34 caractères alphanumériques. Dans le cadre de la solution interbancaire de partage des données de fraude, un IBAN est considéré comme valide si : ▪ Il est constitué de caractères alphanumériques d'une longueur comprise entre 15 et 34 caractères (inclus) dont: Les deux premiers caractères sont des caractères alphabétiques *([A-Z]).* Les deux caractères suivants sont des chiffres *([0-9]).* Les caractères suivants sont des caractères alphabétiques et/ou des chiffres. ▪ La clé de contrôle est valide. Le **BBAN** *« **Basic Bank Account Number** »* représente un numéro de compte bancaire spécifique à un pays. Le BBAN est la dernière partie de l'IBAN. Un BBAN est considéré comme valide sur le FNC-RF si : ▪ Il est renseigné à partir d'une chaine de caractères alphanumériques de longueur strictement supérieure à 1.

TABLEAU 1 : Annexe à la question C4 :

Exemples de raisons objectives de suspecter une fraude par un PSP :

Indicateurs de fraude

1. Données de connexion

- Utilisation d'un même appareil de connexion pour plusieurs comptes clients distincts.
- Changement suspect du système d'exploitation
- Connexion depuis un pays incohérent avec le profil client
- Utilisation d'un VPN, proxy ou outil d'anonymisation
- Variation rapide ou inhabituelle des adresses IP
- Tentatives multiples d'un OTP avant de réussir
- SIM Swap (numéro de téléphone détourné vers une autre carte SIM)

2. Données bancaires

- Réutilisation d'un même IBAN dans plusieurs alertes de fraude
- IBAN associé à plusieurs victimes distinctes
- Incohérence entre le nom du bénéficiaire déclaré et le titulaire réel du compte

3. Données KYC

- Réutilisation d'un même numéro de téléphone sur plusieurs comptes
- Réutilisation ou variation d'identité entre plusieurs comptes
- Réutilisation d'emails sur différents comptes

Typologies de fraude

- Account Takeover
  Le fraudeur prend le contrôle d'un compte client existant
- Ouverture de compte frauduleuse
  Compte créé avec une identité fausse ou usurpée
- Compte mule
  Utilisé pour les transferts d'argent
- Fraude fournisseur
  Usurpation pour détourner des paiements
- Fraude à la paie
  Détournement de salaires
- Escroquerie
  Arnaque au président, romance scam etc…
- Contestation frauduleuse de paiement (friendly fraud)
  Contestation abusive d'un paiement légitime pour obtenir un remboursement
- Défaut de paiement frauduleux
  Non remboursement volontaire d'un crédit