ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

Forum Fintech ACPR AMF

Atelier « Lutte contre le blanchiment et le financement du terrorisme (LCB-FT) »

Points d'attention des superviseurs et principaux enjeux pour les acteurs

14 octobre 2024

LCB-FT : POINTS D'ATTENTION DES SUPERVISEURS, PRINCIPAUX ENJEUX POUR LES ACTEURS

I. **IBANs virtuels, transparence de la chaine de paiement… : retours sur le questionnaire ACPR et réflexions autours de la recommandation 16 du GAFI** *(Stéphane Mahieu, ACPR DLCB-FT)*

II. **Présentation de LUCIA** *(Vincent Vasques & Jean-François Cotier, ACPR DCP)*

III. **Orientations « TFR » : exigences en matière d'information concernant les transferts de fonds et certains transferts de crypto-actifs** *(Sylvain Aubert, AMF)*

IV. **FATF Standards on Virtual Assets and Virtual Assets Service Providers** *(Dooyoung Kim, FATF - Henriette Richard & Jocelyn Long, ACPR DAJ)*

I. IBANs virtuels, transparence de la chaine de paiement… : retours sur le questionnaire ACPR et réflexions autours de la recommandation 16 du GAFI

INTRODUCTION

En mars 2023, la Direction LCB-FT de l'ACPR a adressé un questionnaire à 23 entités, dans le but de faire un état des lieux des pratiques des services de vIBAN impliquant la France.

Périmètre de l'étude :

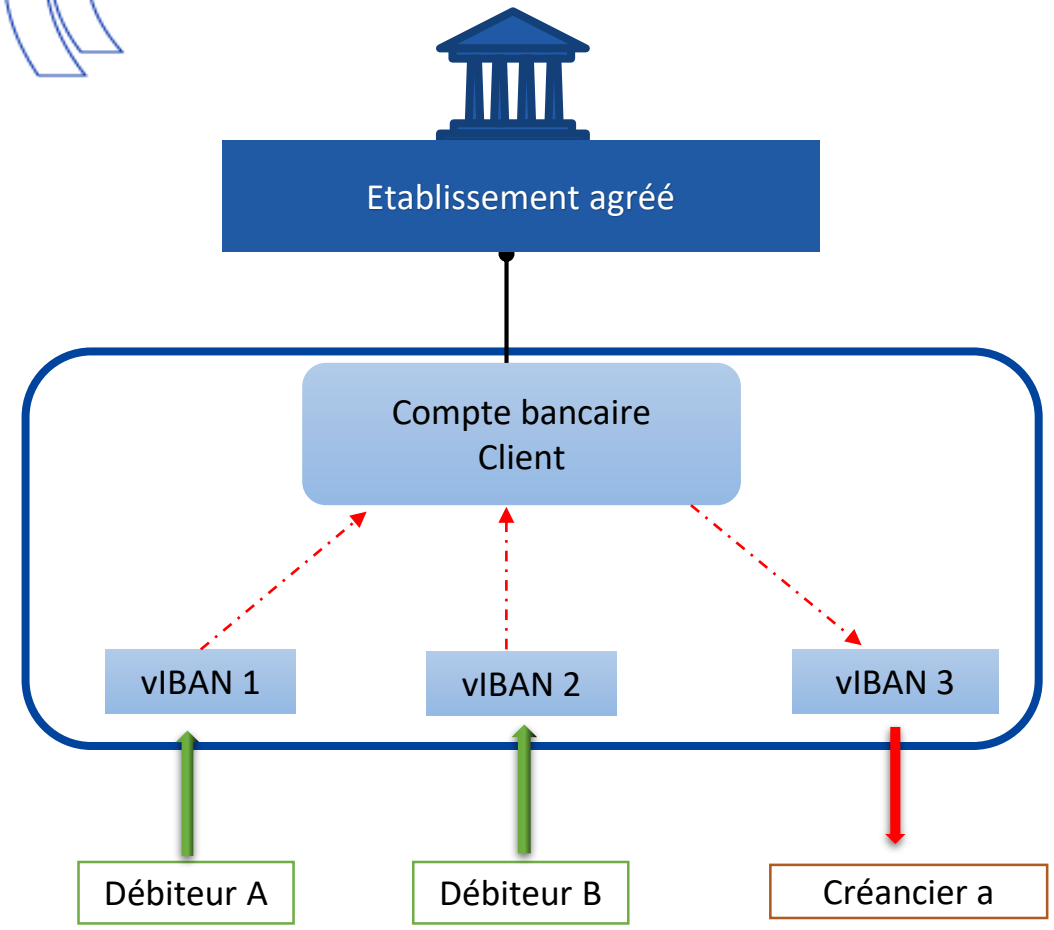
✓**vIBAN définis comme « des pratiques consistant à associer plusieurs codes ayant l'apparence formelle d'IBAN (vIBAN) à un unique compte de paiement. Des virements faits à destination ou en provenance d'un vIBAN mouvementent en réalité cet unique compte maître. »**

✓**Service de vIBAN impliquant la France :**

- le **compte maître** a un IBAN FR,
- un **vIBAN** avec un code FR,
- offre de VIBAN par une **entité française** supervisée par l'ACPR (y compris codes vIBAN étrangers, et clients résidents étranger)
- offre de VIBAN aux **clients français** par des entités d'un groupe étranger

** Document FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021)*
*** Revue thématique de l'ACPR sur les dispositifs automatisés de surveillance des opérations en matière de LCB-FT (Avril 2023)*

CAS D'USAGE N°1 - RÉCONCILIATION COMPTABLE



1 VIBAN = 1 contrepartie

Comptes clients	
Client A	VIBAN 1
Client B	

1 VIBAN = référence du compte principal

Titulaire VIBAN = titulaire compte principal

VIBAN et IBAN tous les deux de code FR

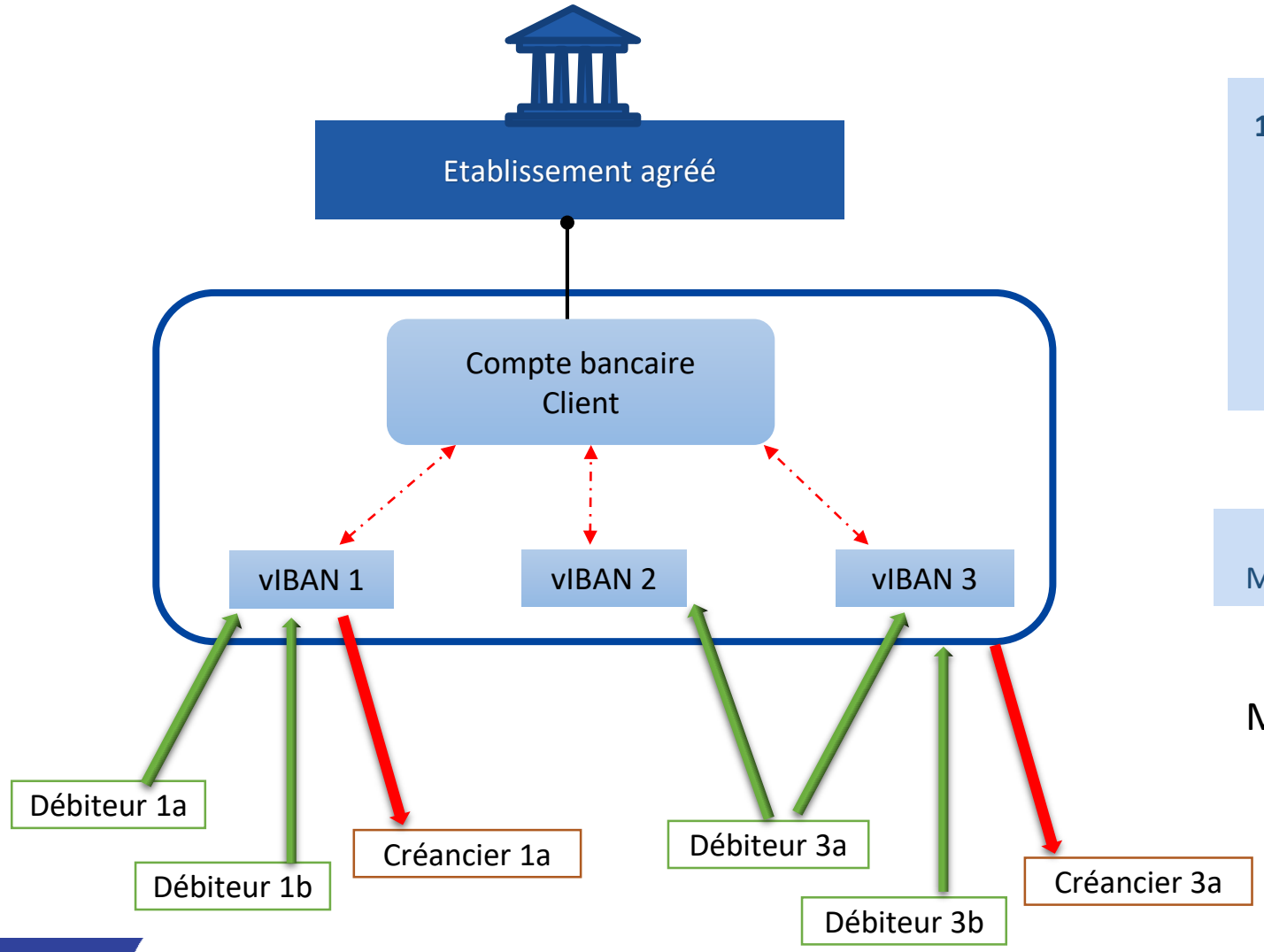
Risques limités associés à la pratique:

- Due diligence plus complexe de la part de tiers sur les transactions financières en raison de la fragmentation de l'activité financière du client entre plusieurs identifiants de compte

Recommandations:

- Proposer plusieurs vIBAN ou comptes uniquement aux entreprises ayant une justification économique claire, dans des scénarios à faible risque.
- L'utilisation d'identifiants d'entité dans les messages de paiement pourrait également constituer un facteur atténuant à l'avenir (entrée en vigueur de TFR révisé fin 2024).

CAS D'USAGE N°2 - GESTION ANALYTIQUE DES FLUX



1 vIBAN = 1 catégorie d'opérations /activité…
Équivalent d'un sous-compte

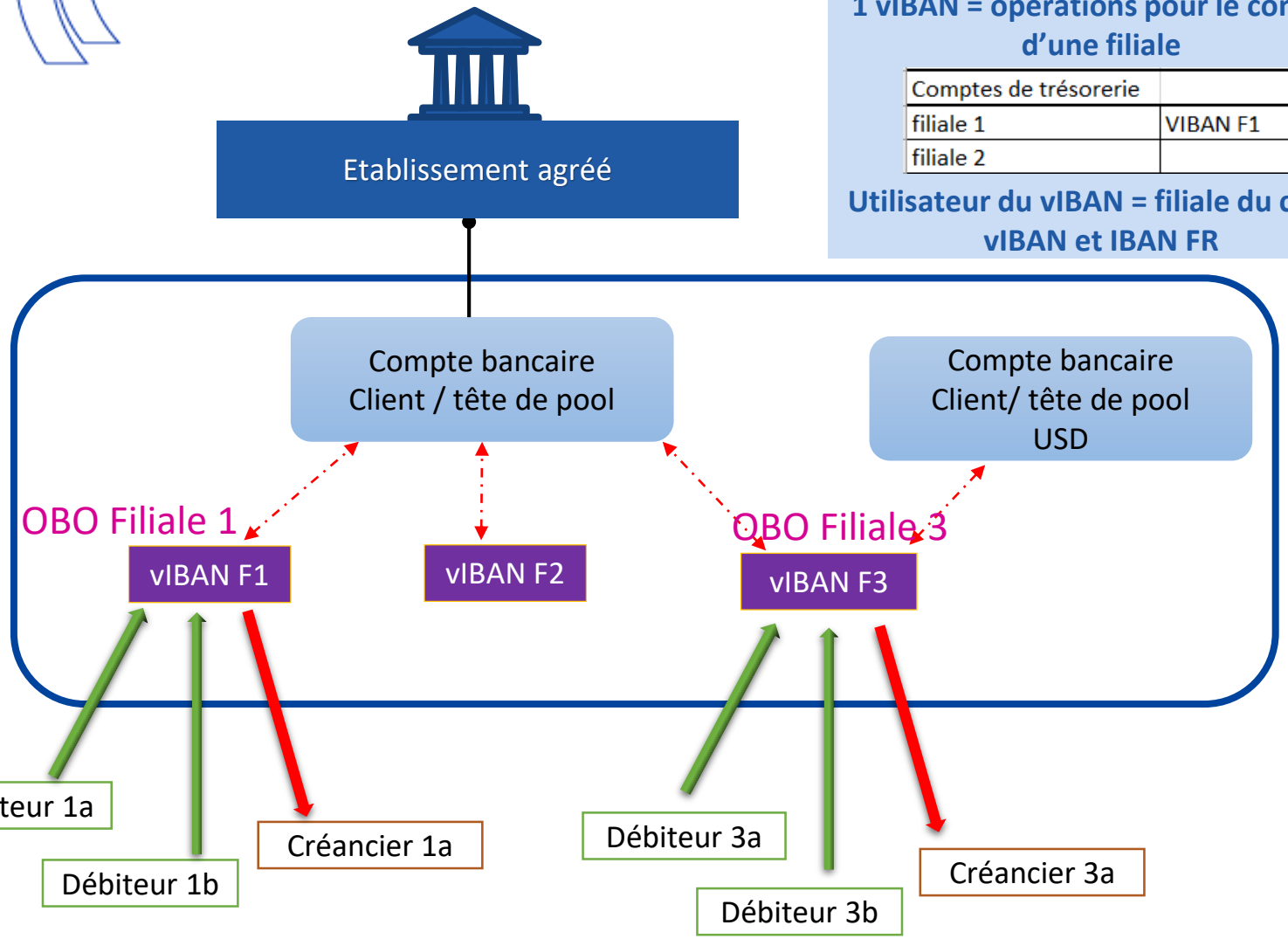
Comptabilité analytique	
branche d'activité 1	VIBAN 1
branche d'activité 2	

Titulaire vIBAN = titulaire compte principal
vIBAN et IBAN FR

Point d'attention :
Multiples comptes maitres pour 1 VIBAN (par devise)

Même analyse des risques que le cas n°1

CAS D'USAGE N°3 - CENTRALISATION DE TRÉSORERIE



1 vIBAN = opérations pour le compte d'une filiale

Comptes de trésorerie	
filiale 1	VIBAN F1
filiale 2	

Utilisateur du vIBAN = filiale du client vIBAN et IBAN FR

Risques modérés:

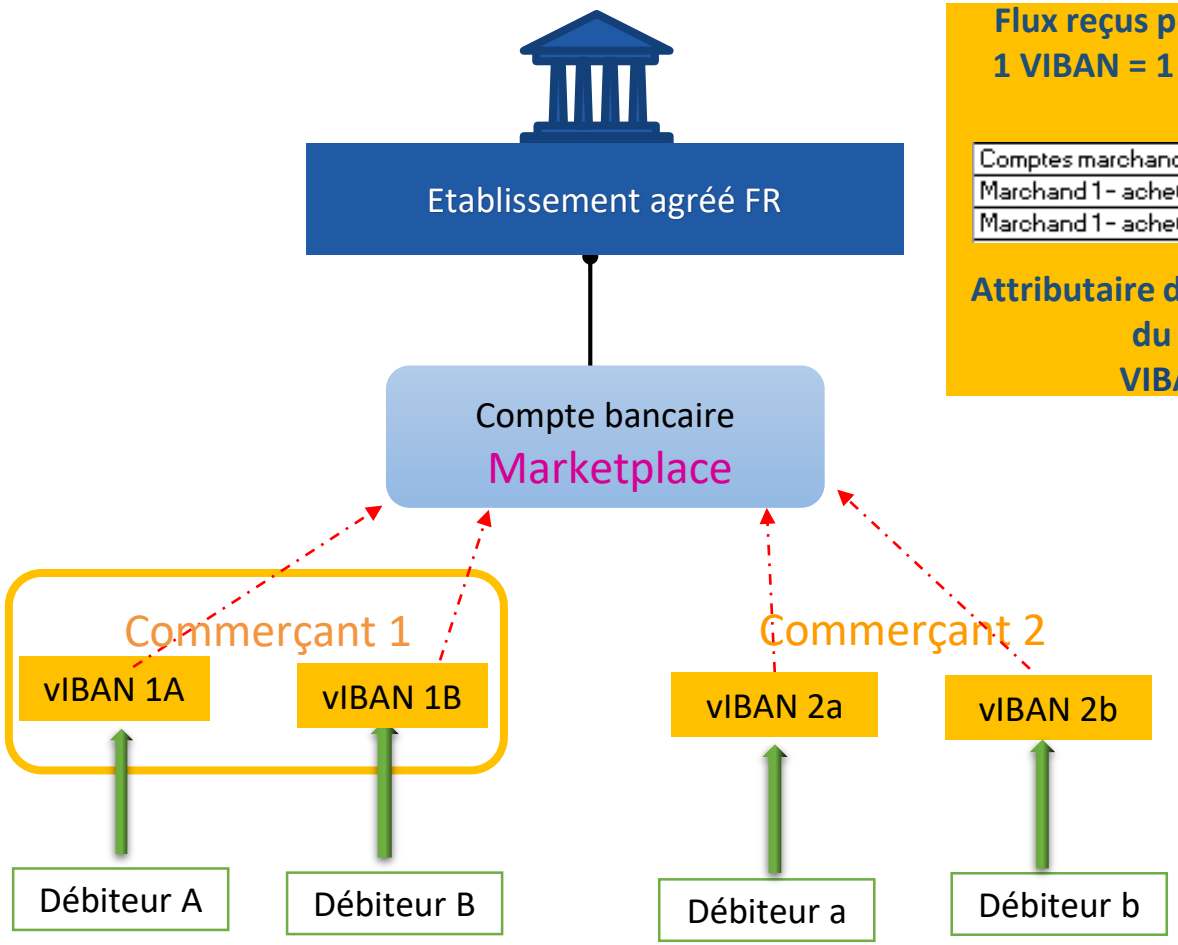
- Collecte KYC insuffisante par l'institution émettrice du vIBAN.
- Délits comptables ou délits fiscaux possibles en cas de mauvaise affectation des fonds dans la comptabilité de la filiale
- Le titulaire du Compte Maître vIBAN pourrait être qualifié d'institution financière non autorisée

Recommandations:

- Utilisation des vIBAN réservée aux groupes d'entreprises; respect des règles en matière de centralisation de trésorerie
- Vérification des liens capitalistiques et de la réalité du groupe d'entreprises
- Collecte du KYC des filiales

Point d'attention :
Risque lié à l'attribution des flux (filiale ou mère)

CAS D'USAGE N°4 - RÉCONCILIATION DE FLUX POUR COMPTE DE TIERS / CASCADE



Flux reçus pour le compte de tiers
1 VIBAN = 1 contrepartie du client final

Comptes marchands	
Marchand 1 - acheteur a	VIBAN 1a
Marchand 1 - acheteur b	VIBAN 1b

Attributaire du VIBAN = contrepartie du client du PSP
VIBAN et IBAN FR

Risques élevés:

- Les utilisateurs d'IBAN virtuels n'ont aucune relation commerciale avec l'institution émettrice des vIBAN.
- Peut permettre une activité de collecte d'argent pour le compte de tiers sans aucune autorisation
- Absence de collecte KYC par l'institution émettrice du vIBAN
- Obscurcissement de l'identité de l'utilisateur réel du compte
- Les due diligences peuvent être effectuées sur les flux globaux enregistrés sur le compte principal et non utilisateur par utilisateur

Recommandations:

- Qualification de compte de paiement, déclaré au registre des comptes bancaires comme compte complet OU
- Interdiction de distribuer des vIBAN comme comptes de paiement et utilisation des vIBAN restreinte à la collecte de flux avec KYC sur les utilisateurs effectifs des vIBAN (cf paquet AML6)
- vIBAN fournis aux agents autorisés uniquement

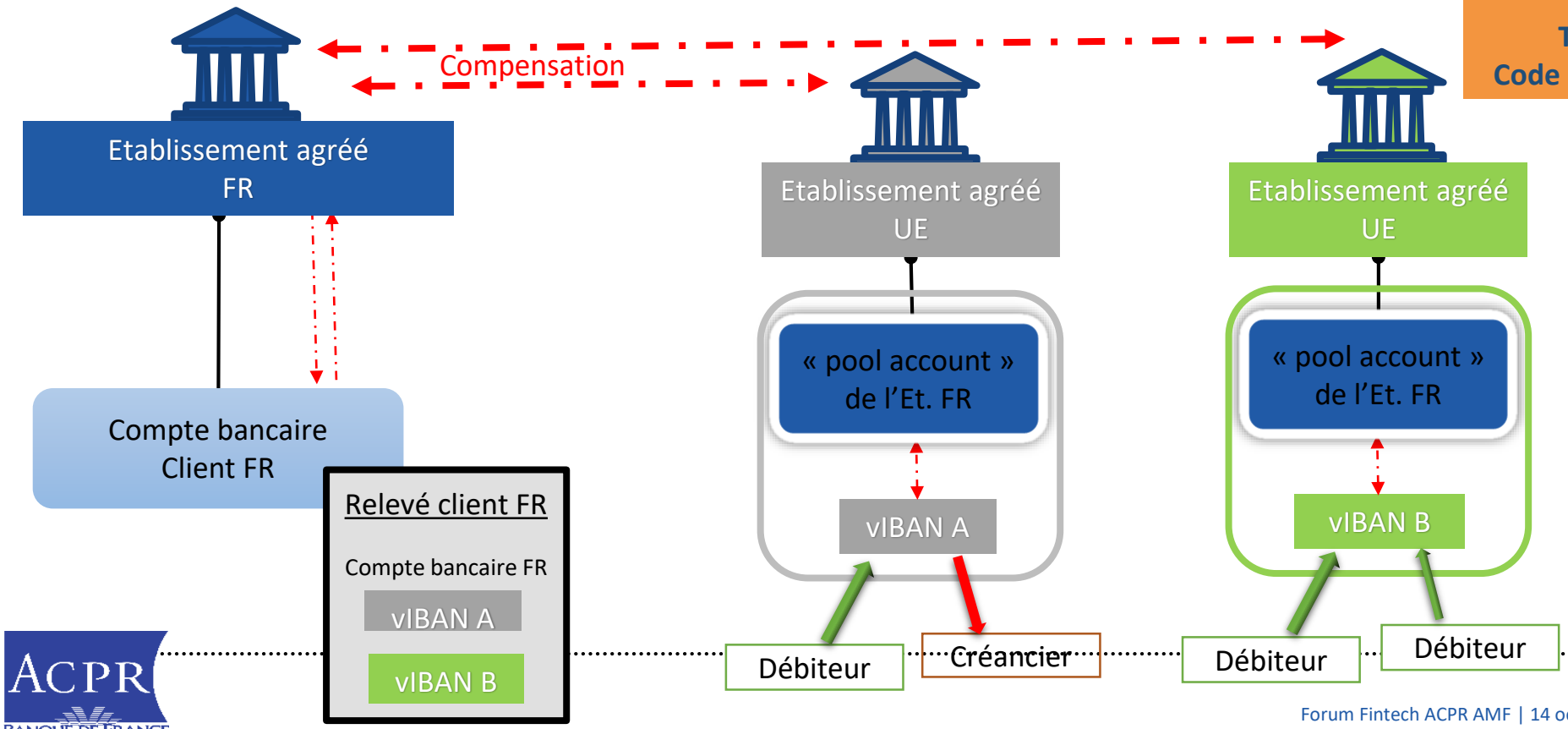
Points d'attention :
- Encaissement de fonds pour compte de tiers
- Pas de relation d'affaires directe/ bénéficiaire des flux

CAS D'USAGE N°5 - SERVICES IMPLIQUANT UN VIBAN ETRANGER ASSOCIE A UN COMPTE FR

1er CAS / FOURNITURE d'identifiant UE

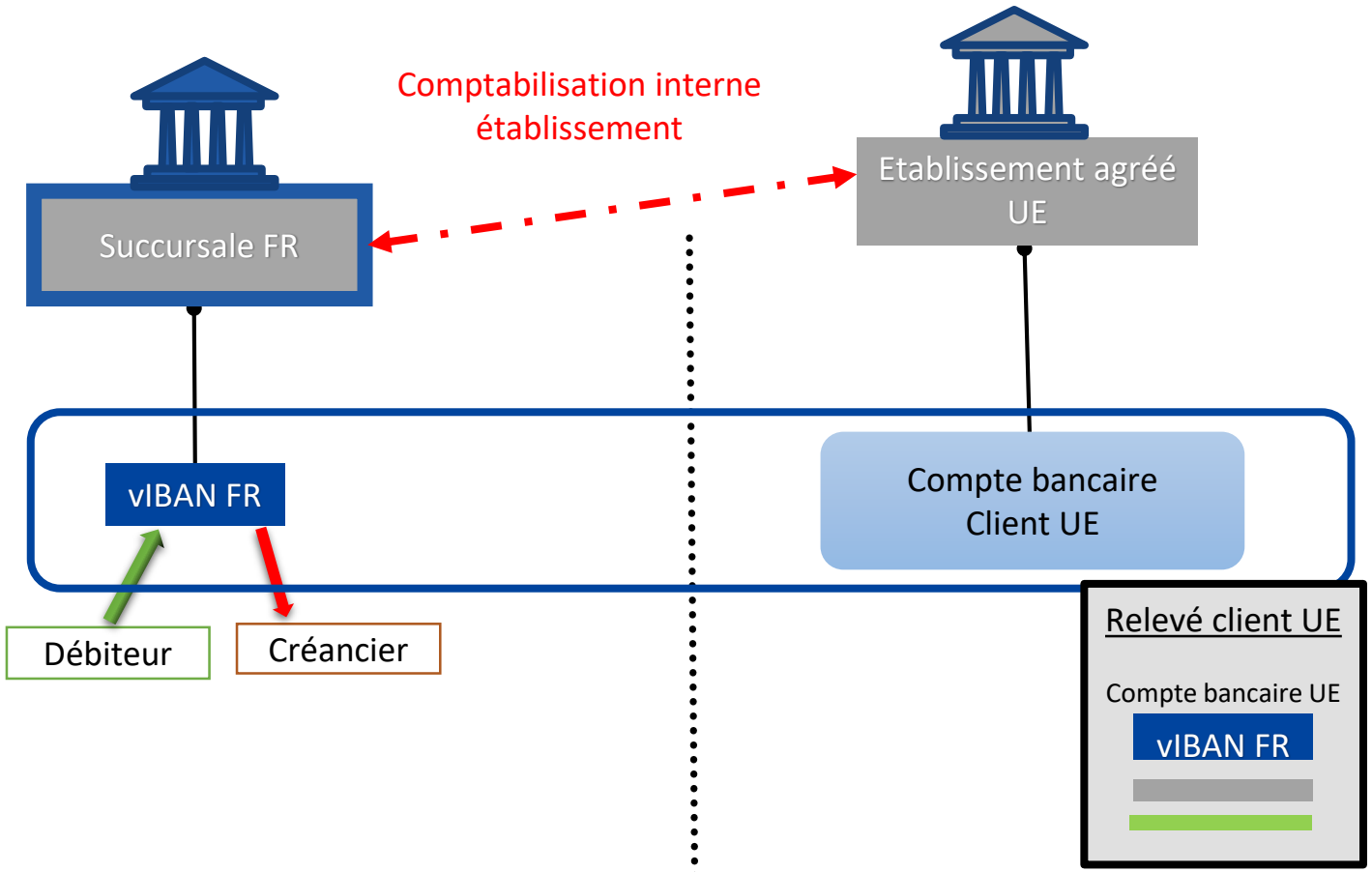
Client FR	
opérations France (EUR)	IBAN FR
opérations / pays A (devise A)	vIBAN A
opérations / pays B (devise B)	vIBAN B

Titulaire vIBAN = établissement FR
Code pays différent COMPTE CLIENT / vIBAN



Analyse de risque: voir cas 5bis

CAS D'USAGE N°5BIS - SERVICES IMPLIQUANT UN VIBAN FR ASSOCIÉ À UN COMPTE ÉTRANGER



Risques très élevés associés à la pratique, qui paraît illicite:

- affecte la bonne évaluation des risques géographiques par des tiers
- mise en œuvre incorrecte de sanctions financières ciblées par l'institution financière émettrice et les institutions tierces ;
- Induit en erreur les CRF et les forces de l'ordre : demandes envoyées au mauvais pays.
- Affecte l'application de nombreuses législation de l'UE reposant sur le code pays de l'IBAN, notamment le recouvrement des créances, les procédures d'insolvabilité et le système CESOP de lutte contre la fraude à la TVA.
- Risque de confusion des consommateurs sur la mise en place de systèmes d'assurance des dépôts (perception de plusieurs comptes auprès de plusieurs établissements, chacun éligible au plafond, alors qu'en réalité le client ne possède qu'un seul compte)

Recommandations:

- Utilisation de comptes réels avec transfert automatique (sweep accounts), lorsqu'il existe une justification économique établie et avec un suivi adéquat compte tenu du niveau de risque élevé ;
- Limitation du nombre de comptes fournis à chaque client
- Les codes de pays doivent refléter le pays où se trouve le compte. Un compte avec un IBAN français doit être géré sous la responsabilité de l'entité française, les avoirs des clients doivent être reflétées dans les comptes de l'entité française et peuvent y être saisies ; L'entité applique les lois et réglementations françaises en matière de LBC/FT ainsi que le régime de gel des avoirs, déclare à la CRF française. Vue consolidée des comptes associés dans toutes les entités

CONCLUSION SUR LES IBAN VIRTUELS

Certaines clarifications ont été introduites au niveau de l'UE :

- Le **règlement 2024/1624** relatif à la prévention de l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme, applicable à compter du 10 juillet 2027, **définit « l'IBAN virtuel »** comme «un identifiant qui a pour effet de **rediriger les paiements** vers un compte de paiement identifié par un IBAN différent de cet identifiant» (art. 2).

- L'article 22 de ce règlement précise que «Les établissements de crédit et les établissements financiers obtiennent des informations pour **identifier et vérifier l'identité des personnes physiques ou morales utilisant tout IBAN virtuel** qu'ils émettent, ainsi que le compte bancaire ou de paiement associé ».

- L'établissement de crédit ou l'établissement financier gérant le compte bancaire ou de paiement vers lequel un IBAN virtuel, émis par un autre établissement de crédit ou établissement financier, redirige des paiements, veille à pouvoir obtenir de l'établissement émettant l'IBAN virtuel les informations permettant d'identifier et de vérifier l'identité de la personne physique utilisant cet IBAN virtuel sans retard et, en tout état de cause, dans un délai de cinq jours ouvrables à compter de sa demande d'informations.

- Par ailleurs, l'article 16 de la directive 2024/1640, qui doit être transposée en droit national d'ici le 10 juillet 2027, exige que les **IBAN virtuels soient inscrits dans les registres des comptes bancaires**, y compris « le numéro IBAN virtuel, l'identifiant unique du compte vers lequel les paiements adressés à l'IBAN virtuel sont automatiquement réacheminés et les dates d'ouverture et de clôture du compte». Le texte précise en outre que «Dans le cas d'un IBAN virtuel, le titulaire de compte client visé au premier alinéa, point a), est le titulaire du compte vers lequel les paiements adressés à l'IBAN virtuel sont automatiquement réacheminés. »

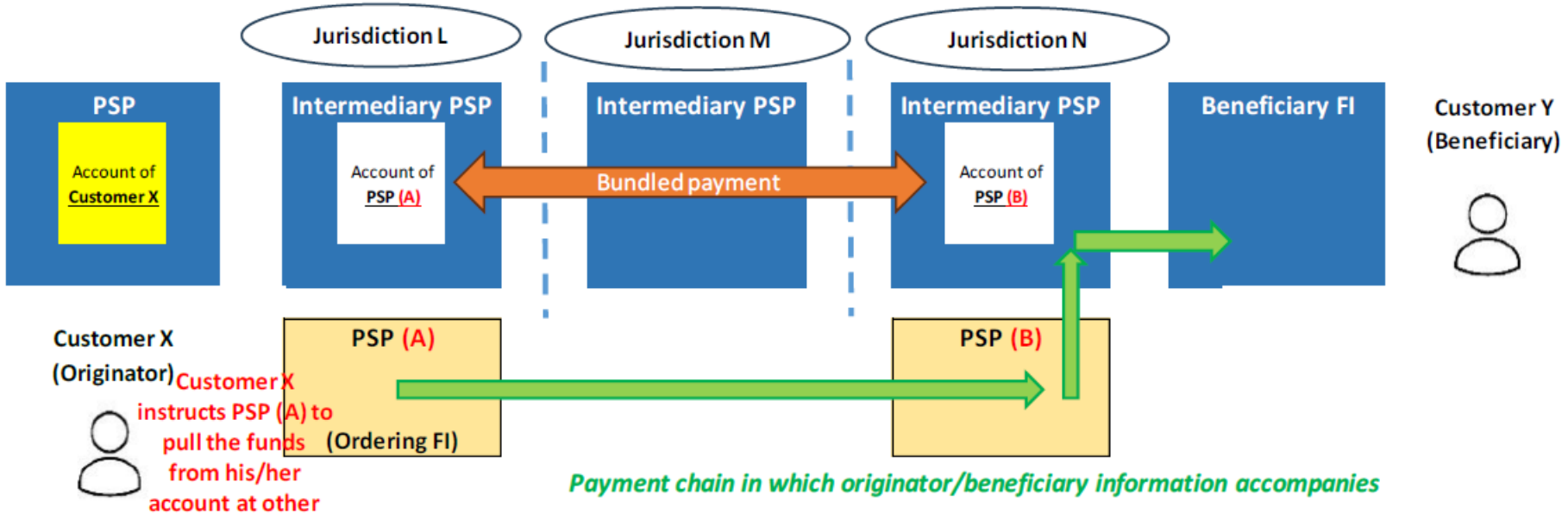
L'ABE a publié un rapport sur le sujet en mai 2024, qui souligne les risques associés

L'ACPR devrait publier son rapport fin 2024

RECOMMANDATION 16 DU GAFI SUR LA TRANSPARENCE DES PAIEMENTS

La révision en cours a donné lieu à une première consultation publique, concernant trois thèmes principaux:

- La **définition de la chaîne de paiement et la question de la compensation nette** (cf graphique ci-dessous): les flèches en vert représentent une chaîne de paiement unique, et le PSP bénéficiaire doit donc recevoir un message montrant que le client X est le donneur d'ordre)
- **Le contenu des informations sur les donneurs d'ordre et les bénéficiaires**: on se dirige vers une exigence plus systématique de l'adresse, et pour les personnes morales, d'identifiants uniques (LEI, SIREN, …)
- **L'adaptation aux modifications du marché**, notamment concernant la carte de paiement et les paiements instantanés: clarification de l'exception dont bénéficie les cartes, notamment s'agissant des retraits d'espèces transfrontaliers, et de son champ (paiement de biens et de services). Question de l'égalité entre cartes et paiements instantanés.



II. Présentation de LUCIA

Logiciel à l'Usage du Contrôle assisté par l'Intelligence Artificielle

INTRODUCTION

Le GAFI a rappelé en 2021* que l'IA présente un potentiel substantiel pour améliorer les performances des dispositifs de LCB-FT. L'utilisation de l'IA (*machine learning*, *natural language processing*) peut contribuer à améliorer les processus d'onboarding, de KYC et de surveillance des transactions (vigilance constante).

→ Le recours à l'IA dans le domaine de la LCB-FT est en développement tant au niveau des établissements assujettis que des autorités de supervision.

Au niveau des établissements assujettis, les cas d'usage concernent principalement :**

- La caractérisation des profils de transaction des clients
- la priorisation et l'optimisation de la gestion du flux d'alertes y compris via des fonctionnalités de réplication des décisions
- l'analyse de graphes favorisant le traitement d'une alerte

L'usage le plus fréquent reste la priorisation des alertes au moyen d'algorithmes de *machine learning* (objectif d'élimination des alertes présentant une faible probabilité d'escalade en examen renforcé).

Depuis 2019, l'ACPR s'est engagée dans une démarche dite SUPTECH dont l'objectif est d'augmenter ses capacités de supervision grâce aux nouvelles technologies. Cette démarche s'inscrit dans le plan stratégique de la Banque de France.

** Document FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021)*

*** Revue thématique de l'ACPR sur les dispositifs automatisés de surveillance des opérations en matière de LCB-FT (Avril 2023)*

LUCIA : UN OUTIL SUPTECH

LOGICIEL À L'USAGE DU CONTRÔLE ASSISTÉ PAR L'INTELLIGENCE ARTIFICIELLE

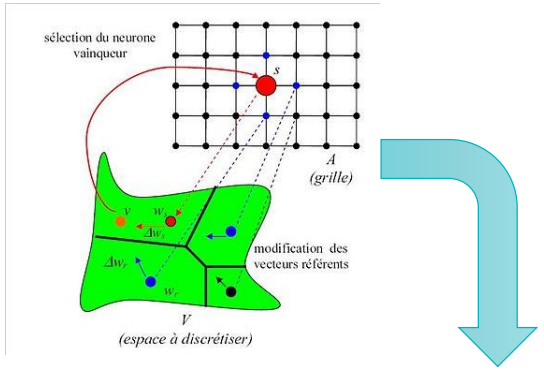
LUCIA est construit sur un réseau de neurones artificiels qui :

restitue visuellement les informations sous la forme d'une cartographie intelligente (carte auto-adaptative* également appelée carte de Kohonen) en regroupant automatiquement les clients par profils de risque

met en œuvre des algorithmes d'exploration de données (data mining) pour extraire des signaux faibles de risque des opérations et des données de connaissance clientèle

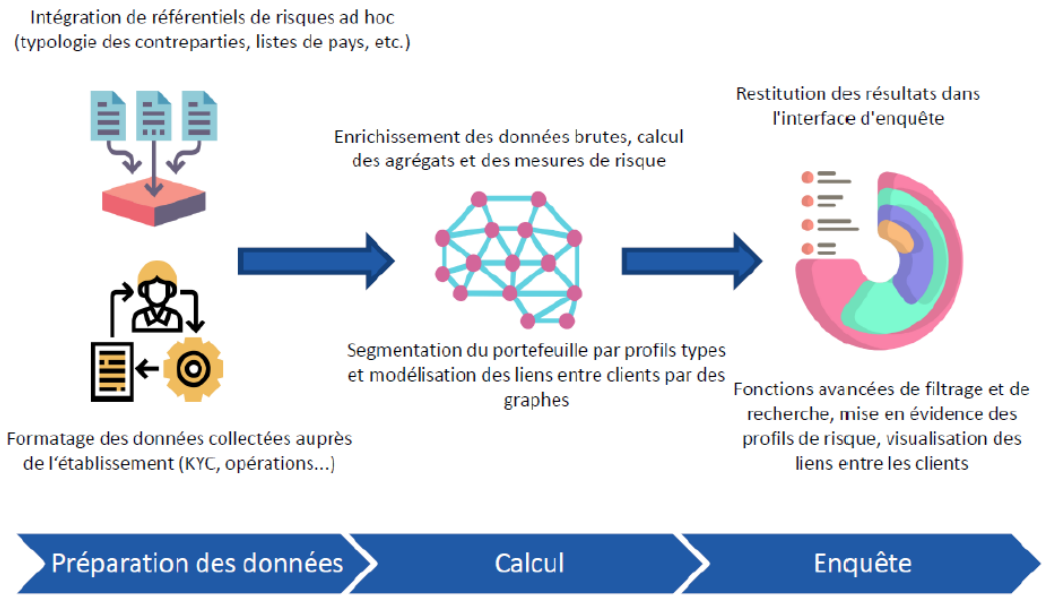
permet d'investiguer des dossiers individuels en mettant en évidence les profils de risque et les informations à valeur ajoutée identifiées via des techniques de traitement du langage naturel (NLP)

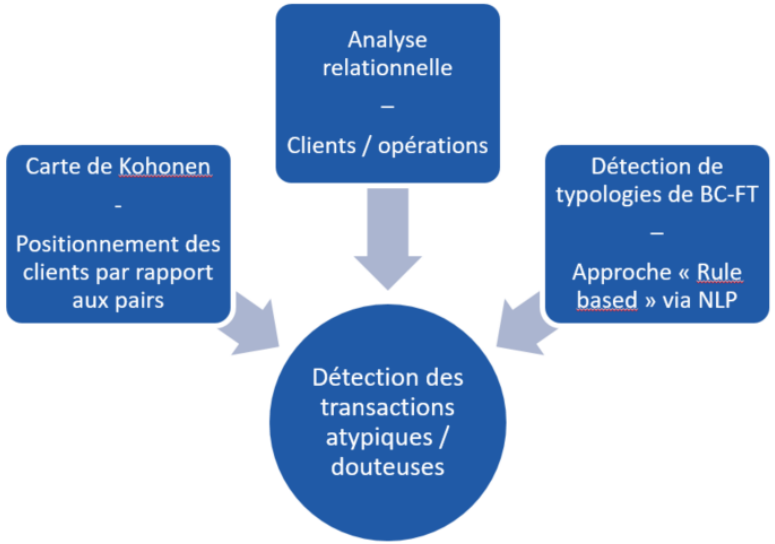
facilite l'analyse de l'environnement du client avec des modèles de graphes relationnels



LUCIA : UN OUTIL SUPTECH

LOGICIEL À L'USAGE DU CONTRÔLE ASSISTÉ PAR L'INTELLIGENCE ARTIFICIELLE





LUCIA : UN OUTIL SUPTECH

LOGICIEL À L'USAGE DU CONTRÔLE ASSISTÉ PAR L'INTELLIGENCE ARTIFICIELLE

La démarche de contrôle repose sur l'exploitation :

des données communiquées par l'établissement à la demande de l'Inspection de l'ACPR (cahier des charges adressé en général plusieurs semaines avant le début des investigations sur place)

La mission d'Inspection de l'ACPR réalise des contrôles sur l'exhaustivité et la qualité des données communiquées (données censées être utilisées par l'établissement contrôlé pour son propre dispositif de surveillance)

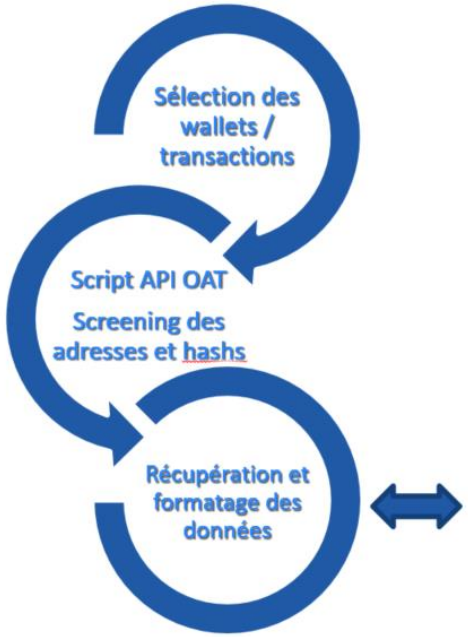
de référentiels de données choisis par l'Inspection, selon une approche par les risques, à partir de sources de données publiques

API Pappers	• Récupération des informations KYC des clients PM et leurs bénéficiaires effectifs (contrôle données) • Identification de l'écosystème des clients PM : sociétés "mère/soeurs" liées à l'entreprise cliente via un BE / dirigeant → identification des transactions intragroupe + « écosystème à risque » (cf. slide suivant)
Registre national des élus	• Criblage des bases clients / tiers de l'établissement pour identifier les élus (y/c < PPE) et leur attribuer un flag « élu » (facteur de risque) • Analyse des transactions pour identifier les opérations impliquant des élus (atteintes à la probité)
ZSP	• Analyse des adresses des clients et localisation géographique par rapport aux ZSP • Attribution d'un flag "ZSP" aux clients (facteur de risque)
Offshore Leaks	• Criblage des bases clients / tiers de l'établissement pour identifier les personnes physiques impliquées et leur attribuer un flag « Offshore Leaks » (facteur de risque) • Récupération du référentiel des personnes morales liées aux PP pour identification dans les transactions
Délégataires CEE | OPCO (CPF)	• Prise en compte de la liste des délégataires CEE P5 / Liste des OPCO (CPF) • Identification des transactions impliquant les clients PM de l'établissement et des contreparties « délégataires » + autres critères de risque (par ex : secteur d'activité client, flux vers l'étranger)
Listes noires AMF	• Identification des transactions vers/depuis contreparties "liste noire AMF"
Répertoire national des associations	• Identification et caractérisation des associations dans les transactions (par exemple avec focus partis politiques / associations religieuses, etc.)

Évaluation risques pays	• Listes grise et noire du GAFI • Listes UE des pays tiers à haut risque / pays et territoires non coopératifs à des fins fiscales • Liste FR des États et territoires non coopératifs en matière fiscale
Référentiels de contreparties	• Plateformes de crowdfunding platforms, prestataires cryptoactifs, établissements de monnaie électronique, transmission de fonds, centres pénitentiaires, etc. • Autres types d'entités : casinos, associations, partis politiques, etc.
Mots-clés	• Avance, aide familiale, cadeau, donation, héritage, note de frais, remboursement, trusts, fiducie, etc. • Advance, family support, gift, inheritance, legacy, miscellaneous, property, reimbursement, trusts, etc.

LUCIA : UN OUTIL SUPTECH

LOGICIEL À L'USAGE DU CONTRÔLE ASSISTÉ PAR L'INTELLIGENCE ARTIFICIELLE



Addressed linked	Risk category
12JMHjoKu4JoKKTcZrovPKStfE4kaYakbB (BTC)	Dark
12evi7xCWoLcCSUZb9EWAawBw6jmVr38DP (BTC)	Dark
0x01Db4F50EB9C1aD22e8F4b41cCcB2FEc6e22dEfF (ETC)	Casino
0x01Db4F50EB9C1aD22e8F4b41cCcB2FEc6e22dEfF (ETH)	Casino
123mhnrko8iAqN9zHFRgdifUSTYUmi5eVN (BTC)	Casino
12Aknn8qtVnNXYXqtpkGhX7TycqDUUPGXG (BTC)	Casino
0x4ad8d9cf9424b477e77a0d7c339c4de792b92fc6 (USDC)	Casino
0x974caa59e49682cda0ad2bbe82983419a2ecc400 (BUSD)	Casino
0x6A5f57603B02126674cdbdD6882540F58D79db34 (ETH)	Child abuse material
17KuGn3gfNW9fxsJLw3VmBLmd2raNHcPBQ (BTC)	Child abuse material
0x072f3252d0eb025fbd30ec43181ae6cea8566004 (ETH)	Sanction
0x4BFF1e6f00450aee0a4FFC8A661B50030d079Fae (BUSD)	Sanction
0x9b322e68bee8f7d6c1c4d32083e9fe159a36aab1 (USDC)	Sanction
1A6J5TGdG4QT3DtuBqedEYZNGwYtZNCAu9 (BTC)	Sanction
0x362b1A3d404F8455813dA218339765D6600e0c48 (BUSD)	Scam
0x3801ADe522e90b8AABb2a2916Dc49595B6Ed67C9 (ETH)	Scam
...	...
...	...
...	...

L'interfaçage entre LUCIA et un OAT permet d'identifier les clients et transactions à risque lors du contrôle d'un PSAN

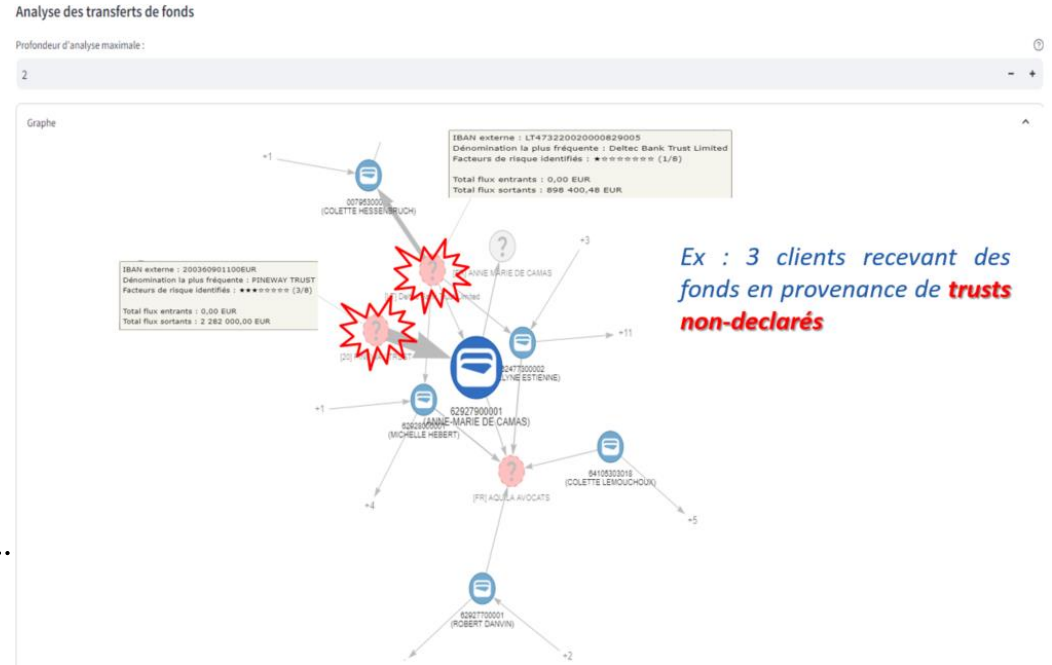
- **L'appel à l'API d'un OAT permet de récupérer les facteurs de risque associés aux wallets et transactions afin de les intégrer dans les référentiels de données utilisés dans le cadre du contrôle**
- **Possibilité de prendre en compte simultanément les données de connaissance clientèle, les transactions fiat, off-chain et on-chain pour identifier les cas à investiguer**

IDENTIFICATION DE TYPOLOGIES DE BC-FT

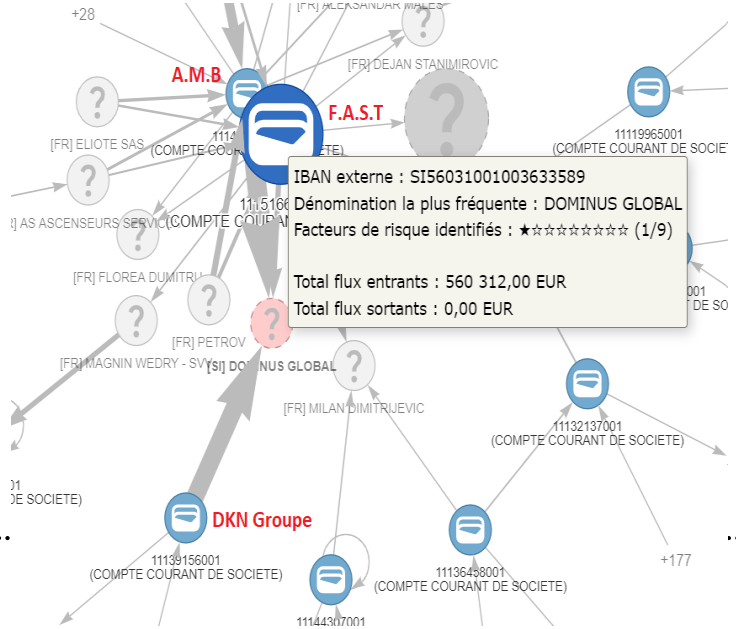
L'identification de typologies de BC-FT est un axe de développement permettant notamment de capitaliser sur les traitements IA embarqués dans l'outil.

➢L'objectif est de mettre en œuvre des méthodes de détection correspondant aux priorités de contrôle définies par les autorités et aux cas typologiques définis notamment par TRACFIN.

➢L'approche par les risques mise en œuvre se fonde en particulier sur les résultats de l'Analyse sectorielle des risques de l'ACPR.

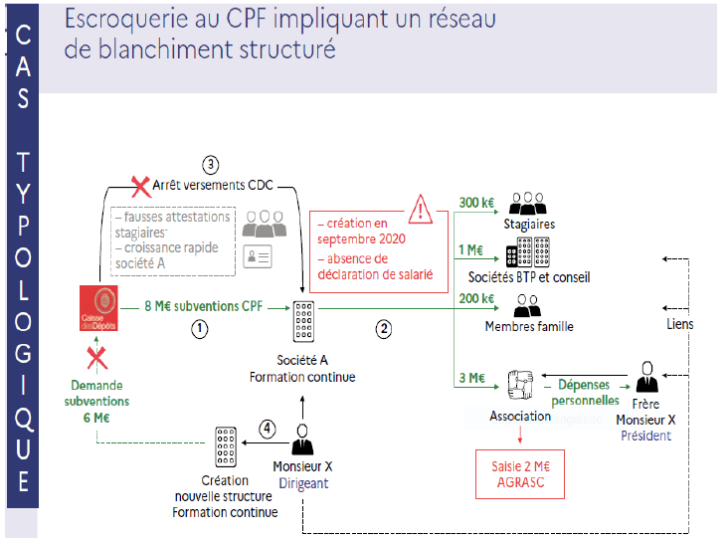


*Ex : 3 clients PM du secteur de la construction envoyant des fonds vers une contrepartie en Slovénie (**société taxi**)*



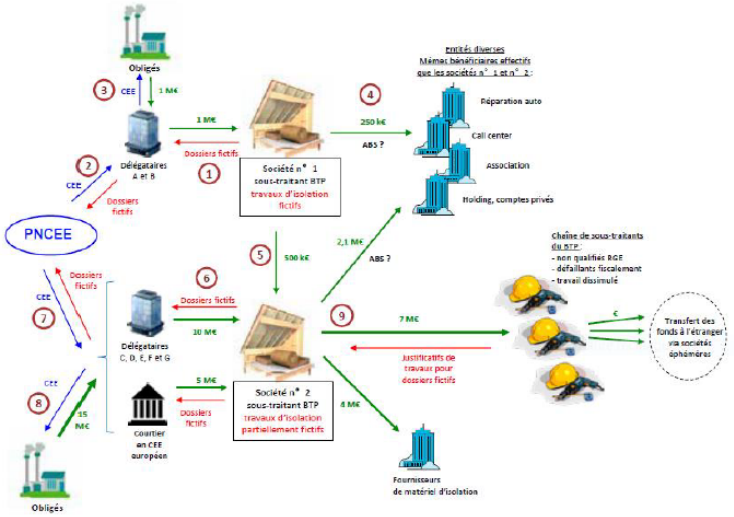
IDENTIFICATION DE TYPOLOGIES DE BC-FT

Blanchiment de fraude aux CEE via les chaînes de sous-traitants utilisés par les sociétés délégataires



- **Mise en œuvre** : identifier les clients personnes morales ayant reçu des virements créditeurs en provenance des opérateurs de compétences (OPCO) dans le cadre des dispositifs de CPF. L'identification des opérations est réalisée à partir de LUCIA, en intégrant dans le référentiel de données la liste des OPCO afin de les identifier parmi les contreparties des clients.

Blanchiment de fraude aux CEE via les chaînes de sous-traitants utilisés par les sociétés délégataires



- **Mise en œuvre** : identifier les clients personnes morales ayant reçu des virements créditeurs en provenance des délégataires d'obligations d'économie d'énergie des périodes P4 et P5 dans le cadre des dispositifs de certificats d'économie d'énergie (CEE). L'identification des opérations a été réalisée à partir de l'outil LUCIA, en intégrant dans le référentiel de données la liste des délégataires P4 et P5, afin de les identifier parmi les contreparties des clients.

III. Orientations « TFR »

Exigences en matière d'information concernant les transferts de fonds et certains transferts de crypto-actifs au titre du règlement (UE) 2023/1113 (EBA/GL/2024/11)

ORIENTATIONS TFR (ASPECTS CRYPTO)

Contexte

- Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs - ***TFR2*** (JOUE – 9/6/2023)
  - Refonte du règlement (UE) 2015/847 (***TFR***), appliquant en UE les exigences GAFI (obligation d'accompagner les transferts de fonds d'informations sur le donneur d'ordre et le bénéficiaire)
  - Juin 2019 : les normes GAFI prévoient des obligations similaires pour les prestataires de services sur actifs virtuels, afin de faciliter la traçabilité des transferts d'actifs virtuels (recommandation 15 et note interprétative, §7 b) – Lignes directrices PSAV)
  - **TFR2 : élargissement aux transferts d'actifs virtuels** (recours aux définitions MiCA de crypto-actifs, services sur crypto-actifs, prestataires de services sur crypto-actifs (***PSCA*** ou ***CASP***, en ligne avec les notions GAFI)
  - **Objectif** : assurer la transmission des informations tout au long de la chaîne de transfert de crypto-actifs
  - Entrée en application de TFR2 : **31 décembre 2024** (cf. MiCA)

ORIENTATIONS TFR (ASPECTS CRYPTO)

TFR2 – Principaux apports

- Règles relatives aux informations sur les initiateurs/bénéficiaires accompagnant les transferts de crypto-actifs et aux politiques, procédures et contrôles internes visant à garantir la mise en œuvre de mesures restrictives
- Modifie AMLD (Directive 2015/849) : inclut les catégories de CASP définies dans MiCA dans la catégorie des établissements financiers assujettis aux fins de la directive AMLD
- Transposition « négative » : habilitation loi « DDADUE » n° 2024-364 du 22 avril 2024 - *Ordonnance en cours d'examen au Conseil d'Etat*
- TFR2 ne s'applique notamment pas aux transferts de crypto-actifs si:
  - Expéditeur et bénéficiaire tous deux CASP agissant pour propre compte ; ou
  - Transfert entre particuliers sans implication d'un CASP

TFR2 – Principales dispositions

Obligations du CASP de l'initiateur

- Veiller que tous les transferts soient accompagnés d'informations relatives à l'initiateur et au bénéficiaire, tels que :
  - Noms ; adresses de registre distribué ou numéro de compte de crypto-actifs des initiateurs et bénéficiaires ou à défaut identifiant de transaction unique
  - Adresse, nom du pays, numéro du document d'identité officiel, numéro d'identification client de l'initiateur
  - Identifiant d'entité juridique –***IEJ***- de l'initiateur et du bénéficiaire (si fournis par l'initiateur à son CASP et existence du champ dans le format de message nécessaire, ou autre identifiant officiel équivalent disponible)
- Communiquer les informations « *avant le transfert de crypto-actifs, parallèlement à celui-ci ou en même temps que celui-ci, de manière sécurisée et conformément au règlement (UE) 2016/679* [RGPD] »
- Avant transfert, vérifier l'exactitude des informations reçues sur la base de documents, de données ou de renseignements obtenus auprès d'une source fiable et indépendante
- Vérifier si une adresse auto-hébergée est détenue ou contrôlée par l'initiateur pour tous les transferts supérieurs à 1 000€

ORIENTATIONS TFR (ASPECTS CRYPTO)

TFR2 – Principales dispositions

Obligations du CASP du bénéficiaire
▪ Vérifier que les informations sur l'initiateur et le bénéficiaire accompagnent, ou suivent, le transfert de crypto-actifs ▪ Assurer que le transfert des crypto-actifs à partir d'une adresse auto-hébergée puisse être identifié individuellement ▪ Evaluer, pour tous les transferts de plus de 1 000€ à partir d'une adresse auto-hébergée, que le bénéficiaire possède ou contrôle cette adresse ▪ Vérifier l'exactitude des informations sur le bénéficiaire avant remise des crypto-actifs ▪ Décider d'effectuer, de rejeter, de renvoyer ou de suspendre un transfert de crypto-actifs qui n'est pas accompagné des informations requises et prendre les mesures de suivi qui s'imposent ▪ Peut rejeter ou renvoyer les crypto-actifs ou demander des détails supplémentaires si les informations sont manquantes ou incomplètes ▪ Avertir un CASP s'il ne fournit pas de manière répétée les informations requises avant de rejeter les transferts de cette source, de restreindre ou de résilier leur relation commerciale, et d'informer l'autorité compétente LBC/FT ▪ Tenir compte des informations manquantes pour évaluer si un transfert est suspect et doit être signalé à la cellule de renseignement financier

ORIENTATIONS TFR (ASPECTS CRYPTO)

TFR2 – Principales dispositions

Obligations communes aux CASP de l'initiateur et du bénéficiaire

- Mettre en place des politiques, procédures et contrôles internes pour garantir l'application des règles européennes et nationales lors du transfert de crypto-actifs
- Donner suite, de manière exhaustive et sans tarder, aux demandes de renseignements de l'autorité compétence en matière LCB/FT concernant les informations requises en vertu de TFR2
- Conserver les informations relatives à l'initiateur et au bénéficiaire pendant cinq ans (délai supplémentaire de cinq ans, sur option nationale)

Obligations des CASP intermédiaires (CASP-I)

- En cas d'absence d'informations, veiller à ce que toutes les informations de l'initiateur et du bénéficiaire soient transmises avec le transfert et que les informations soient conservées et mises à disposition sur demande

ORIENTATIONS TFR (ASPECTS CRYPTO)

Fondement et objet des Orientations TFR

TFR2 (article 36, 1er alinéa)

- L'EBA émet des orientations à l'intention des autorités compétentes et des CASP sur les mesures à prendre en ce qui concerne la mise en œuvre des obligations TFR applicables aux CASP de l'initiateur et du bénéficiaire et des CASP intermédiaires

AMLD (Directive (UE) 2015/849, art. 19 bis (2))

- L'EBA précise les mesures relatives à l'identification et à l'évaluation des risques de BC/FT liés aux transferts de crypto-actifs effectués vers ou depuis une adresse auto-hébergée

Les Orientations TFR ont ainsi pour objet de :

- Définir les facteurs à prendre en pour la mise en place de procédures visant à détecter/gérer les transferts de crypto-actifs qui ne contiennent pas les informations requises, et pour garantir l'efficacité de ces procédures
- Préciser les mesures de gestion des risques BC/FT lorsque les informations requises sont manquantes ou incomplètes

ORIENTATIONS TFR (ASPECTS CRYPTO)

Contenu des Orientations

1.	Dispositions générales
2.	Exclusion du champ d'application du règlement (UE) 2023/1113 et dérogations
3.	Transmission et réception d'informations lors du transfert
4.	Informations à transmettre lors du transfert
5.	Détection d'informations manquantes
6.	Transferts pour lesquels des informations sont manquantes ou incomplètes
7.	Omissions répétées
8.	Transferts effectués vers ou depuis une adresse auto-hébergée

ORIENTATIONS TFR (ASPECTS CRYPTO)

1. Dispositions générales

- Pour déterminer quelles informations doivent accompagner un transfert et quelles mesures doivent être prises pour se conformer à TFR2, les politiques et procédures doivent indiquer le statut choisi pour chaque transfert (selon que le CASP agit comme CASP de l'initiateur, du bénéficiaire ou CASP-I)
- Les politiques et procédures mises en place doivent être/demeurer efficaces : pour cela, nécessité de tester « *un échantillon aléatoire de tous les transferts traités* »
- Tenir les politiques et procédures à jour et les améliorer s'il y a lieu

2. Exclusion du champ d'application et dérogations

- Politiques et procédures devraient préciser comment déterminer si les conditions d'application des exclusions ou dérogations prévues par TFR2 sont remplies
- A défaut d'être en mesure d'établir que les conditions sont remplies, application de TFR2 pour tous les transferts

ORIENTATIONS TFR (ASPECTS CRYPTO)

3. Transmission et réception d'informations lors du transfert

3.1 - Systèmes de messagerie

- Utiliser des infrastructures et des services techniquement capables de transmettre et de recevoir **intégralement** les informations, sans lacunes ni erreurs
  - ✓ **Par dérogation, CASP/CASP-I peuvent, jusqu'au 31 juillet 2025, utiliser à titre exceptionnel** des infrastructures/services pour lesquels des limitations techniques liées à l'exhaustivité des données sont compensées par des mesures supplémentaires, incluant d'autres mécanismes pour la collecte, la détention et la mise à la disposition des informations qui ne peuvent être transmises du fait de limitations techniques
- Veiller à ce que les systèmes puissent préserver **l'intégrité** des données – A défaut, passer à un système capable d'offrir de telles garanties
- Veiller à ce que les systèmes utilisés soient **sécurisés** (application par les CASP des orientations EBA sur la gestion des risques liés aux TIC et à la sécurité + celles relatives à l'externalisation)
- CASP/CASP-I de l'initiateur devraient transmettre les informations requises :
  - Soit dans le cadre du transfert (blockchain ou autre DLT), soit de manière indépendante (par l'intermédiaire de différents canaux de communication : communication directe entre CASP / API / « solution de code fonctionnant au-dessus » de la blockchain / autres solutions fournies par des tiers)
  - Immédiatement et au plus tard lors de l'initiation de la transaction via blockchain
- Choix des systèmes de messagerie : mesures proportionnées et fondées sur les risques pour évaluer notamment la capacité du système à communiquer avec d'autres systèmes, l'accessibilité du protocole, la manière dont le système permet au CASP/CASP-I de détecter un transfert avec informations manquantes ou incomplètes, les capacités d'intégration des données, la sécurité et la fiabilité des données

3.2 - Transferts transfrontaliers impliquant plusieurs intermédiaires

- Lorsque le CASP-I ne reçoit pas les informations requises relatives à un transfert, il devrait obtenir les informations manquantes par un autre mécanisme (notamment API et solutions fournies par des tiers)

ORIENTATIONS TFR (ASPECTS CRYPTO)

4. Informations à transmettre lors du transfert

- Les CASP ne devraient pas modifier la transmission initiale, sauf sur invitation du CASP-I /CASP du bénéficiaire, lorsqu'ils estiment que certaines des informations sont manquantes ou si à la suite du transfert, le CASP de l'initiateur détecte une erreur dans les informations transmises
- Si modification, CASP initiateur devrait informer le CASP suivant dans la chaîne de transfert et soumettre les informations correctes. Les CASP suivants dans la chaîne de transfert devraient alors effectuer, de nouveau, les tâches nécessaires pour détecter les informations manquantes ou incomplètes

4.1 – Le CASP de l'initiateur doit fournir des éléments précisément définis quant aux **noms de l'initiateur et du bénéficiaire**

- *Personnes physiques* : noms et prénoms complets du client (cf. pièce d'identité ou identification électronique conforme aux normes visées à l'article 13 AMLD) ou si, motif légitime d'indisponibilité, documents visés par les orientations EBA sur l'accès aux services financiers. Si limitations techniques et mesures dérogatoires (cf. supra): premier prénom et du dernier nom du client
- *Personnes morales* : dénomination sociale complète. Si mesures dérogatoires (cf. supra): nom commercial (permettant de remonter sans équivoque jusqu'à la personne morale et correspondant aux registres officiels)
- *Transferts à partir d'un compte/adresse/portefeuille commun* : noms de tous les titulaires du compte/adresse/ portefeuille. Si mesures dérogatoires (cf. supra): nom du titulaire ou titulaire principal du compte/adresse/ portefeuille qui initie le transfert

ORIENTATIONS TFR (ASPECTS CRYPTO)

4. Informations à transmettre lors du transfert

4.2 – Le CASP de l'initiateur doit fournir les éléments suivants quant à l'**adresse de l'initiateur:**

- *Personnes physiques* : lieu de résidence habituel (en l'absence d'adresse de résidence fixe, adresse postale à laquelle la personne physique peut être contactée)
- *Personnes morales* : adresse du siège social ou du siège officiel
- *Transferts à partir d'un compte/adresse/portefeuille commun* : informations de tous les titulaires du compte/adresse/portefeuille. Si mesures dérogatoires (cf. supra): titulaire ou titulaire principal du compte/adresse/portefeuille qui initie le transfert

Ordre de priorité : Nom complet du pays (ou abréviation cf. ISO 3166 - alpha-2 ou alpha-3) > Code postal > Ville > Etat > Province > Municipalité > Nom de la rue > Numéro du bâtiment ou nom du bâtiment

Concernant le numéro du document d'identité officiel et le numéro d'identification de client (ou, à défaut, date/lieu de naissance) : La combinaison des éléments d'information requis devrait être fondée non seulement sur leur disponibilité, mais aussi sur leur capacité à identifier au mieux l'initiateur sans ambiguïté

ORIENTATIONS TFR (ASPECTS CRYPTO)

4. Informations à transmettre lors du transfert

4.3 – Identifiant équivalent à l'identifiant d'entité juridique (IEJ) de l'initiateur et du bénéficiaire de crypto-actifs

- Conditions d'équivalence strictement définies
- Le CASP de l'initiateur ne devrait considérer comme équivalents à un LEI que les **identifiants officiels** qui :
  - Constituent des codes d'identification unique propres à l'entité juridique
  - Sont publiés dans des registres publics
  - Sont émis lors de la constitution de l'entité par une autorité publique dans la juridiction où l'entité juridique est établie
  - Permettent l'identification des éléments relatifs au nom et à l'adresse
  - Sont accompagnés d'une description du type d'identifiant utilisé dans le système de messagerie

ORIENTATIONS TFR (ASPECTS CRYPTO)

5. Détection d'informations manquantes

5.1 – Procédures de détection d'informations manquantes

- Intègrent au moins (i) étapes de détection d'informations manquantes, incomplètes et dépourvues de sens ou de caractères ou éléments non admissibles, (ii) combinaison de pratiques de surveillance pendant et après le transfert, proportionnée au risque BC/FT (cf. orientations EBA sur les facteurs de risque), (iii) critères aidant l'identification des facteurs d'augmentation des risques

5.2 – Suivi des transferts

- CASP/CASP-I bénéficiaires devraient définir la manière dont ils détermineront les transferts faisant l'objet d'un suivi pendant ou après le transfert, et au moins indiquer (i) les facteurs de risque pris en compte pour cette évaluation et (ii) quels facteurs d'augmentation des risques, ou quelle combinaison de facteurs d'augmentation des risques, déclencheront systématiquement un suivi durant le transfert, et ceux qui déclencheront un réexamen ciblé après transfert
  - Se référer aux orientations de EBA sur les facteurs de risque, aux facteurs de risque pertinents résultant de l'évaluation des risques à l'échelle de l'entreprise, à l'évaluation sectorielle ou nationale des risques, en incluant a minima certains facteurs (seuil de valeur prédéfini en tenant compte de la valeur moyenne des transferts / initiateur ou bénéficiaire situés dans des pays ou des territoires faisant l'objet de mesures restrictives ou associés à un risque BC/FT élevé …)

5.3 – Contrôles relatifs aux informations manquantes

- CASP bénéficiaire / CASP-I devraient considérer les informations comme manquantes si champs laissés vides ou informations dépourvues de signification ou incomplètes (chaînes de caractères aléatoires ou illogiques, utilisation de titres sans nom, désignations incohérentes ou incompréhensibles…)

ORIENTATIONS TFR (ASPECTS CRYPTO)

6. Transferts pour lesquels des informations sont manquantes ou incomplètes

6.1 – Procédures fondées sur les risques

- Politiques et procédures doivent définir selon quelles modalités sont décidés les rejets/suspension/transferts (énumérer les facteurs de risque pris en considération pour chaque transfert).
- Examiner, avant de décider des mesures à adopter si (i) les informations permettent de déterminer les entités visées par le transfert et (ii) un/plusieurs facteurs d'augmentation des risques ont été identifiés (risque élevé de BC/FT ou soupçon de BC/FT)

6.2 – Rejet ou renvoi d'un transfert

- Si rejet/renvoi par CASP bénéficiaire/CASP-I : information des précédents CASP/CASP-I de la chaine
- Si rejet impossible techniquement : renvoi à l'initiateur. Si renvoi à l'adresse initiale techniquement impossible: méthodes alternatives définies dans politiques/procédures (renvoi sur compte ségrégué sécurisé/contact initiateur pour convenir d'une méthode appropriée)

6.3 – Demande des informations requises

- Si CASP/CASP-I demande les informations : fixer un délai raisonnable à compter de la date d'identification (transferts intra UE : 3 jours ouvrables / transferts reçus depuis extérieur : 5 jours ouvrables) + notification au CASP/CASP-I précédent des mesures prises concernant ce transfert
- Envoi des demandes : même système de messagerie qu'utilisé pour transmettre les informations requises. Si limitations techniques/dérogations : moyens de communication sécurisés *RGPD compliant*
- Informations demandées non fournies/non fournies dans le délai: adaptation des mesures en fonction des risques et anticipation pour les transferts futurs (rejets de futurs transferts depuis/vers le CASP précédent – restriction ou fin de la relation d'affaires avec ce CASP)

ORIENTATIONS TFR (ASPECTS CRYPTO)

6. Transferts pour lesquels des informations sont manquantes ou incomplètes

6.4 – Exécution d'un transfert pour lequel les informations sont manquantes/incomplètes

- Documenter la raison de l'exécution du transfert et prendre des dispositions en vue du traitement futur du CASP/ CASP-I précédent
- Si l'initiateur ou le bénéficiaire ne peut être identifié sans ambiguïté en raison d'informations manquantes ou incomplètes: **ne pas effectuer le transfert**

6.5 – Détection post-transfert d'informations manquantes ou incomplètes

- Demander au CASP ou au CASP-I précédent dans la chaîne de transfert de fournir les informations manquantes

ORIENTATIONS TFR (ASPECTS CRYPTO)

7. Omissions répétées

7.1 – Traitement

- Politiques et procédures définissant les critères quantitatifs et qualitatifs pour déterminer si un CASP/CASP-I est responsable d'« omissions répétées » et documenter tous les transferts avec informations manquantes/incomplètes
  - **Quantitatifs**
    - % de transferts par CASP/CASP-I avec informations manquantes/incomplètes dans un laps de temps donné
    - % pourcentage de demandes de retours sans réponse/non traitées dans un délai donné
  - **Qualitatifs** :
    - Niveau de coopération pour les précédentes demandes d'informations manquantes
    - Existence d'un accord avec CASP/CASP-I nécessitant davantage de temps pour fournir les informations
    - Type d'informations manquantes/incomplètes et raison invoquée par CASP/CASP-I pour ne pas fournir ces informations
- Avertissement informant CASP/CASP-I précédent des dispositions appliquées si persistance à ne pas fournir les informations requises (échéances) - Envisager un nouvel avertissement signifiant le rejet de tout futur transfert incomplet

7.2 – Signalement

- Déclaration à l'autorité compétente (TFR2, art. 17(2) et 21) : sans retard indu, et au plus tard trois mois après identification d'omissions répétées
- Déclaration incluant : identification du CASP/CASP-I – Pays d'autorisation – nature de l'infraction

ORIENTATIONS TFR (ASPECTS CRYPTO)

8. Transferts effectués vers ou depuis une adresse auto-hébergée

8.1 – Identification individuelle

- Transfert vers/depuis adresse auto-hébergée réputé identifié individuellement lorsque : identifiant unique utilisé pour chaque transfert (ex. hachage de transaction ou un numéro de référence) + informations supplémentaires incluses dans le transfert afin de permettre l'identification du transfert

8.2 – Identification d'une adresse auto-hébergée

- CASP initiateur/bénéficiaire devraient s'appuyer notamment, mais pas exclusivement, sur l'analyse des chaînes de blocs, les fournisseurs de données tiers et les identifiants utilisés par les systèmes de messagerie
- Si impossible techniquement, obtenir ces informations directement auprès des clients
- Dans ce cas, si transfert est effectué vers/à partir d'un autre CASP, CASP initiateur/bénéficiaire devraient prendre les mesures nécessaires pour identifier avec précision le CASP de la contrepartie

8.3 – Identification de l'initiateur et du bénéficiaire

- Lorsqu'une adresse auto-hébergée est utilisée à l'autre extrémité de la chaîne d'un transfert, obtenir les informations sur l'initiateur ou le bénéficiaire des crypto-actifs auprès du client

ORIENTATIONS TFR (ASPECTS CRYPTO)

8. Transferts effectués vers ou depuis une adresse auto-hébergée

8. 4 – Transferts supérieurs à 1 000€

- Détermination à l'initiation (CASP initiateur) ou à la réception (CASP bénéficiaire)
- Prise en compte du taux de change du crypto-actif transféré au moment du transfert (hors frais de transaction)
- Détermination du contrôle par initiateur/bénéficiaire - méthodes de vérification :
  - Vérifications automatisées indiquant l'adresse (cf. orientations EBA - solutions d'entrée en relation d'affaires à distance)
  - Vérifications non automatisées (cf. orientations EBA - solutions d'entrée en relation d'affaires à distance)
  - Envoi d'un montant prédéfini (de préférence la plus petite valeur d'un crypto-actif donné), fixé par le CASP, depuis et vers l'adresse auto-hébergée sur le compte du CASP
  - Demander au client de signer numériquement un message spécifique dans le logiciel de compte/portefeuille avec la clé correspondant à l'adresse
  - Autres moyens techniques appropriés (sous conditions)
- Choix de la méthode : fonction des capacités techniques de l'adresse auto-hébergée, de la fiabilité de l'évaluation de chaque méthode, du risque BC/FT
- Combinaison nécessaire si une seule méthode n'est pas assez fiable
- Une fois le contrôle établi, le documenter pour ne pas répliquer les mesures pour les transferts suivants (liste blanche), sauf évolution du risque BC-FT

ORIENTATIONS TFR (ASPECTS CRYPTO)

8. Transferts effectués vers ou depuis une adresse auto-hébergée

8.5 – Mesures d'atténuation

- Evaluer le risque associé à ces transferts (cf. orientations EBA - facteurs de risque) – Utiliser toutes les informations relatives aux initiateurs/bénéficiaires, aux schémas et aux zones géographiques, ainsi que les informations provenant de régulateurs, de services répressifs et de tiers
- Mesures d'atténuation en fonction des risques (introduites par TFR2 dans AMLD) :
  - Identifier et vérifier l'identité de l'initiateur/bénéficiaire ou de leur BE, y compris en faisant appel à des tiers;
  - Renseignements supplémentaires sur l'origine et la destination des crypto-actifs transférés;
  - Suivi continu renforcé de ces transactions;
  - Toute mesure pour atténuer/gérer risques BC/FT + irrespect/contournement des sanctions financières
- Application d'au moins une mesure d'atténuation si :
  - Informations relatives à l'initiateur ou au bénéficiaire de crypto-actifs utilisant l'adresse auto-hébergée sont inexactes
  - Schémas de transactions inhabituels ou suspects – situations présentant des risques BC/FT plus élevés associés à des transferts impliquant des adresses auto-hébergées (cf. orientations EBA - facteurs de risque)
- Si adresse auto-hébergée détenue ou contrôlée par un tiers et non par le client du CASP, les mesures d'identification/vérification d'identité sont réputées satisfaites si le CASP :
  - Obtient des données supplémentaires auprès d'autres sources afin de vérifier les informations transmises (eg données analytiques sur les chaînes de blocs, données de tiers, données d'autorités reconnues, informations accessibles au public, si fiables et indépendantes) ;
  - Utilise d'autres moyens appropriés, pour autant qu'il soit pleinement convaincu qu'il connaît l'identité de l'initiateur ou du bénéficiaire de crypto-actifs et qu'il peut le démontrer à son autorité compétente
- Déclaration CRF si soupçon

IV. FATF Standards on Virtual Assets and Virtual Assets Service Providers

FINANCIAL ACTION TASK FORCE
GROUPE D'ACTION FINANCIÈRE

FATF Standards on Virtual Assets and Virtual Assets Service Providers

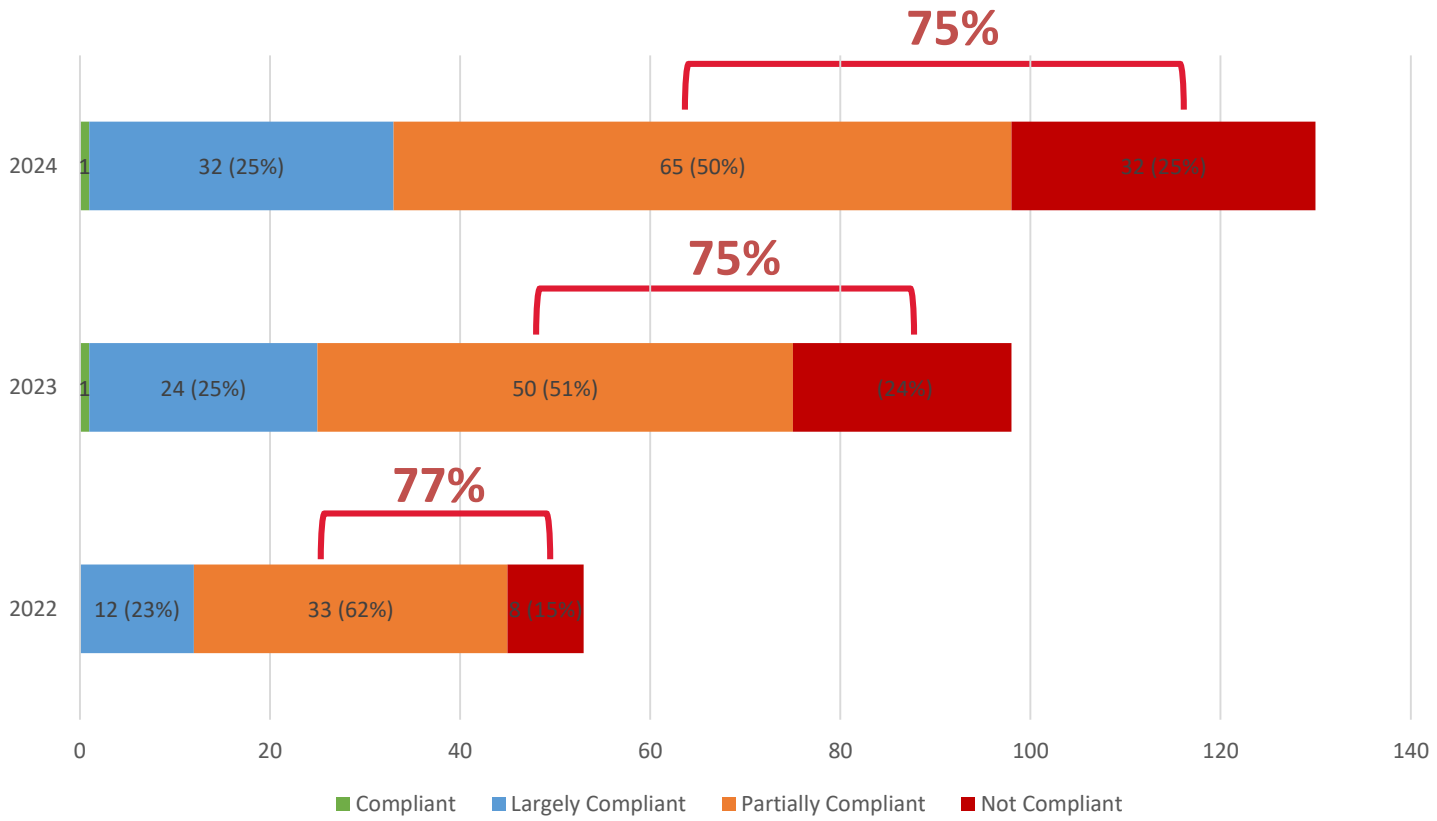
ACPR-AMF Fintech forum - AML-CFT workshop

14 October 2024

Financial Action Task Force

Global implementation of the revised R.15

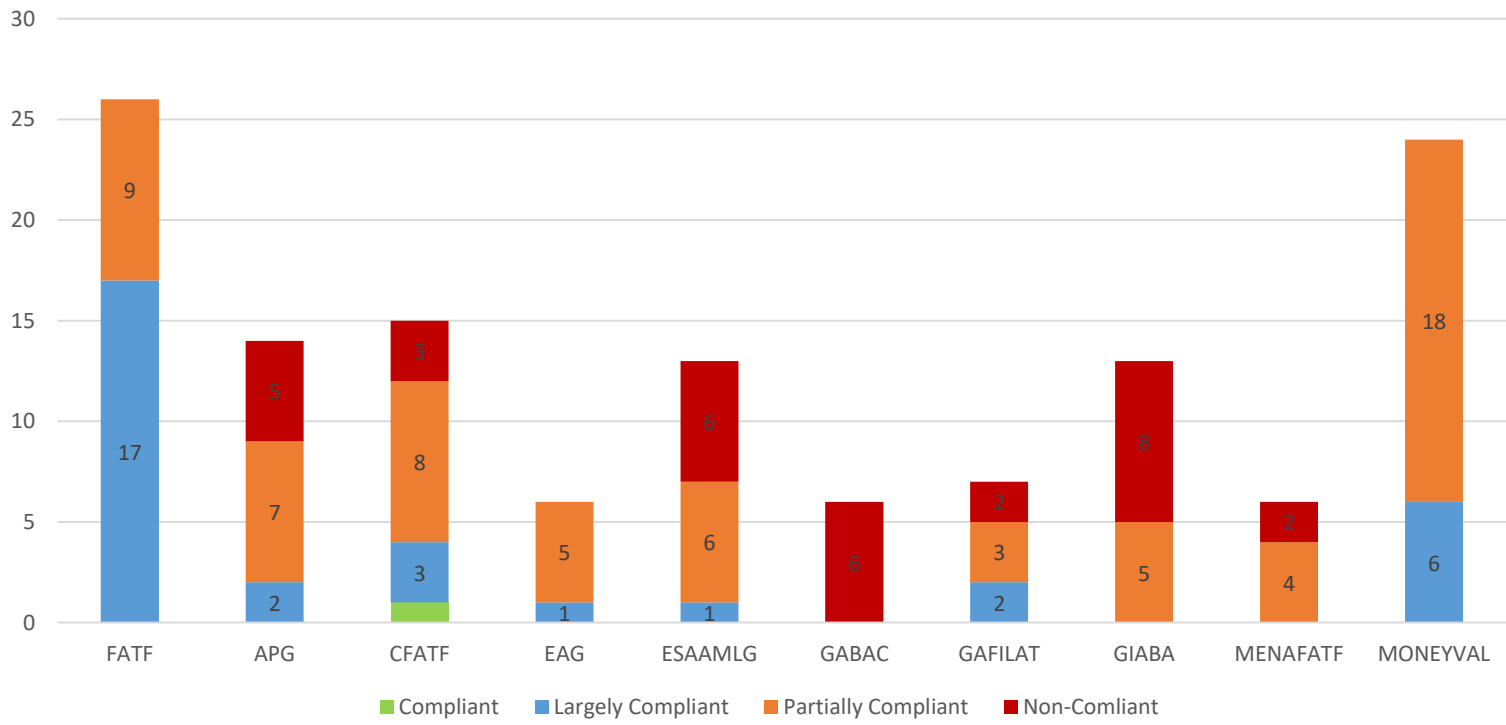
Compliance with revised R.15/INR.15
130 jurisdictions (2024 Targeted Update)
98 jurisdictions (2023 Targeted Update)
53 jurisdictions (2022 Targeted Update)



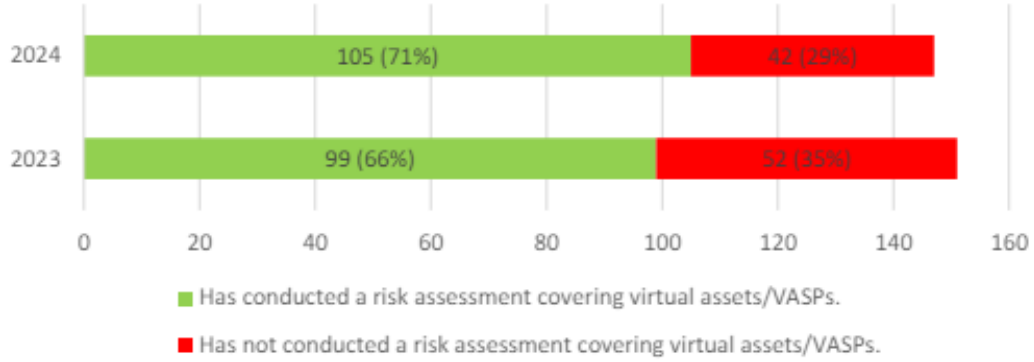
Global implementation of the revised R.15

Compliance with revised R.15/INR.15

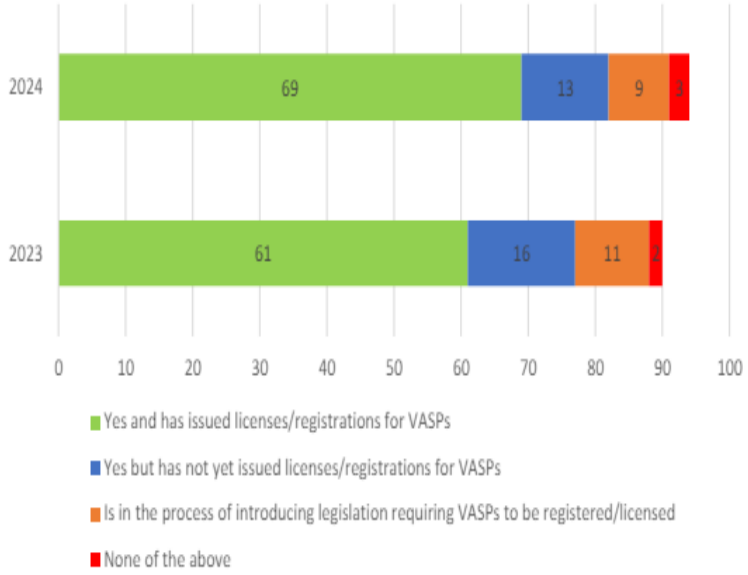
130 jurisdictions (2024 Targeted Update)



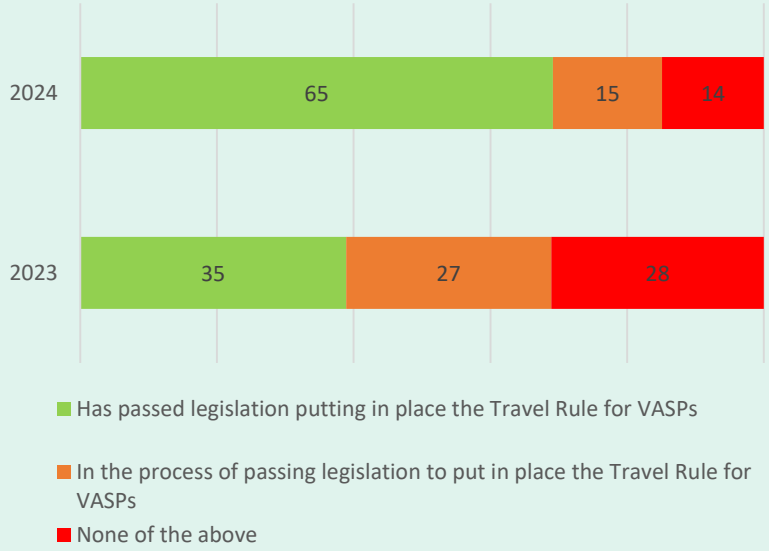
15.3 Risk assessment and application of a risk-based approach



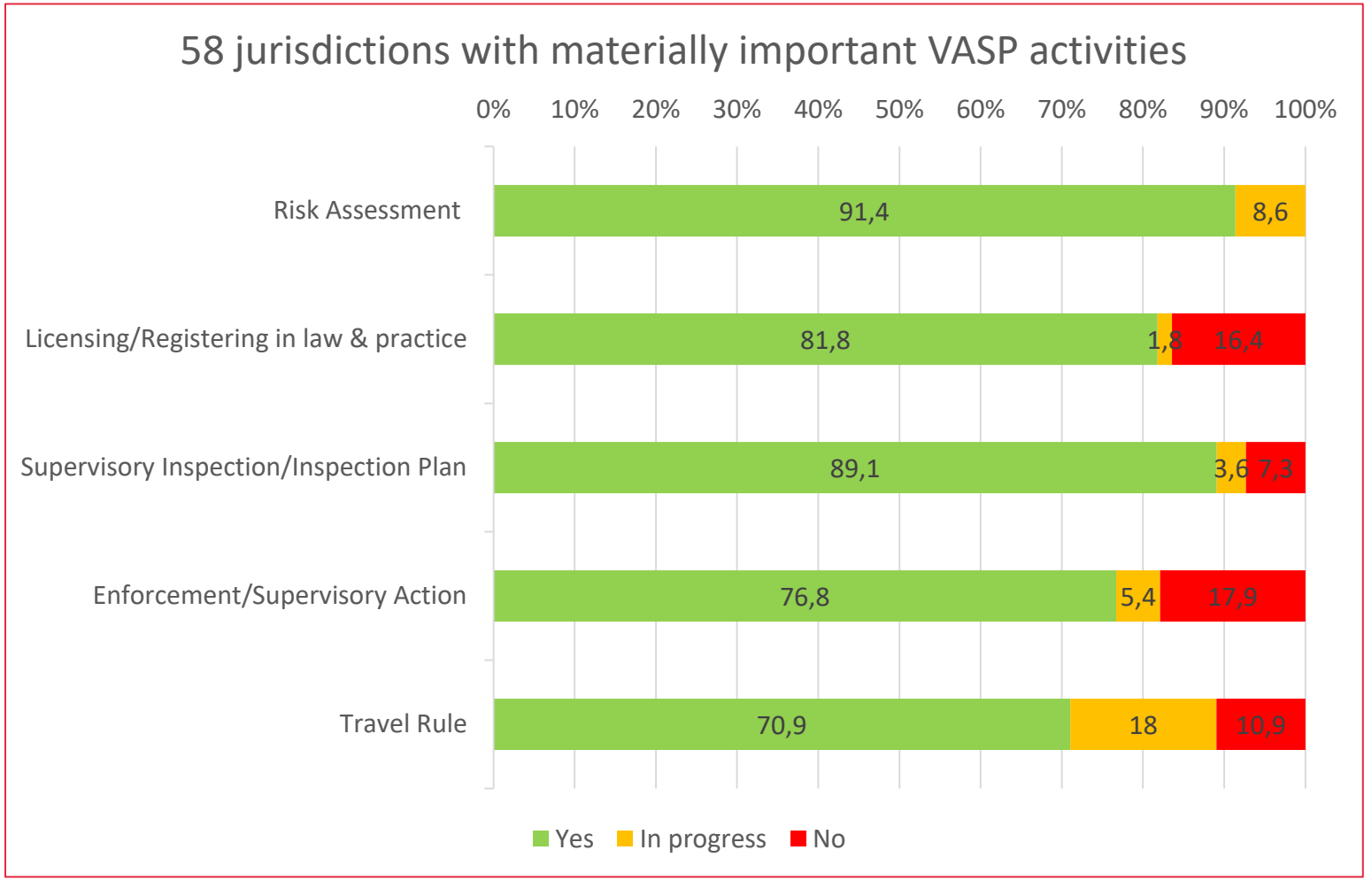
15.4 Licensing/Registering VASPs

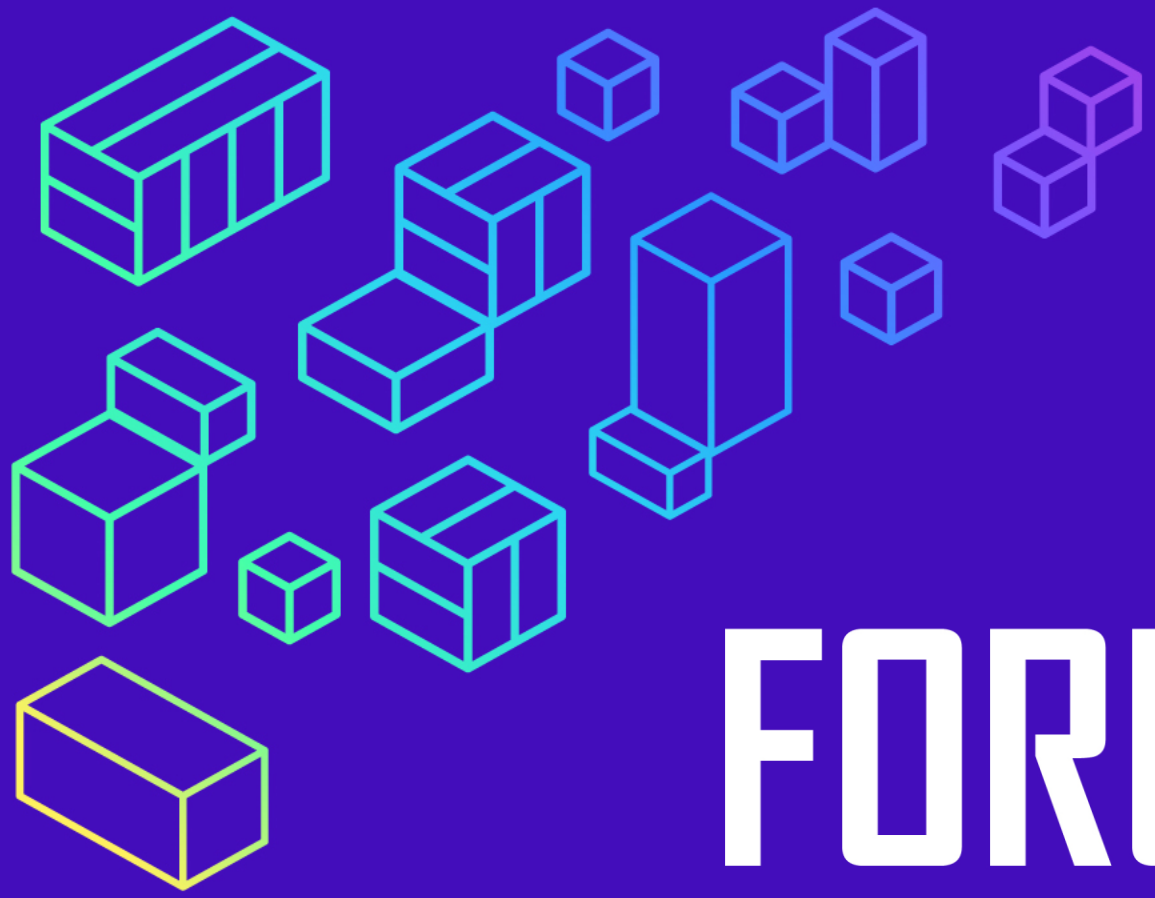


15.9 Preventative AML/CFT measures including the Travel Rule



Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity (March 2024)





ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

FORUM FINTECH

ACPR - AMF

14 octobre 2024