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

9 octobre 2025

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

I. **État des lieux du déploiement de l'IA en matière de LCB-FT (Antonin Weiss)**

II. **Présentation et dernières évolutions de l'outil Lucia (Vincent Vasques)**

III. **Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes (Elodie Chanut)**

IV. **Orientations EBA sur les mesures restrictives (Sylvain Aubert)**

V. **Point d'étape sur la supervision du secteur des crypto-actifs (Aloïs Gareste)**

I. État des lieux du déploiement de l'IA en matière de LCB-FT

CONTEXTE ET POINT DE DÉPART DES TRAVAUX

Les réflexions de l'ACPR sur le déploiement des systèmes à base d'IA partent d'un double constat :

Dans l'ensemble, le fonctionnement des outils utilisés par les établissements assujettis est sous-optimal.

- Le fonctionnement de certains outils utilisés en matière de surveillance est peu efficient.
- Les sujets de qualité et de disponibilité des données sont fréquents.
- La qualité des outils à la main des analystes de la conformité est perfectible.

Lors de ses entretiens et contrôles, l'ACPR a constaté une forte dynamique d'innovation.

CAS D'USAGE THÉORIQUES DE L'IA EN MATIÈRE DE LCB-FT

Les lignes directrices conjointes de l'ACPR et de TRACFIN relatives aux obligations de vigilance sur les opérations et aux obligations de déclaration et d'information identifient plusieurs cas d'usages de l'IA en matière de LCB-FT :

- **Profilage clients** : outils de *scoring* avancé, meilleure segmentation de la clientèle tenant compte de critères de risque multiples ;
- **Surveillance des transactions** : renforcement de la pertinence des alertes générées par les outils de surveillance des transactions et réduction du volume de faux positifs ;
- **Assistance à la rédaction ou à la saisine des échanges** : pré-rédaction de déclarations de soupçon, analyse de RFI ;
- **Analyse comportementale** : détection de réseaux ou de circuits de blanchiment organisés non observables avec les approches traditionnelles ;
- **Contrôle interne** : renforcement des dispositifs de contrôle permanent et périodique.

CAS D'USAGE OBSERVÉS EN PRATIQUE (1/2)

Les entretiens du contrôle permanent sur l'IA dans le domaine de la LCB-FT permettent de distinguer quatre grandes catégories d'usage:

Les modèles ML de type *boosting*

- Il s'agit de modèles prédictifs entraînés à partir de décisions passées pour améliorer les décisions futures.
- Ces modèles sont particulièrement efficaces pour réduire la volumétrie de faux-positifs.

Les modèles ML semi-supervisés (Isolation Forest, anomalies)

- Il s'agit de modèles permettant de détecter des anomalies dans des volumes de données importants.
- Ce type de solution complète bien les modèles de ML car il permet d'explorer des zones de risques non couvertes.

CAS D'USAGE OBSERVÉS EN PRATIQUE (2/2)

Les modèles *de langage* utilisant le NLP et le LLM

- Une majorité des usages observés vise à renforcer les capacités d'analyses des opérationnels chargés du traitement des alertes (graphes relationnels, instrument de visualisation des données, aide à la décision).
- Le LLM offre des perspectives d'automatisation pour certaines tâches (RFI, pré-rédaction de DS, orientation du processus d'escalade).

Les modèles non supervisés

- Leur utilisation est plus expérimentale, à ce jour.
- Ils offrent des perspectives en matière de détection de réseaux ou de liens entre clients.

PREMIERS RETOURS

Sur la base de ces entretiens, le potentiel de l'IA en matière de LCB-FT semble considérable.

***Big data*: le déploiement de modèles d'IA en matière de LCB-FT n'est possible qu'au terme d'un travail préalable sur la donnée.**

- Il est nécessaire d'avoir une vue à 360° du client et de ses opérations pour entraîner des modèles performants.
- Les acteurs *digital natives* ont un temps d'avance en matière de *big data.*

La gouvernance et le suivi des modèles est un enjeu central.

- L'efficacité des modèles doit être monitorée en permanence pour permettre un réentraînement en cas de dérive.
- La gouvernance des modèles doit impérativement inclure le métier.

Le cadre réglementaire autour de l'usage de l'IA est en déploiement.

- Le déploiement de l'IA doit s'effectuer dans le respect des dispositions de l'*AI Act* et du RGPD.
- Dans ce cadre, la LCB-FT est reconnue d'utilité publique.

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

I. **État des lieux du déploiement de l'IA en matière de LCB-FT (Antonin Weiss)**

II. **Présentation et dernières évolutions de l'outil Lucia (Vincent Vasques)**

III. **Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes (Elodie Chanut)**

IV. **Orientations EBA sur les mesures restrictives (Sylvain Aubert)**

V. **Point d'étape sur la supervision du secteur des crypto-actifs (Aloïs Gareste)**

II. Présentation et dernières évolutions de l'outil Lucia

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)*

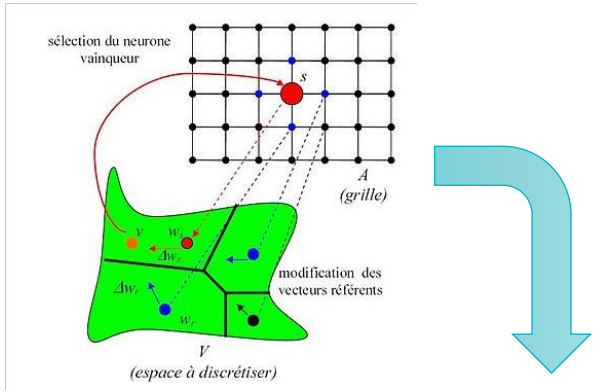
*** Revue thématique de l'ACPR sur les dispositifs automatisés de surveillance des opérations en matière de LCB-FT (Avril 2023)*

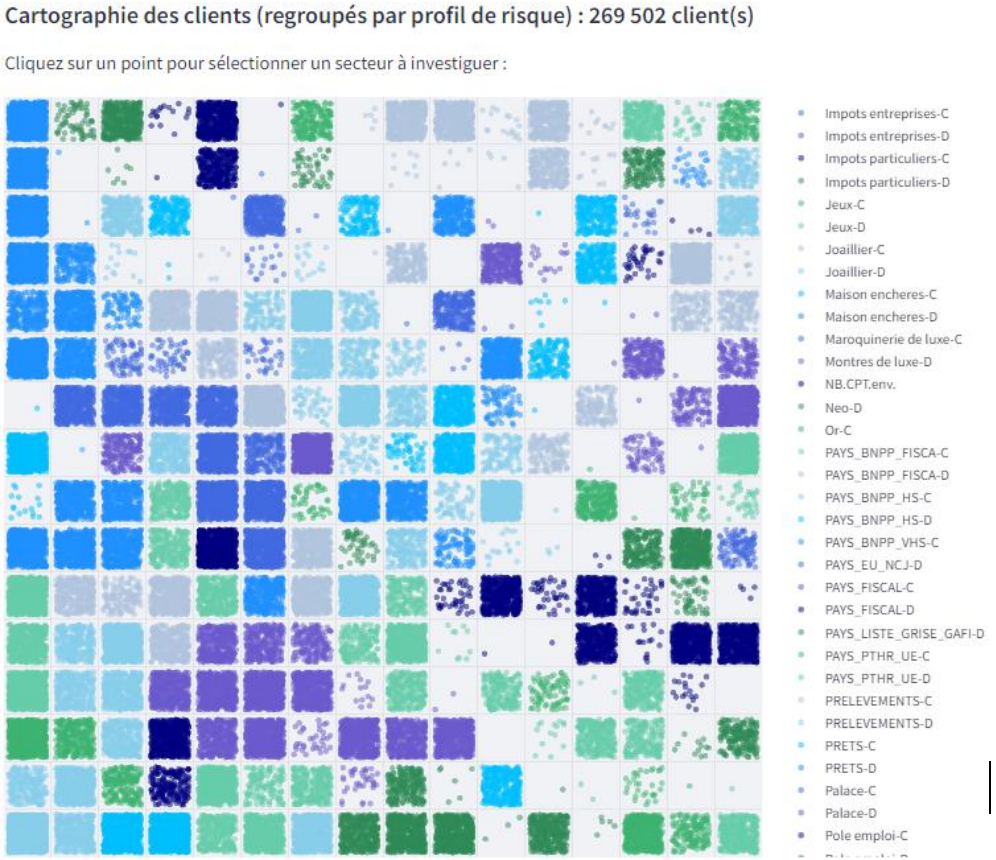
LUC!A : UN OUTIL SUPTECH

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

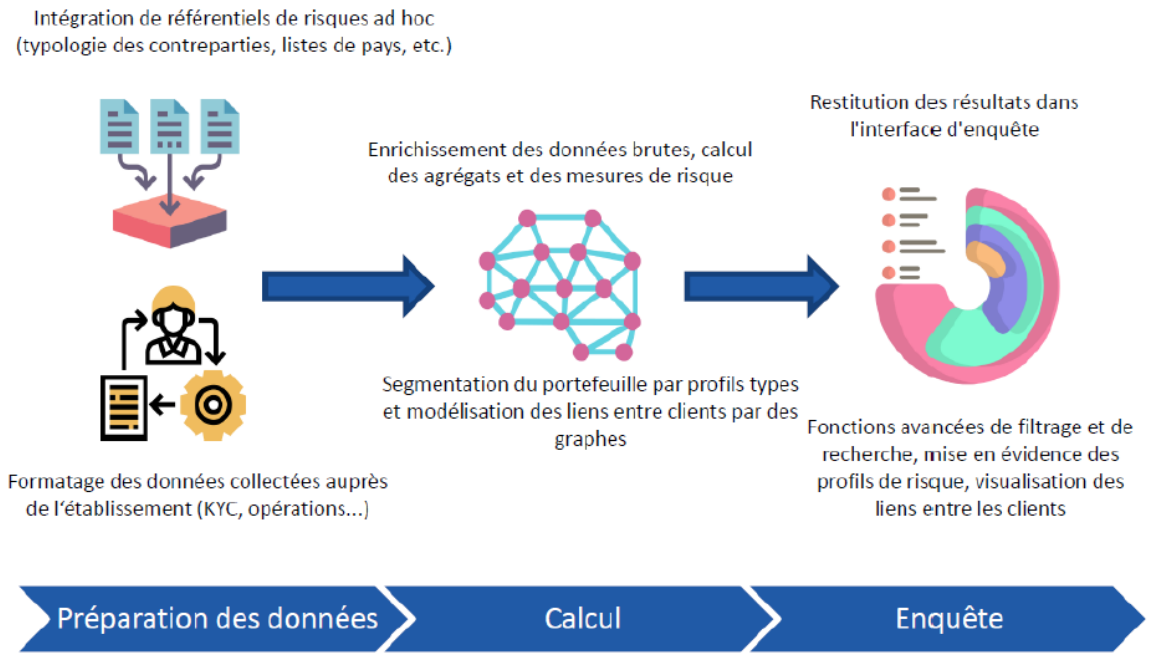
L'outil **LUCIA** est construit sur un réseau de neurones artificiels qui :

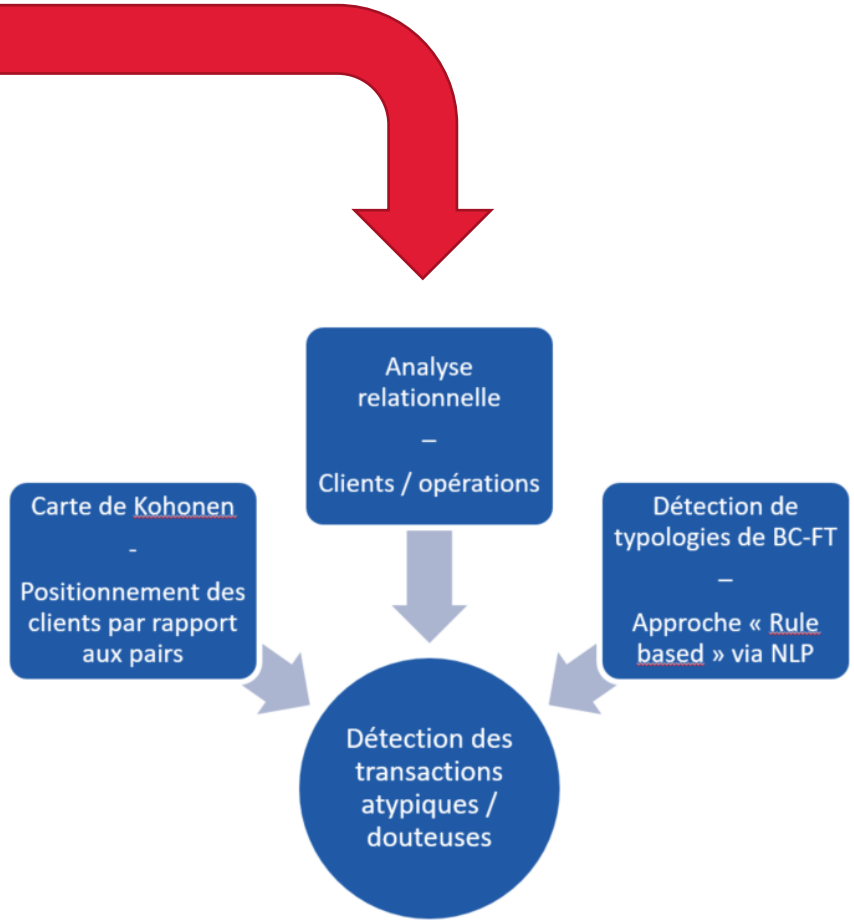
- restitue visuellement les informations sous la forme d'une cartographie intelligente (**carte auto-adaptative*** également appelée **carte de Kohonen**) en regroupant automatiquement les clients par profils de risque
- met en œuvre des algorithmes d'exploration de données (**data mining**) pour extraire 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**





DES DONNÉES À L'ANALYSE





DES DONNÉES À L'ANALYSE

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

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)**

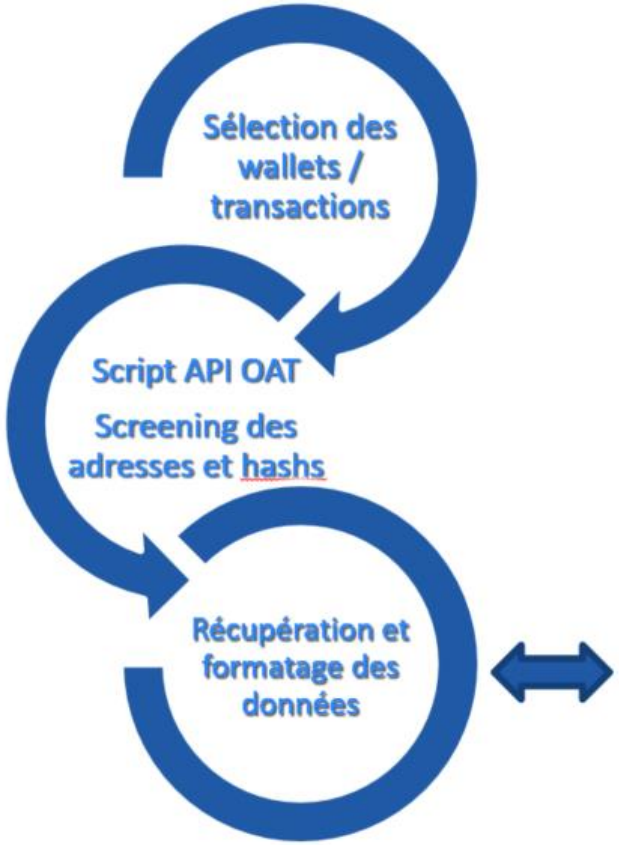
La mission d'Inspection de l'ACPR réalise des contrôles sur l'exhaustivité et la qualité des données communiquées (données censées être utilisées par l'établissement contrôlé pour son propre dispositif de surveillance)

- **de référentiels de données choisis, 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.

DES DONNÉES À L'ANALYSE



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
...	...
...	...
...	...

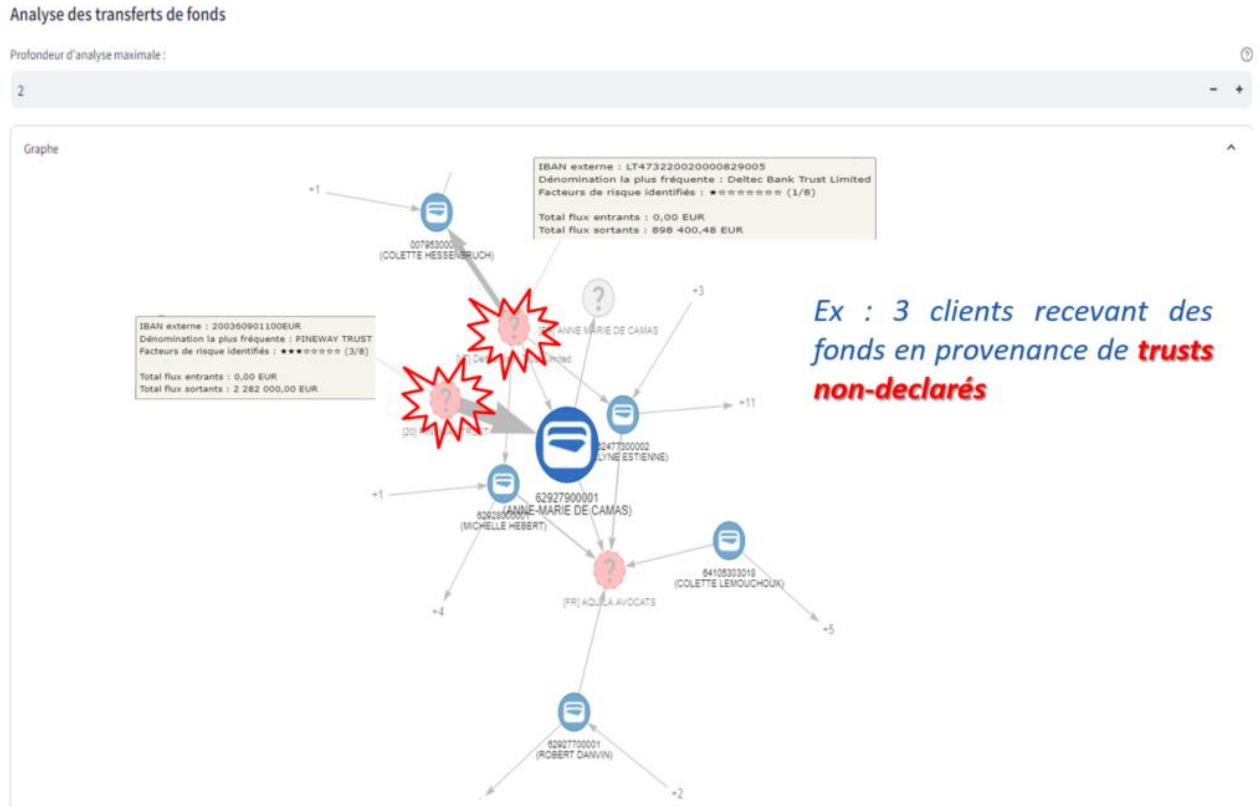
L'interfaçage entre LUCIA et un OAT permet d'identifier les clients et transactions à risque lors du contrôle d'un PSAN

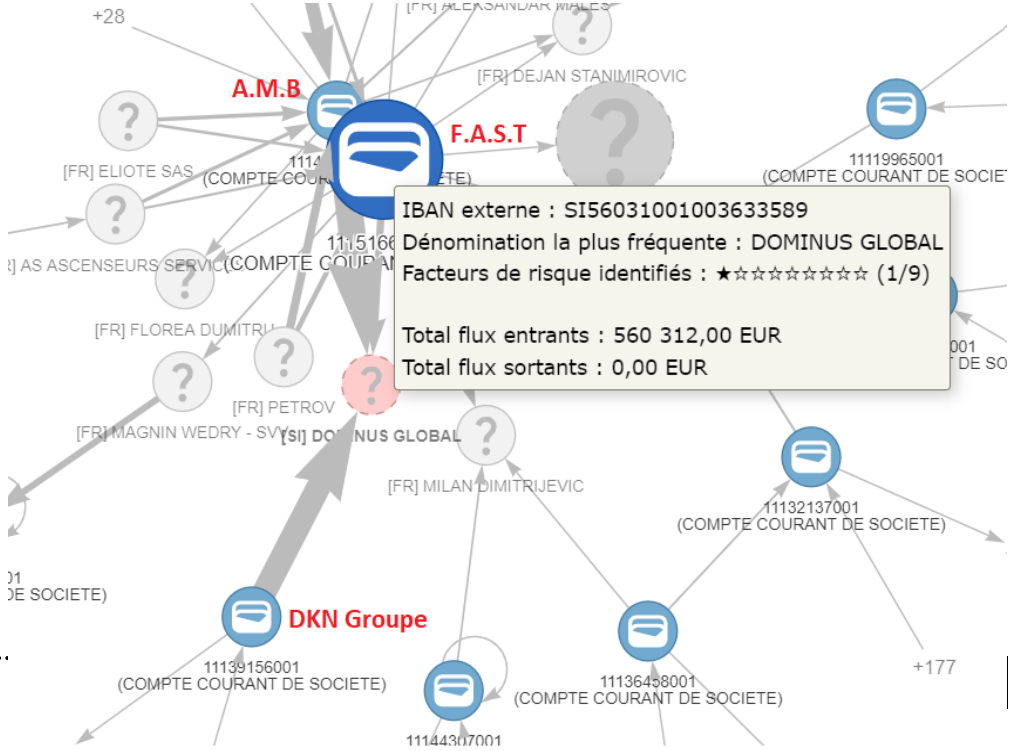
- L'appel à l'API d'un OAT permet de récupérer les facteurs de risque associés aux wallets et transactions afin de les intégrer dans les référentiels de données utilisés dans le cadre du contrôle
- Possibilité de prendre en compte simultanément les données de connaissance clientèle, les transactions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

LES APPORTS DE L'ANALYSE EN GRAPHE RELATIONNEL

L'analyse en graphe relationnel, guidée en amont par la sélection des facteurs de risques pertinents, permet de détecter plus efficacement les réseaux de clients / contreparties dont le comportement transactionnel correspond à des schémas à risque :

- Exemple n°1 : typologie de fraude fiscale impliquant des rapatriements de fonds depuis des trusts non-déclarés
- Exemple n°2 : typologie de blanchiment par l'intermédiaire de comptes rebonds et sociétés dites « taxis »





GAGNER EN EFFICACITÉ / EFFICIENCE

Principaux axes de travail 2025-2026 :

1. Nouvelle fonctionnalité « ***Natural Language to SQL*** »
2. Développements méthodologiques sur la **détection des typologies de BC-FT** : analyse des cas typologiques (Tracfin, Egmont, etc.), identification des facteurs de risques pertinents (red flags) et des sources d'informations additionnelles publiques, cartographie des activités exposées à chaque typologie
3. **Déclinaison opérationnelle des méthodes de détection des typologies** (process existant, objectif d'industrialisation)
4. Identification / caractérisation des contreparties parties prenantes des virements (***entity resolution***) et enrichissement automatisée de l'information
5. Développements sur la **carte de Kohonen** et l'analyse en **graphes relationnels**

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

I. **État des lieux du déploiement de l'IA en matière de LCB-FT (Antonin Weiss)**

II. **Présentation et dernières évolutions de l'outil Lucia (Vincent Vasques)**

III. **Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes (Elodie Chanut)**

IV. **Orientations EBA sur les mesures restrictives (Sylvain Aubert)**

V. **Point d'étape sur la supervision du secteur des crypto-actifs (Aloïs Gareste)**

III. Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes

UNE ÉTUDE VISANT LES COMPTES REBOND FRANÇAIS

En avril 2024, la Direction LCB-FT de l'ACPR a adressé un questionnaire à 13 établissements destinataires des montants les plus élevés de virements frauduleux en 2022, dans un contexte de hausse significative de la fraude aux virements (quadruplement depuis 2017 selon l'Observatoire de la Sécurité des Moyens de Paiement) et de recours accru à des comptes français pour en blanchir le produit (multiplié par près de 7 en cinq ans).

Cette revue conduite par l'ACPR se concentre sur les comptes récipiendaires de virements que les établissements interrogés suspectent d'être frauduleux ou émis dans le cadre d'une escroquerie.

Le questionnaire utilisé par l'ACPR comporte 3 catégories d'informations :

- des données statistiques générales sur l'année 2022 et 2023,
- les mesures et les procédures de réduction du risque de blanchiment du produit de la fraude
- un recueil de 650 cas individuels, correspondant aux 50 relations d'affaires des établissements interrogés ayant reçu un montant de demandes de rappels de virements le plus important en 2023, sur des IBAN français.

Périmètre de l'étude : Le soupçon peut découler :

- D'une demande de rappel de virement par son émetteur
- D'une réquisition judiciaire
- D'une demande des autorités
- Du dispositif interne
- D'une mesure de vigilance renforcée pour le motif de blanchiment de fraude : DS ou clôture de compte

ANALYSE DES DONNÉES GÉNÉRALES

- **Une hausse des soupçons de blanchiment par l'utilisation de comptes français**

	2022	2023	Croissance entre 2022 et 2023
Montant brut de virements suspects	457 M€	661 M€	45 %
Nombre de virements suspects reçus	510 392	757 432	48 %
Montant moyen d'un virement suspect reçu	896 €	873 €	-2,6 %

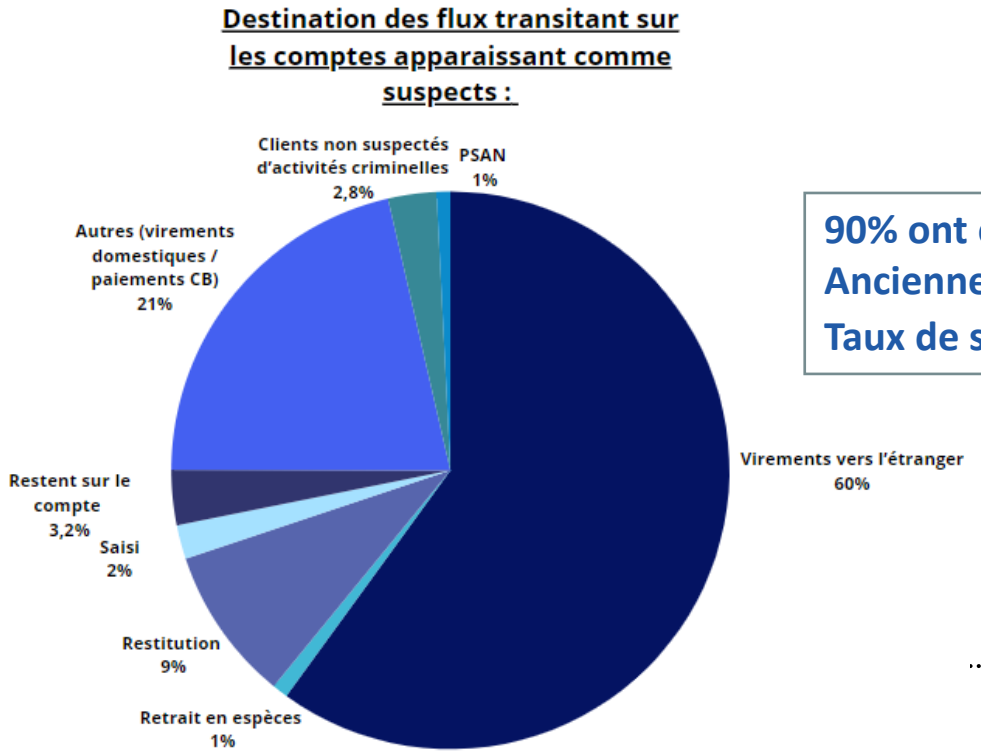
- **Caractéristiques remarquables des comptes et établissements destinataires des virements suspects :**
  - Des titulaires majoritairement personnes physiques (95%)
  - Des relations d'affaires récentes (43% ouverts en 2023)
  - Parmi les relations d'affaires personnes morales, 35% de création très récente (moins de 18 mois)
  - Une croissance importante de la clientèle (>20% pour 8 des établissements)
  - Des entrées en relation à distance (à 76%)

- **Un phénomène massif d'ouvertures de comptes et de sorties rapides des fonds qui complique l'action répressive**
  - 71 274 clôtures de comptes pour un motif fraude en 2023; un tiers des comptes sont fermés dans les 3 mois de leur ouverture
  - 982 M€ ont transité par les comptes clôturés, sans être ni restitués ni saisis ni immobilisés

DESTINATION DES FLUX APRÈS REBOND (650 CAS)

- **Analyse de la destination des fonds suspects reçus par les 650 relations d'affaires visées par les principales demandes de retours de virements en 2023**

	Demandes de rappels de virement	Virements suspects reçus (hors recalls)	Total des virements suspects reçus
Montant total	65,7 M€	73 M€	138,7 M€
Nombre total	4 145	15 469	19 614



90% ont été clôturés
Ancienneté <1an (70% des cas)
Taux de succès des recalls : 31%

ZONES DE VULNÉRABILITÉ IDENTIFIÉES

- **Une sous-estimation du risque de la clientèle, qui conduit à des diligences peu approfondies**
  - Vérification d'adresse (26%)
  - Collecte du montant des revenus (68% des personnes physiques)
  - Collecte du montant du chiffre d'affaires (52% des personnes morales, les 4/5^{e} étant de création très récente ou en formation)

- **Vigilance des opérations insuffisante**
  - plus d'un quart des relations d'affaires personnes physiques ayant déclaré des revenus lors de l'entrée en relation (montant ou tranche) ont reçu des virements suspects plus de 5 fois plus importants que leurs revenus attendus sur la durée de vie de leur compte
  - 65% des premières alertes sur les comptes sont d'origine interne

- **Conception des produits**
  - Absence de seuils d'opérations de virements (3 établissements)
  - Seuils de virements ou de paiement par carte très élevés (jusqu'à 1M€/jour par virement ; jusqu'à 1M€/semaine de paiement par carte)
  - Des capacités de blocage limitées
  - Services d'IBAN virtuels (34% des cas les plus graves pour 1 établissement) ou multidétention (1 établissement relèvent 877 comptes pour 50 relations d'affaires)

BONNES PRATIQUES ET POINTS D'ATTENTION (1/2)

- **<u>Adapter le pilotage du dispositif de gestion des risques afin d'éviter que leurs services soient utilisés par les réseaux criminels de blanchiment du produit de fraude ou d'escroquerie</u>**

- Prise en compte du risque de blanchiment de fraude dans la **cartographie des risques.**
- Mise en place d'**indicateurs de suivi** par les instances dirigeantes (traitement des demandes de rappels de virements, des saisies judiciaires).
- Renforcement du **contrôle interne** pour s'assurer du bon fonctionnement des dispositifs.
- En cas d'apparition de nouvelles fraudes ou de détection de défaillances majeures exploitées par un réseau criminel, envisager des **actions rapides** (suspension ou adaptation des produits et processus en cause jusqu'à correction, réexamen des relations d'affaires).

- **<u>Lors de l'entrée en relation, une vérification d'identité fiable</u>**

- Mettre en oeuvre au moins **deux mesures de vérification en cas d'entrée en relation à distance** (article R. 561-5-2 du Code Monétaire et Financier).
- S'appuyer sur des pièces justificatives recueillies auprès de **sources indépendantes fiables**, notamment pour les clients personnes morales (recueil auprès des registres officiels, vérification des mandataires).
- **Renforcer les mesures** de vérification d'identité en cas de risque élevé, avec la possibilité de recourir à un nombre de mesures plus important.
- Le recours à un **prestataire de vérification d'identité à distance (PVID)** est une bonne pratique.

BONNES PRATIQUES ET POINTS D'ATTENTION (2/2)

- **Une connaissance client adaptée pour évaluer le risque**

- Caractère indispensable des informations sur l'**activité exercée** et la **situation financière**, y compris pour les sociétés nouvellement créées.
- Collecter des **éléments de connaissance complémentaires** en cas de risque élevé : justification de l'adresse du domicile ou siège social, typologies d'opérations attendues.
- Pour écarter le risque de falsification ou d'usurpation, utiliser des **justificatifs robustes** (code barre « 2D-Doc » apposé sur le justificatif de domicile, open banking, lettres avec AR).
- Déterminer dès l'entrée en relation et actualiser le **profil de risque** de la relation d'affaires.

- **Une vigilance des opérations pertinente et efficace, permettant de détecter les opérations atypiques, mener un examen renforcé**

- Paramétrer les dispositifs de vigilance au regard de la connaissance client, afin de **détecter les incohérences avec les opérations attendues**, les revenus voire le patrimoine.
- **Adapter les produits et services financiers** proposés et leurs modalités d'usage (plafonds d'opérations sans l'intervention d'un membre du personnel) au regard du profil de risque client
- Mettre en place des outils automatisés permettant la **suspension d'opérations** dans un temps court, voire en amont de l'exécution de l'opération, selon une approche par les risques, afin de conduire un **examen renforcé**.
- Prendre en compte les modalités techniques d'accès aux produits et services proposés à distance pour faciliter la **détection des utilisations illégitimes des services**.
- En cas de suspicion sur un compte, vérifier lors de l'examen renforcé les autres comptes présentant des **caractéristiques similaires**.

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

I. **État des lieux du déploiement de l'IA en matière de LCB-FT (Antonin Weiss)**

II. **Présentation et dernières évolutions de l'outil Lucia (Vincent Vasques)**

III. **Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes (Elodie Chanut)**

IV. **Orientations EBA sur les mesures restrictives (Sylvain Aubert)**

V. **Point d'étape sur la supervision du secteur des crypto-actifs (Aloïs Gareste)**

IV. Orientations 2024/15

Orientations sur les politiques, procédures et contrôles internes visant à garantir la mise en œuvre des mesures restrictives nationales et de l'Union au titre du règlement (UE) 2023/1113 (TFR2

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

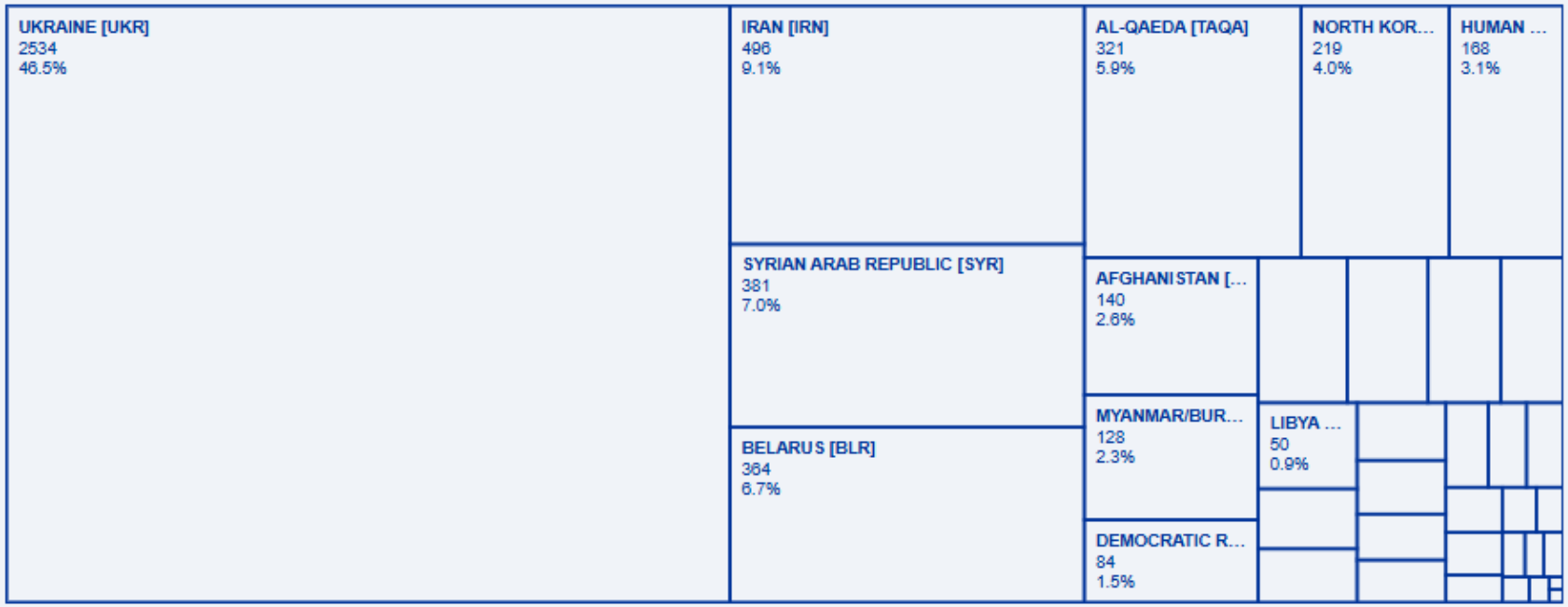
- **Contexte**
  - Les « mesures restrictives » : un élément de plus en plus central de la politique étrangère et de sécurité commune de l'Union
  - Plus de 35 régimes de sanctions EU, concernant plus de 5600 personnes ou entités
    - Ukraine : 18 paquets depuis 2022
    - Iran : rétablissement fin septembre 2025 de mesures suspendues en 2015 (dont gel d'avoirs)

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

Sanctions regimes sizes

This chart shows the volume and composition of different sanctions regimes based on the number of listings under each regime. A sanctions regime refers to the restrictive measures adopted either in view of the situation in a given country, or adopted to target specific horizontal actions (such as terrorism). Note that Ukraine (UKR) contains two regimes: restrictive measures regarding actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (which has most of the current designations) and restrictive measures directed against certain persons, entities and bodies given the situation in Ukraine (misappropriation of state funds regime). In addition also Iran (IRN) contains three regimes: restrictive measures in relation to the non-proliferation of weapons of mass destruction, restrictive measures in relation to serious human rights violations in Iran as well as restrictive measures in view of Iran's military support of Russia's war of aggression against Ukraine.

Individuals sanctioned with asset freezes, and travel bans are counted only once to produce the actual number of natural persons. Hovering over the regime shows detailed information about the percentual size of the regime compared to other regimes, the number of sanctioned individuals and entities, and the number of individuals under financial sanctions and travel bans.



SOURCE: EUROPEAN UNION

https://data.europa.eu/apps/eusanctionstracker/

INFO | DOWNLOAD

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

Contexte

- Principes directeurs : **application sans délai – obligation de résultat**
  - CMF (L. 562-4 & s. et R. 562-1 & s.) - Guide gel des avoirs (AMF) - Lignes directrices gel des avoirs et principes d'application sectoriels relatifs aux PSAN (ACPR)
- Mesures restrictives prises en compte par le nouveau cadre européen LCB-FT, notamment :
  - **Règlement (UE) 2024/1624 (AMLR), art. 9** : obligation de disposer de politiques, procédures et contrôles internes visant à garantir la conformité au règlement (UE) 2023/1113 (TFR2) et à tout acte administratif émis par tout superviseur; obligation d'appliquer des sanctions financières ciblées, d'atténuer et de gérer les risques d'absence de mise en œuvre et de contournement de sanctions financières ciblées
  - **Règlement (UE) 2023/1113 (TFR2), art. 23** : impose aux PSP/PSCA de disposer de politiques, procédures et contrôles internes visant à garantir la mise en œuvre de mesures restrictives et mandate l'EBA pour publier des orientations sur ce point
  - **Orientations EBA** (2024/14 et **2024/15**) sur les politiques, procédures et contrôles internes visant à garantir la mise en œuvre des « mesures restrictives » nationales et de l'Union

Périmètre des Orientations EBA/GL/2024/15

- Prestataires de services de paiement (PSP) pour les transferts de fonds & **Prestataires de services de cryptoactifs (PSCA) pour les transferts de cryptoactifs**

Application

- A compter du **30 décembre 2025**
- AMF et ACPR s'y conforment : **Position AMF DOC-2025-02** - **Avis ACPR (EBA/GL/2024/15)**

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

« Mesures restrictives » – notion

- Mesures **de l'UE** (au sens de la directive (UE) 2024/1226, art. 2(1)) soit celles adoptées par l'Union sur la base des articles 29 TUE ou 215 TFUE) et mesures **nationales**
- Mesures comprenant les « **sanctions financières ciblées** » et les « **mesures restrictives sectorielles** »
  - **Sanction financière ciblée** : gels des avoirs et interdictions de mettre des fonds/avoirs à la disposition de personnes et d'entités désignées
    - Définition EU non exhaustive de la notion de fonds/avoirs : permet de capter les cryptoactifs (cf. FAQ COM, PAS PSAN ACPR)
  - **Mesure restrictive sectorielle** : inclut les mesures économiques et financières telles que les restrictions ou interdictions de fourniture de certains services
    - Ex. : interdiction de fournir des services de portefeuille de cryptoactifs, de compte en cryptoactifs et de conservation de cryptoactifs à des ressortissants russes ou à des personnes physiques résidant en Russie, ou à des personnes morales, des entités ou des organismes établis en Russie (Règlement (UE) no 833/2014 du Conseil du 31 juillet 2014, art. 5 ter, §(2))

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

TFR2 – quelques rappels

- Modifie AMLD (Directive 2015/849) : inclut l'ensemble des catégories de CASP définies dans MiCA dans la catégorie des établissements financiers assujettis aux fins de la directive AMLD
- Définit les règles relatives aux informations relatives aux initiateurs/bénéficiaires accompagnant les transferts de cryptoactifs et les politiques, procédures et contrôles internes visant à garantir la mise en œuvre de mesures restrictives
- Transposition « négative » : ordonnance n° 2024-937 du 15 octobre 2024
- Entrée en application : **30 décembre 2024**

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

Présentation des Orientations

	Dispositions générales
1.	**Filtrage des mesures restrictives**
2.	**Mesures de vigilance et de vérification requises pour l'analyse des alertes**
3.	**Mesures de gel et de notification**
4.	**Garantir l'efficacité continue des politiques, procédures et systèmes de filtrage relatifs aux mesures restrictives**

Présentation non exhaustive des Orientations & limitée aux PSCA

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

Dispositions générales

- Mettre en place des politiques, des procédures et des contrôles pour être en mesure de se conformer aux mesures restrictives, **conformes aux orientations EBA/GL/2024/14** sur les politiques, procédures et contrôles internes visant à garantir la mise en œuvre des mesures restrictives nationales et des mesures restrictives de l'Union
- Ces politiques, procédures et contrôles doivent permettre :
  - **d'identifier** les personnes physiques ou morales, entités ou organismes faisant l'objet de mesures restrictives
  - de **prendre les mesures nécessaires** pour s'assurer vis-à-vis des personnes visées de
    - l'absence de mise à disposition de cryptoactifs
    - l'absence d'exécution de transactions financières
    - l'absence de fourniture de services interdits
  - de **prendre les mesures nécessaires** pour gérer les risques de contournement

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

1.	**Filtrage des mesures restrictives**

1.	Choix du système de filtrage
2.	Gestion des listes
3.	Définition de l'ensemble de données à filtrer
4.	Filtrage de la clientèle
5.	Filtrage des transferts de cryptoactifs
6.	Calibrage
7.	Recours à des tiers et externalisation

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

2.	**Mesures de vigilance et de vérification requises pour l'analyse des alertes**

1.	Politiques et procédures en matière de gestion et d'analyse des alertes
2.	Mesures de vigilance pour l'analyse des alertes
3.	Évaluer si une entité est détenue ou contrôlée par une personne désignée
4.	Contrôles et mesures de vigilance pour se conformer aux mesures restrictives sectorielles
5.	Mesures de vigilance visant à détecter les tentatives de contournement des mesures restrictives

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

3. Mesures de gel et de notification

1. Gel des transferts de cryptoactifs
2. Mesures de signalement
3. Procédures d'exemption ou en cas de levée des mesures restrictives

ORIENTATIONS EBA - MESURES RESTRICTIVES (ASPECTS CRYPTO)

4. Garantir l'efficacité continue des politiques, procédures et systèmes de filtrage relatifs aux mesures restrictives

Les politiques, procédures et systèmes de filtrage devraient permettre de :

- **détecter** de manière fiable les correspondances positives
- dès confirmation, **suspendre immédiatement** l'exécution de tout transfert, **bloquer tout transfert entrant** et le déposer sur un compte d'attente, **geler sans délai les cryptoactifs** et informer de ces actions l'autorité nationale compétente pour la mise en œuvre des mesures restrictives pour instructions complémentaires
- **déclarer** les actifs gelés aux autorités nationales compétentes, sans tarder ou dans les délais prévus
- **signaler** toute suspicion de **contournement** ou de tentative de contournement des mesures restrictives à l'autorité nationale compétente pour la mise en œuvre de mesures restrictives ou à la CRF nationale si la législation applicable l'exige
- **régulièrement tester** les paramètres du système de filtrage (approprié / efficace: évaluer le calibrage, l'exactitude de la gestion des listes, le filtrage intégral des clients et des flux, l'adéquation et la pertinence des champs d'information utilisés, la rapidité de la suspension des opérations)
- **Signaler à l'organe de direction les faiblesses ou insuffisances** significatives du système de filtrage et adopter des **mesures correctives sans délai**

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

I. **État des lieux du déploiement de l'IA en matière de LCB-FT (Antonin Weiss)**

II. **Présentation et dernières évolutions de l'outil Lucia (Vincent Vasques)**

III. **Rapport sur la prévention des comptes rebond pour le blanchiment d'escroqueries et autres fraudes (Elodie Chanut)**

IV. **Orientations EBA sur les mesures restrictives (Sylvain Aubert)**

V. **Point d'étape sur la supervision du secteur des crypto-actifs (Aloïs Gareste)**

V. Point d'étape sur la supervision du secteur des crypto-actifs

LCB-FT : *POINTS D'ETAPE SUR LA SUPERVISION DU SECTEUR DES CRYPTO-ACTIFS*

I. **État du marché des crypto-actifs en France**

II. **Principaux points d'attention en matière de supervision des PSAN/PSCA**

III. **Principaux points d'attention en matière d'agrément des candidats PSCA**

I – ÉTAT DU MARCHÉ DES CRYPTO-ACTIFS EN FRANCE

ÉTAT DU MARCHÉ DES CRYPTO-ACTIFS EN FRANCE

❑ De PACTE à MiCA

- Depuis mars 2020, 117 prestataires de services sur actifs numériques (PSAN) ont été enregistrés conformément aux dispositions de la loi PACTE du 22 mai 2019, dont 23 PSAN européens n'ayant pas d'établissement en France.

- **Début 2025, 109 PSAN étaient toujours enregistrés, dont 89 supervisés en France**. La France est 5ème en nombre de PSAN parmi les États-membres de l'UE.

- Début octobre 2025, 5 prestataires de services sur crypto-actifs (PSCA) ont été agréés conformément aux dispositions du règlement MiCA, dont 3 disposaient de l'enregistrement PSAN. 20 dossiers d'agrément sont à divers stades d'instruction. A l'été 2025, elle était en 3ème position en nombre de PSCA, derrière l'Allemagne (12) et les Pays-Bas (11), à égalité avec Malte.

- L'ACPR est compétente sur le volet BC-FT.

ÉTAT DU MARCHÉ DES CRYPTO-ACTIFS EN FRANCE

❑ État de la menace

L'Analyse Nationale des Risques de 2023 a classé ce secteur comme présentant un risque très élevé. Le rapport de Tracfin sur l'état de la menace (septembre 2025) associe également les actifs numériques à un risque élevé et ils seraient **utilisés de manière croissante dans des schémas de BC-FT.**
Tracfin souligne que certains groupes terroristes affichent une utilisation quasi systématique des cryptoactifs dans leurs schémas de financement.

La problématique de la fraude fiscale se pose également, dans un contexte des plus-values latentes élevées suite à l'appréciation de certains crypto-actifs.

Pour mémoire, s'agissant des techniques d'anonymisation, l'article 79 du règlement UE 2024/1624, en vigueur depuis décembre 2024 dispose **: «** *Il est interdit aux établissements de crédit, aux établissements financiers et aux prestataires de services sur crypto-actifs de tenir des comptes bancaires et de paiement anonymes […] ainsi que tout autre type de compte permettant l'anonymisation du titulaire d'un compte client* ***ou l'anonymisation ou une opacification accrue des transactions, y compris par des jetons à anonymat renforcé.*** » Des dispositions ont été ajoutées dans la loi française en juin 2025 pour étendre la présomption de blanchiment à ce type de services.

❑ Retour sur le premier cycle de supervision depuis la fin de la période d'enregistrement PSAN

Conformément à **l'approche par les risques**, l'ACPR a eu recours à ses différents outils de supervision :

- Collecte d'informations sur l'activité et le dispositif LCB-FT
- Entretiens de surveillance rapprochée
- Visites ou contrôles sur place, en fonction des risques et du volume d'activité.

Une proportion significative des acteurs les plus risqués ou les plus actifs a ainsi fait l'objet de **visites ou contrôles sur place depuis 2022**. Pour de nombreux acteurs, ces contrôles étaient les premiers au sein de leurs établissements. Ils ont permis de mettre l'accent sur des points de faiblesse et les attentes de l'ACPR en matière de BC-FT.

En fonction de la sévérité des observations, les contrôles ont donné lieu à des lettres de suite ou de suivi, des mesures de police disciplinaire voire des radiations.

Les actions de remédiation font l'objet d'un suivi par le contrôle permanent afin de s'assurer de la mise en conformité des dispositifs LCB-FT. Au-delà, des contrôles sur place seront réalisés, conformément à l'approche par les risques de l'ACPR, pour vérifier les progrès réalisés et le bon fonctionnement des dispositifs.

II – PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE DE SUPERVISION DES PSAN/PSCA

PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE DE SUPERVISION DES PSCAN/PSCA

- **Gouvernance :** Les dirigeants et les organes de surveillance, quand ils existent, **ne disposent pas de toutes les informations pertinentes** pour s'assurer que l'entité se conforme à ses obligations en matière de LCB-FT.
- Les **ressources** dédiées au dispositif LCB-FT peuvent être sous-dimensionnées et la **formation** est également insuffisante. Pour aborder correctement les risques BC-FT, les personnes en charge doivent cumuler les compétences techniques sur les produits et également sur les schémas de blanchiment, de fraude fiscale ou de financement du terrorisme.
- **Classification des risques** : les classifications des risques de BC-FT en vigueur au moment des missions sont apparus **incomplètes** (non-prise en compte des facteurs de risques listés dans les principes d'application sectoriels - PAS), **insuffisamment actualisées** (en particulier pour l'évaluation du risque géographique) **et parfois inopérantes** sur le plan opérationnel du fait des problèmes de collecte et d'enregistrement des informations de connaissance clientèle.
- **Identification et vérification de l'identité** : des **insuffisances ont été régulièrement** identifiées, y compris pour les PSAN ayant recours à des prestataires spécialisés en la matière. Des cas d'usurpation d'identité ont ainsi été détectées par certaines missions.
- **Connaissance de la clientèle** : la connaissance de la clientèle ressort régulièrement comme insuffisantes, qu'il s'agisse des informations sur les revenus, le patrimoine, la localisation, les données financières pour les personnes morales ou la nature des activités envisagées; les procédures de vérification sur base documentaire sont régulièrement lacunaires. Des insuffisances ont également été identifiées en matière de définition et d'actualisation des profils de risque des clients, et partant des niveaux de vigilance associés.

PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE DE SUPERVISION DES PSCAN/PSCA

- Bien que rappelée dans les PAS de l'ACPR, la **surveillance des transactions en monnaie ayant cours légal n'est pas suffisamment assurée.**
- **La surveillance des transactions sur crypto-actifs**, réalisée par les PSAN à partir d'outils d'analyse transactionnelles (ci-après « OAT ») n'est pas suffisamment développée et encadrée (absence de déclinaison d'une politique de risque dans le paramétrage de l'OAT utilisée, procédures et modes opératoires insuffisamment précis, couverture partielle des actifs numériques par l'OAT utilisé). Certains établissements commercialisaient également des crypto-actifs non couverts par leur OAT ou par un autre outil de surveillance.
- La surveillance des transactions en crypto-actifs ne tient pas suffisamment compte du **profil de risque des clients**, des informations de connaissance clientèle et les analyses rétrospectives ne sont pas réalisées sur les transactions (ce qui est fondamental pour identifier les wallets exposés à des entités sanctionnées ou liés à des problématiques de FT).
- **Activité déclarative : le contenu, la qualité des DS ou les délais de transmission sont parfois insuffisantes,** en lien **notamment avec l'insuffisance des ressources ou les défaillances du dispositif de surveillance des opérations.**
- **Contrôle interne:** les dispositifs de contrôle permanent et périodiques sont souvent **embryonnaires** et le contrôle interne ne peut jouer son rôle de force de rappel.

PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE DE SUPERVISION DES PSCAN/PSCA

❑ Bonnes pratiques relevées à l'occasion des visites et contrôles sur place

- **Actualiser régulièrement les procédures afin qu'elles reflètent les mesures effectivement mises en œuvre** pour maîtriser les risques de BC-FT auxquels l'établissement est exposé **en fonction des variations de son activité** en matière de produits ou services offerts mais également de caractéristiques des clients et **de typologies de BC-FT observées** : usurpations d'identité, fraudes, usage de blockchains nouvelles pour lesquelles le mapping des OAT est moins développé que celui des blockchains classiques...

- **Mettre en place un reporting régulier d'indicateurs pertinents à l'attention des dirigeants et/ou de l'organe de surveillance :** panier moyen des opérations (général et concernant les opérations à risque) ; nombre d'alertes global (à comparer au nombre d'opérations) et pour chaque scénario d'alerte, avec le taux de transformation en ER puis en DS afin de repérer les scénarios plus ou moins efficaces ; délais de détection, de traitement et de signalement des opérations, nombre de cas détectés avant l'exécution de l'opération.

- **Mettre en place des scénarios bloquants ou des autorisations préalables** : par exemple, si un client n'a pas transmis toutes les informations requises à l'entrée en relation, s'il présente des critères présageant d'une usurpation d'identité, s'il tente d'effectuer une opération d'un montant incohérent avec sa situation financière connue.

- **Mettre en place des revues portant sur les stocks et pas seulement sur les flux** : plan de remédiation KYC, recherche d'opérations passées similaires aux cas de défaut d'ER ou de DS identifiés par la mission de contrôle sur place. Ces mesures doivent être mises en œuvre sans attendre les suites décidées par le SGACPR.

III – POINTS D'ATTENTION EN MATIÈRE D'AGRÉMENT DES CANDIDATS PSCA

PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE D'AGRÉMENT DES CANDIDATS PSCA

➢ Principaux compléments de la procédure d'agrément PSCA par rapport à l'enregistrement PSAN sur le volet LCB-FT

Les PSAN déjà enregistrés intègrent généralement mieux les éléments du dispositif LCB-FT déjà exigés, qui doivent toutefois être actualisés en fonction du développement de l'activité (ex : classification des risques, description opérationnelle des scénarios d'alertes mis en place dans le cadre du dispositif de surveillance des opérations).

Outre les exigences supplémentaires non liées à la LCB-FT (cybersécurité, exigences prudentielles**…), les dossiers d'agrément PSCA incluent de nouveaux volets liés à la LCB-FT :**

- **Mesures de vigilances complémentaires, notamment à l'égard des PPE.** Ces éléments sont généralement décrits de manière détaillée et opérationnelle.

- **Mesures répondant aux obligations en matière de transfert de fonds.** La qualité de ces éléments est plus variable selon les dossiers, certaines procédures n'étant pas assez détaillées (elles rappellent les obligations applicables mais ne décrivent pas de manière suffisamment opérationnelles les mesures mises en œuvre pour s'y conformer).

- **Dispositif de contrôle interne.** Les plans de contrôle interne sont souvent insuffisamment développés, y compris dans les dossiers déposés par des PSAN déjà enregistrés.

PRINCIPAUX POINTS D'ATTENTION EN MATIÈRE D'AGRÉMENT DES CANDIDATS PSCA

➢ Principaux axes d'amélioration identifiés à l'occasion des demandes d'agrément :

- **Classification des risques** : En écho aux constats des contrôles sur place, les classifications des risques sont **parfois incomplètes (principalement les nouveaux candidats) ou insuffisamment actualisées (certains PSAN pré-enregistrés)**. Tous les services, produits et jetons offerts par les candidats PSCA doivent être intégrés, et signalés à l'ACPR par l'intermédiaire du QLB annuel après l'enregistrement PSAN ou l'agrément PSCA.

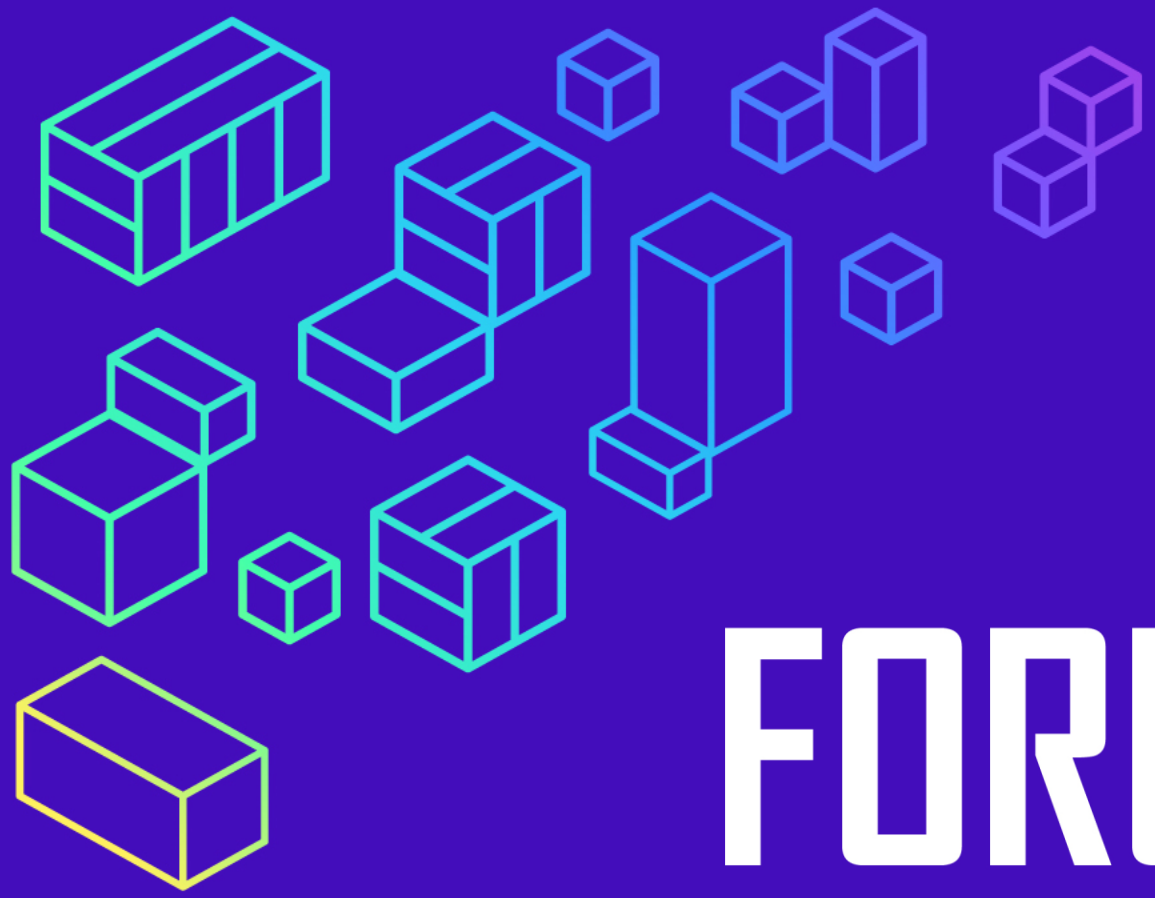
- **Le dispositif de surveillance des opérations et les scénarios d'alertes doivent être décrits de manière détaillée et opérationnelle** et mis en relation avec la classification des risques et le dispositif de connaissance clientèle : l'établissement doit indiquer quels critères sont utilisés pour chaque scénario afin de générer une alerte, et les conséquences en matière de notation du risque présenté par le client et de mesures de vigilance mises en œuvre à son égard (demandes d'informations ou de justificatifs supplémentaires par exemple).

- **Les plans de contrôle interne** doivent également être opérationnels et détailler la nature des contrôles (ex : échantillonnage), les personnes en charge des contrôles, la périodicité…

ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

QUESTIONS ?



ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

FORUM FINTECH

ACPR - AMF

9 octobre 2025

French FinTech Weeks