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

16 octobre 2023

Intervenants

- **Sylvain Aubert**, AMF
- **Yvan Bazouni**, ACPR
- **Stéphane Mahieu**, ACPR
- **Jocelyn Lelong**, ACPR
- **Vincent Vasques**, ACPR

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

I. **Analyse sectorielle des risques de blanchiment des capitaux et de financement du terrorisme (BC-FT)**

II. **Point d'actualité : Orientations de l'EBA relatives aux solutions d'entrée en relation d'affaires à distance**

III. **Point d'actualité : IFP – TFR – AML6**

IV. **LCB-FT : retour d'expérience sur l'utilisation des outils de surveillance**

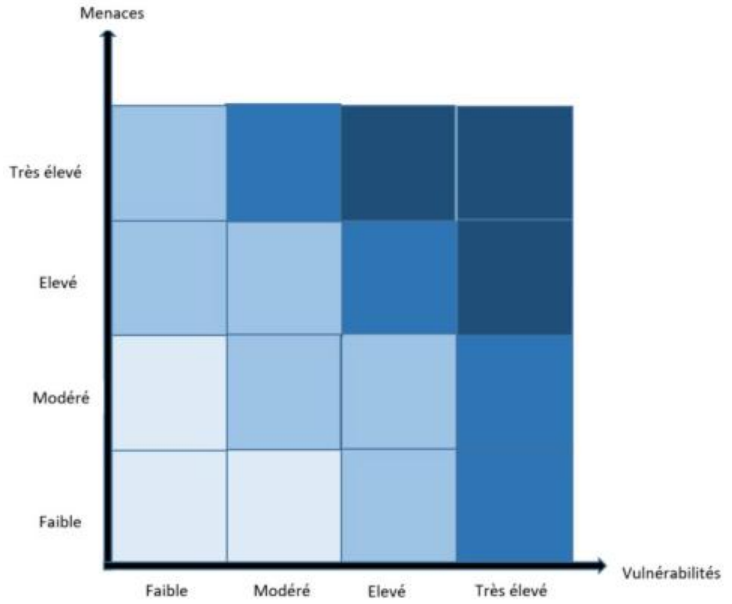
I. Analyse sectorielle des risques de blanchiment des capitaux et de financement du terrorisme (BC-FT)

OBJECTIFS DES ANALYSES NATIONALES ET SECTORIELLES DE BC-FT

- L'analyse nationale des risques de BC-FT (ANR) est prévue par l'article L. 561-4-1 du CMF et l'article L. 561-36 prévoit également que les autorités de contrôle veillent à disposer d'une **bonne compréhension des risques de BC-FT**
  - Dernière version de l'ANR publiée le 14 février 2023 ; la précédente version datait de septembre 2019
  - Première Analyse Sectorielle des Risques de BC-FT (ASR) de l'ACPR publiée en décembre 2019, nouvelle version juin 2023
  - L'ANR et l'ASR sont complémentaires et ont été préparées en parallèle.
- **Les organismes financiers doivent en tenir compte pour l'identification et l'évaluation de leurs propres risques** de BC-FT
  - L' ASR précise, comme le faisait la version de 2019, que les organismes financiers n'ont pas à adopter telles quelles l'ANR et l'ASR
  - Ils peuvent considérer qu'une activité qu'ils conduisent présente un niveau de risque différent (sauf risque élevé imposé par la réglementation)

MÉTHODOLOGIE DE L'ASR LCB-FT: CROISEMENT DES MENACES ET DES VULNÉRABILITÉS DANS UNE MATRICE

- **Principales menaces identifiées dans l'ANR**
  - fraudes fiscales, sociales et douanières
  - trafic de stupéfiants
  - escroqueries et vols.
  - trafic d'êtres humains
  - corruption et les atteintes à la probité
  - FT : principalement micro-financement
- **Travaux fondés sur**
  - Des statistiques (poursuites, condamnations, saisies, déclarations de soupçon, …)
  - Des analyses qualitatives (typologies, retours d'expérience, …)



Analyse des vulnérabilités intrinsèques de chaque secteur

- Possibilité d'anonymat/opacification
- Présence d'espèces
- Vulnérabilités transfrontalières
- Rapidité
- Complexité/accessibilité du produit

- **Le caractère adapté des mesures d'atténuation aux menaces et aux vulnérabilités intrinsèques permet d'évaluer la vulnérabilité résiduelle**
  - Réglementation LCB-FT
  - Autres réglementations (ex : fiscale)
  - Actions de contrôle et de sensibilisation
  - Bonnes pratiques des organismes
- **Travaux fondés notamment sur les évaluations individuelles des OF**
  - Questionnaires, rapports de contrôle interne
  - Informations de Tracfin, signalements
  - Contrôles, visites sur place, entretiens, revues thématiques

PROBLÉMATIQUES HORIZONTALES EXAMINÉES PAR 6 ATELIERS ET DÉCRITES DANS L'ASR 2023

- **corruption**
  - travaux de l'Agence Française Anticorruption (analyse de risque nov. 2022)
  - ne se limite pas aux personnes politiquement exposées ;
- risque de **prolifération** des armes de destruction massive
  - renforcement des exigences du GAFI dans ce domaine
  - publication d'une Analyse nationale du risque de prolifération
  - Focus ACPR: blanchiment du produit des infractions associées ;
- **criminalité environnementale**,
  - publication d'une analyse des risques nationale sur ce thème ;
- risque de **fraude**,
  - forte hausse des fraudes aux moyens de paiement ces dernières années,
  - fraude aux finances publiques ;
- les **produits favorisant l'anonymat**, espèces, monnaie électronique anonyme, l'or et les actifs numériques, certains usages abusifs de produits en principe traçables (chèques sans mention de bénéficiaire, cartes de paiement étrangères, IBAN virtuels) ;
- la **cybercriminalité**, notamment les rançongiciels.

ILLUSTRATION DES ASPECTS STATISTIQUES DE L'ÉVALUATION

- Les saisies visent de manière prédominante les espèces et les comptes :

Biens non immobiliers saisis							
	Numéraire	Comptes bancaires	Assurance-vie/ins-truments financiers	Créances	Parts de sociétés	Actifs numériques	Total
2020	89,5%	8,5%	1,6%	0,3%	0,0%	0,1%	100%
2021	87,6%	10,3%	1,6%	0,3%	0,0%	0,2%	100%

- L'accessibilité de ces produits participe à leur vulnérabilité au risque de BC-FT :

	Numéraire	Comptes bancaires et de paiement	Assurance-vie	Instruments financiers	Actifs numériques
2021	100%	99%	41%	16%	6%

- La perception des acteurs eux-mêmes, via la proportion de flux suspects déclarés à Tracfin indique le caractère plus risqué des EP, EME, PSAN et changeurs :

Proportion de flux suspects (2021)								
	EC	OA	EP	EME	EI-SGP	PSAN	IFP	Chan-geurs
% des DS du secteur financier	47,2%	4,3%	44,6%	2,0%	0,3%	0,2%	0,4%	0,5%
Enjeux (en millions d'euros)	28 200	1 139	3 087	740	-	164	4	59
Flux (en milliards d'euros)	42 000	471,5	237,2	16,5	-	2,3	1,88	0,716
Enjeux/flux	0,1%	0,2%	1,3%	4,5%	-	7,1%	0,2%	8,2%

- Cela est confirmé par la fréquence des défauts de déclaration de soupçon :

Nombre moyen de défauts de déclaration de soupçon (DS) par contrôle sur place (2020-2021)					
	EP/EME	EC	OA	Changeurs	EI
Nombre moyen de défauts de DS	23,7	18,1	11,4	4,0	2,5

COMPARAISON DES COTATIONS ACPR 2019 ET 2023

Légende : Risque très élevé | Risque élevé | Risque modéré | Risque faible

	Faible	Modérée	Elevée
	Banque de détail	Gestion de fortune Crédits à la consommation (FT) Monnaie électronique Transmission de fonds Changeurs manuels	Établissements de paiement hors transmission de fonds
	Correspondance bancaire UE/EEE Crédits à la consommation Leasing Affacturage Financement de l'immobilier Services d'investissement	Crédit aux entreprises BFI Financement du commerce international Correspondance bancaire hors EEE Actifs numériques Assurance-vie et contrats de capitalisation	Intermédiaires en financement participatif
	Cautions et nantissements IOBSP Assurance non-vie Intermédiaires d'assurance		

Menace \ Vulnérabilité	Faible	Modérée	Elevée	Très élevée
Très élevée		Change	- Actifs numériques - Transmission de fonds	
Elevée		- Banque de détail - Correspondance bancaire intra-UE - Assurance rançon	- IFP - Établissement de paiement - Gestion de fortune - Crédit conso (FT) - Correspondance bancaire hors UE	Monnaie électronique
Modérée	- Leasing - Affacturage	- Services d'investissement (BC) - BFI et crédits aux entreprises (BC) - Trade finance - Assurance-vie - Crédit immo luxe - Courtiers assur. vie	Crédit conso (BC)	
Faible	- Cautionnement et nantissement - Certains leasings - Crédit immobilier (hors luxe) - Courtiers OBSP et d'assurance (hors vie)	- Activités de crédit hors conso - BFI et crédits aux entreprises (FT) - Services d'investissement (FT) - Assurance non-vie (hors rançon)		

- Outre le passage à 4 niveaux de cotation, les principaux changements sont des hausses du niveau de risque global:
  - de modéré à très élevé pour les **actifs numériques**
  - d'élevé à très élevé pour la **transmission de fonds** et la **monnaie électronique**
  - de modéré à élevé pour **la banque de correspondance en dehors de l'EEE**
  - de faible à modéré pour le **crédit à la consommation** et les **services d'investissement**, ainsi que pour la **banque de correspondance dans l'EEE**

FOCUS SUR LE RISQUE DE FRAUDE

- L'escroquerie est l'un des principales menaces identifiée dans l'ASR.
  - De nombreuses escroqueries et fraudes aux finances publiques impliquent l'utilisation d'un compte pour blanchir le produit de l'infraction
  - Le montant des fraudes aux virements a été multiplié par 10 de 2016 à 2022 (313 millions en 2022)
- La réception du produit des fraudes aux virements est concentrée sur quelques établissements
  - 10 établissements français et étrangers reçoivent 60% du montant des virements frauduleux déclarés dans une collecte de données par la Banque de France portant sur l'année 2022 et couvrant l'essentiel du marché français.
  - Alors que pour les grands groupes français, les virements frauduleux représentent en général entre 0,001% et 0,0001 % des montants reçus, une dizaine d'établissements ont des taux proches ou supérieurs à 0,1%
- Les principaux destinataires de virements frauduleux partagent souvent les caractéristiques suivantes:
  - Prestataires en ligne: au moins 35% du montant
  - Établissements récents ou ouvrant beaucoup de comptes: environ 50% du montant
  - Etablissements offrant des IBAN virtuels avec des codes pays ou établissements différents: plus de 20% du montant

MESURES PRISES CONTRE LES PRINCIPAUX ÉTABLISSEMENTS DESTINATAIRES DE VIREMENTS FRAUDULEUX

- Concernant les 10 principaux établissements identifiés lors de l'exercice précédent:
  - Deux ont fait l'objet de contrôles suivis de sanctions disciplinaires par l'ACPR pour la LCB-FT
  - Un a fait l'objet de contrôles suivis d'une mise en demeure ou de demandes de mesures correctives; une suspension de l'ouverture de certains nouveaux comptes
  - 4 établissements étrangers, dont un pour lequel l'ACPR a effectué un contrôle sur place, et 2 soumis à sanctions ou mesures restrictives dans leur pays d'origine
  - 3 établissements interrogés par l'ACPR
- Données 2023 sur année 2022:
  - Analyse encore en cours par l'ACPR
  - Un établissement sanctionné, une procédure disciplinaire en cours, une autre probable
  - Questionnaire et contacts avec superviseurs étrangers prévus

RISQUE DE FRAUDE ET D'USURPATION D'IDENTITÉ

- L'ASR appelle l'attention sur plusieurs points de vulnérabilités en matière de vérification d'identité:
  - Les **copies de pièces d'identité** peuvent être aisément obtenues (détournement de dossiers de location, …) ou falsifiées
  - Vérification insuffisante de ce que le **premier paiement** à partir d'un compte tenu dans l'EEE provient bien d'un compte appartenant à la personne dont il s'agit de vérifier l'identité (paiement par cartes ne permettant pas de confirmation robuste de l'identité du porteur, ou utilisation de cartes rattachées à un porte monnaie électronique)
  - Insuffisante attention au risque que l'autre compte ait lui-même pu être obtenu à la suite d'une fraude (en cas de mesures publiques, ou connaissance d'un taux de fraude élevé) ou qu'il provienne d'un compte dans un pays permettant un différé de vérification d'identité
  - Insuffisante attention portée à l'ouverture de comptes de personnes morales, notamment à distance, et à la **vérification de l'identité et des pouvoirs du représentant**
- Les bonnes pratiques mise en avant dans l'ASR:
  - Utilisation des PVID certifiés par l'ANSSI (preuves du vivant, analyse documentaire)
  - Vigilance sur les opérations, notamment des nouveaux clients, pour détecter des opérations non conforme au profil attendu – ce qui nécessite de définir ce profil avec suffisamment de précision (pas seulement un montant total: montant et fréquence des opérations unitaires, origine et destination, vélocité , lieu de connection…)

II. Point d'actualité : Orientations de l'EBA relatives aux solutions d'entrée en relation d'affaires à distance

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE


Orientations

EBA/GL/2022/15

22/11/2022

sur l'utilisation de solutions d'entrée en relation d'affaires à distance conformément à l'article 13, paragraphe 1, de la directive (UE) 2015/849

Date de publication	22 novembre 2022
Date de publication (FR)	31 mars 2023
Date de publication (FR) **Version corrigée**	1er août 2023
Date d'application	**2 octobre 2023**

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

- **Obligations concernées (Directive (UE) 2015/849)**

  - **Article 13(1)(a) à (c)** : obligations d'identification et de vérification de l'identité du client et du bénéficiaire effectif ; évaluation de l'objet et de la nature envisagée de la relation d'affaires
  - **Chapitre II, section 4** : recours à des tiers pour l'exécution des obligations de vigilance à l'égard de la clientèle prévues
  - **Article 8 (3) et (4)(a)** : politiques, contrôles et procédures pour atténuer et gérer efficacement les risques BC-FT identifiés aux niveaux UE, national et entité

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

- **Objet**
  - Préciser les mesures que les établissements financiers doivent prendre lorsqu'ils :
    - **Décident d'adopter** ou **examinent** des outils d'entrée en relation d'affaires à distance avec de **nouveaux clients**, notamment par internet
    - **Evaluent l'adéquation et la fiabilité de ces outils**, afin de se conformer efficacement à leurs obligations LCB-FT
  - Renforcer la fiabilité de la vérification d'identité : promotion de bonnes pratiques visant à mieux contrôler l'authenticité et l'intégrité des documents d'identité fournis et à s'assurer que le client est le titulaire réel de ces documents (et non l'auteur d'une usurpation d'identité)
  - Les Orientations (de « ***nature non-contraignante*** ») n'introduisent pas de nouvelles exigences mais clarifient comment les exigences existantes s'appliquent dans un contexte d'entrée en relation à distance

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

1.	Politiques et procédures internes
2.	Obtention des informations
3.	Authenticité et intégrité des documents
4.	Mise en correspondance de l'identité du client dans le cadre du processus de vérification
5.	Recours à des tiers et à l'externalisation
6.	Gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité
7.	Recours à des services de confiance et à des processus d'identification nationaux

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

1.	**Politiques et procédures internes**

- Adaptées aux risques, incluant notamment une description générale (i) de la solution utilisée pour recueillir, vérifier et enregistrer les informations et (ii) des situations dans lesquelles elle peut être utilisée
- **Elaboration sous la responsabilité du responsable du respect de la conformité en matière de LCB-FT** (veille à leur mise en œuvre efficace, à leur examen régulier et à leur modification)
- **Approbation par l'organe de direction** (veille à leur bonne application)
- **Evaluation préalable de la solution** avant mise en œuvre (adéquation, exhaustivité et exactitude des données à recueillir ; incidence en termes de risque ; test d'évaluation des risques de fraude)*
- **Suivi permanent** de la solution : vérification du fonctionnement conforme aux attentes (en précisant les mesures assurant la qualité, l'exhaustivité, le caractère adéquat et l'exactitude des données recueillies, l'étendue et la fréquence des examens réguliers, et les circonstances devant déclencher un examen ponctuel ou la mise en œuvre de mesures correctrices)

***Conformité présumée** si recours à des services de confiance ou à des processus d'identification nationaux (cf. 4.7)

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

2.	Obtention des informations

- Nécessité de **définir les informations nécessaires à l'identification** du client et les **types de documents, données ou informations utilisés pour vérifier son identité** et la manière dont ces informations seront vérifiées, en tenant notamment compte du fait que le client est une personne physique ou une personne morale
- Nécessité de **s'assurer que les informations obtenues sont à jour et adaptées** pour satisfaire aux exigences applicables et que les données sont enregistrés dans un **format lisible et de qualité suffisante** pour reconnaître clairement le client*

***Conformité présumée** si recours à des services de confiance ou à des processus d'identification nationaux (cf. 7)

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

3.	**Authenticité et intégrité des documents**

- Lorsque la copie d'un document original est acceptée sans procéder à la vérification du document original, des mesures doivent être mises en place afin de **vérifier que la reproduction est fiable**
- Vérification que les caractéristiques de sécurité intégrées au document original et que les spécifications du document original en cours de reproduction sont valables et acceptables (en les comparant avec des bases de données officielles, telles que PRADO-*Public Register of Authentic identity and travel Documents Online*)

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

4. Mise en correspondance de l'identité dans le cadre du processus de vérification

- Intégration a minima de certains éléments*
  - Pers. Phys. (PP) : correspondance entre informations visibles de la personne physique et documents fournis
  - Pers. Morale (PM) : inscription dans un registre public et habilitation d'une PP à agir en son nom
- Si données biométriques : suffisamment uniques pour être associées sans équivoque à une seule PP*
- Algorithmes vérifiant la correspondance entre données biométriques de la pièce d'identité transmise et le client*
- Si justificatif de qualité insuffisante : interruption, redémarrage ou réorientation vers vérification en physique*
- Vérifications d'intensité variable : solutions automatisées (*eg* tests de vérification du vivant) ou non (guide d'entrevue…)*
- Ordre aléatoire des actions du client et des tâches des employés
- Mesures supplémentaires pour accroitre la fiabilité de la vérification (§44)

* **Conformité présumée** si recours à des services de confiance ou à des processus d'identification nationaux (cf. 7)

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

5.	Recours à des tiers et à l'externalisation

- Préciser l'allocation des fonctions/activités exécutées ou réalisées (assujetti/tiers/prestataire externe)
- Prendre les mesures nécessaires pour s'assurer que les processus et procédures mis en œuvre par le tiers sont conformes aux exigences des Orientations (e.g. rapports réguliers, suivi continu, visites sur place ou analyse d'échantillons ; évaluation des moyens et capacités du prestataire)

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

6.	Gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité

- **Identifier et gérer les risques TIC/sécurité** relatifs à l'utilisation du processus d'entrée en relation d'affaires à distance (y compris en cas d'externalisation)
- Utiliser des **canaux de communication sécurisés** pour interagir avec le client pendant le processus d'entrée en relation d'affaires à distance

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

Contenu

7. Services de confiance et processus d'identification nationaux

- Possibilité de recourir à des **services de confiance** et à des **processus d'identification électronique** réglementés, reconnus, approuvés ou acceptés nationalement :
  - Solutions qui ont fait l'objet d'une certification « eIDAS », délivrée notamment par l'ANSSI (par ex. l'Identité numérique de La Poste ou prestataires de signatures électroniques)
  - Solutions certifiées au plan national, telles que celles des prestataires de vérification d'identité à distance (PVID)
- Dans ce cas, nécessité **d'évaluer** dans quelle mesure la solution respecte les orientations et **d'appliquer les mesures nécessaires pour atténuer tout risque** pertinent découlant du recours à ces solutions (notamment risques liés à l'authentification, en particulier les risques de fraude à l'identité, d'usurpation, de perte, de vol, de suspension, de nullité ou d'expiration d'un justificatif d'identité.)
- **Conformité présumée aux § 14(a), (d) et (e), 25 et 38 à 43 des Orientations**

ORIENTATIONS EBA - SOLUTIONS D'ENTRÉE EN RELATION D'AFFAIRES À DISTANCE

- **Mise en œuvre**
  - **AMF**
    - Position 2023-07
    - Position-recommandation 2019-16 (lignes directrices sur les obligations de vigilance à l'égard des clients) modifiée
    - Application aux acteurs supervisés par l'AMF en matière de LCB-FT (CMF, L.561-36, I, 2°)
  - **ACPR**
    - Avis du 09/06/2023 relatif à la mise en œuvre des orientations
    - Application à l'ensemble des organismes relevant de la supervision de l'ACPR

III. Point d'actualité : IFP – TFR – AML6

POINT D'ACTUALITÉ : FOCUS SUR LES IFP

Rappel du cadre juridique

Principaux points d'attention en matière de LCB-FT :

- Classification des risques;
- Obligations de KYC à l'égard :
  - des porteurs de projet ;
  - des contributeurs en relation d'affaires.
- Formation
- Obligations en matière de gel des avoirs/interdiction de mise à disposition de fonds
- Les perspectives d'AML6

POINT D'ACTUALITÉ : LE RÈGLEMENT TRANSFERT DE FONDS (TFR)

Pour le CASP du donneur d'ordre (art. 14)

- Transmission d'informations sur le DO et sur le bénéficiaire par le CASP du DO dès 0 euro
  - *Informations requises sur le DO, notamment :*
    - *nom du DO ;*
    - *adresse publique / numéro de compte de crypto-actifs du DO ;*
    - *adresse / numéro de document officiel ou date et lieu de naissance du DO*
    - *Identifiant d'entité juridique si disponible*
  - *Informations requises sur le bénéficiaire :*
    - *nom du bénéficiaire ;*
    - *adresse publique / numéro de compte de crypto-actifs du bénéficiaire ;*
    - ***Identifiant d'entité juridique si disponible***
  - *Transmission de ces informations au CASP du bénéficiaire*
- Vérification de l'exactitude des informations sur le DO
- Transmission des informations avant, simultanément ou en parallèle du transfert sans être nécessairement jointes au/incluses dans le transfert

Pour le CASP du bénéficiaire (art. 16 et 17)

- Procédure efficace, notamment un contrôle après ou pendant le transfert, pour s'assurer que les informations accompagnant le transfert sont incluses dans/suivent le transfert
- Vérification de l'exactitude des informations sur le bénéficiaire
- Approche par les risques pour évaluer l'opportunité d'effectuer, rejeter, renvoyer ou suspendre le transfert en cas d'informations incomplètes
- En cas de répétition de transmission d'informations incomplètes, mesures pouvant aller jusqu'au rejet des transferts ou restriction/cessation de la relation d'affaires

Transferts depuis/vers une adresse auto-hébergée

- Obligation pour le CASP de recueillir les informations sur le DO/bénéficiaire du transfert
- Pour tout transfert > 1000€, mesures appropriées pour déterminer si l'adresse est contrôlée ou possédée par le DO/bénéficiaire
- Mesures d'atténuation des risques de BC-FT des transferts depuis/vers une adresse auto-hébergée

POINT D'ACTUALITÉ : LES ÉVOLUTION LIÉES À TFR - MODIFICATION DE AMLD5 ET ORIENTATIONS ABE

- AMLD5 étendue à toutes les catégories de CASPs définies par MiCA et fait entrer les CASPs parmi les entités assujetties dans la catégorie des établissements financiers.

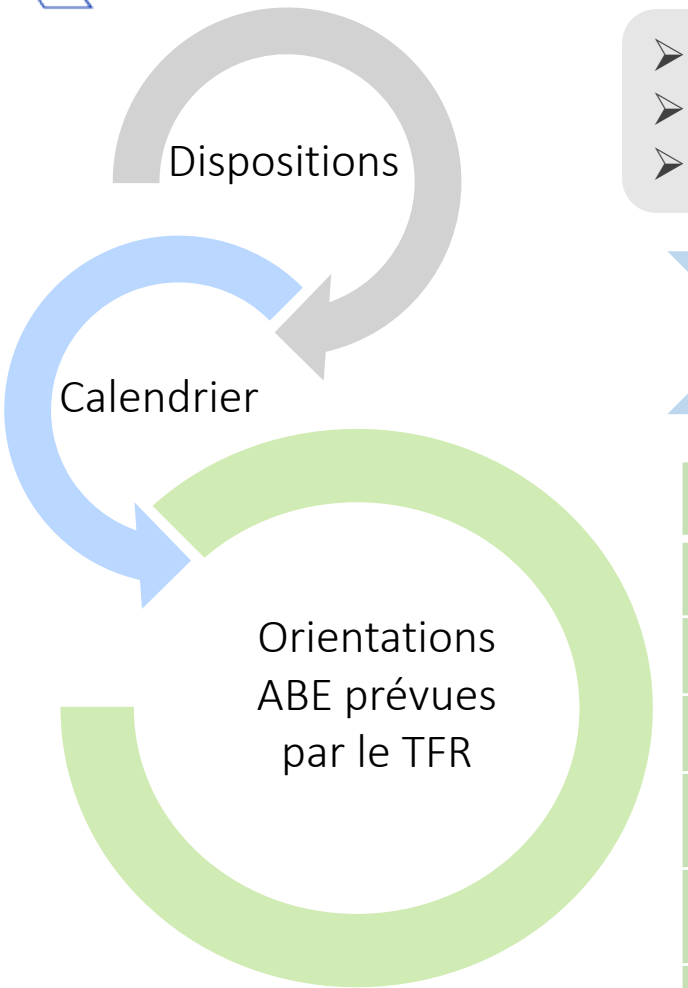
- Introduit les mesures d'atténuation des risques posés par les transferts depuis/vers les adresses auto-hébergées (art. 38, 4) :
  - politiques, procédures et contrôles internes pour évaluer les risques de BC-FT posés par ces adresses ;
  - mesures de vigilance selon une approche par les risques, notamment :
    - renseignements supplémentaires exigés sur l'origine et destination des crypto-actifs ;
    - surveillance renforcée des opérations.

- Prévoit des mesures de vigilance renforcées et d'atténuation des risques pour les relations de correspondance entre CASPs (art. 38, 4), en déterminant notamment si l'entité cliente est enregistrée ou agréée.

- Prévoit les orientations de l'ABE sur :
  - l'application de la Travel rule aux transferts de crypto-actifs :
    - nature des informations requises et mesures de vigilance attendues des CASPs pour s'assurer de la bonne transmission des informations ;
    - consultation publique pour une durée de 3 mois à venir.
  - les facteurs de risque : un chapitre dédié aux CASPs
    - aider les organismes financiers à identifier des facteurs de risque pour associer un niveau de risque à chaque relation d'affaires ;
    - consultation publique conduite entre le 31 mai et le 31 août 2023 ;
    - rappelle que les actifs numériques sont porteurs de risques spécifiques (anonymat facilité par les portefeuilles confidentiels et les services de mixage ou de brassage) et la nécessité de se former au paramétrage et à l'utilisation d'un OAT pour le suivi des transactions.
  - les mesures restrictives.

- Transposition de AMLD5 modifiée au plus tard au 30 décembre 2024

POINT D'ACTUALITÉ : TFR – SYNTHÈSE



- Extension de la *travel rule* aux transferts de crypto-actifs
- Renforcement des mesures de vigilance
- Précisions sur la mise en œuvre des mesures restrictives

31/05/23
Signature de TFR

9 Juin 2023
Publication au JOUE

29 Juin 2023
Entrée en vigueur

30 décembre 2024
Entrée en application

Orientations	Dates d'adoption
Application du TFR aux crypto-actifs	30 juin 2024
Régime de correspondances entre CASPs	30 juin 2024
Application des mesures restrictives	30 décembre 2024
Règles de protection des données et transferts de crypto-actifs (ABE et EDPB)	Mandat confié au Comité européen de la protection des données
Transferts en provenance ou à destination d'une adresse auto-hébergée	30 décembre 2024
Variables et facteurs de risques concernant les crypto-actifs	30 décembre 2024
Mesures de vigilance renforcée sur le DO/bénéficiaire d'un transfert de crypto-actifs	1er janvier 2024

POINT D'ACTUALITÉ : LE VOLET RÉGLEMENTAIRE DU PAQUET AML6

- **Un nouveau règlement :**
  - reprend une partie des dispositions figurant actuellement dans la directive « anti-blanchiment »
  - définit les obligations applicables aux entités assujetties, qui sont précisées, le cas échéant, par des règlements de la Commission européenne élaborés par l'AMLA
- **Une directive anti-blanchiment révisée :**
  - porte notamment sur les missions des superviseurs nationaux et des cellules de renseignement financier et leurs échanges d'information
- Calendrier :
  - Trilogues en cours
  - Objectif : adoption avant le printemps.

POINT D'ACTUALITÉ : LE VOLET RÉGLEMENTAIRE DU PAQUET AML6

- **Vers un renforcement et une harmonisation de la réglementation anti-blanchiment**
- Des précisions sur le champ d'application du dispositif :
  - un champ d'application élargie
  - des précisions sur l'autorité compétente pour superviser les organismes exerçant leur activité au moyen du passeport européen
- Un renforcement et une harmonisation du droit UE en matière de :
  - vigilance à l'égard de la clientèle
  - d'obligation de déclaration de soupçon, définie en des termes plus larges
  - d'organisation du dispositif LCB-FT, y compris en matière d'externalisation
  - Attention particulière du Parlement européen aux sujets liés aux crypto-actifs.

IV. LCB-FT : retour d'expérience sur l'utilisation des outils de surveillance

LCB-FT : RETOUR D'EXPÉRIENCE SUR L'UTILISATION DES OUTILS DE SURVEILLANCE

I. CONTEXTE

II. APPORTS, ENSEIGNEMENTS ET PERSPECTIVES DES OUTILS DE SURVEILLANCE

a) L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA LCB-FT

b) DÉCLINAISON DES TYPOLOGIES DE BC-FT

III. CONCLUSION : DE L'IMPORTANCE D'UNE APPROCHE PAR LES RISQUES

I. CONTEXTE

- La surveillance des opérations joue un rôle crucial dans les dispositifs de LCB-FT des établissements assujettis. Chaque opération est un « signal » porteur d'informations (montant, date, nature d'opération, compte client/contrepartie, dénominations, motif, localisation …) à mettre en regard des informations de connaissance clientèle.

- Les établissements ont l'obligation de recueillir, en fonction d'une approche par les risques, les informations de connaissance clientèle pour l'exercice de la vigilance constante. Toutefois, on observe que les dispositifs de surveillance reposent en général sur des systèmes d'alertes qui n'exploitent que partiellement ces informations et présentent des capacités limitées d'analyse notamment pour identifier certains comportements atypiques. L'identification des opérations atypiques doit amener l'établissement à réaliser un examen renforcé et le cas échéant à transmettre une déclaration de soupçon à TRACFIN.

- La conformité et l'efficacité des dispositifs de LCB-FT sont évaluées lors des missions de contrôle sur place, d'un point de vue organisationnel et procédural mais également d'un point de vue opérationnel. La mise en œuvre des obligations de connaissance clientèle, la pertinence de la classification des risques de BC-FT et sa mise en œuvre ainsi que l'ensemble du dispositif déclaratif font l'objet de contrôles approfondis (analyse des forces et faiblesses du dispositif, identification des éventuels défauts d'examen renforcé et défauts de déclarations de soupçons).

II. APPORTS, ENSEIGNEMENTS ET PERSPECTIVES DES OUTILS DE SURVEILLANCE

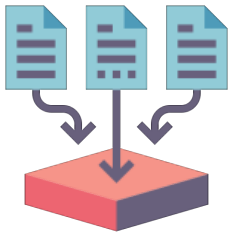
- L'évolution récente des solutions techniques permet une exploitation plus performante des données grâce à (i) des infrastructures de stockage et de calcul plus puissantes et (ii) des méthodes de traitement et des algorithmes plus avancés.

- **LUCIA** (**L**ogiciel à l'**U**sage du **C**ontrôle assisté par l'**I**ntelligence **A**rtificielle) est un **outil Suptech développé par l'ACPR et la BDF** au service des missions de contrôle sur place qui :

  - met en œuvre des **algorithmes de *data mining*** et de ***machine learning*** **pour extraire des signaux faibles** à partir des données d'opérations et de connaissance client collectées dans le cadre des investigations
  - restitue visuellement l'information sous la forme d'une **cartographie intelligente des risques** en groupant automatiquement les clients par profils types de risque
  - permet d'**investiguer les dossiers individuels en mettant en exergue les faits saillants de risque** des clients et donnant accès à un relevé d'opérations enrichi
  - facilite l'analyse de l'environnement économique du client en construisant des **modèles de graphes relationnels**

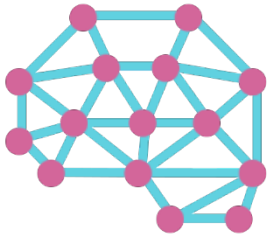
LA SOLUTION LUCIA

Intégration de référentiels de risque ad hoc (typologie de contreparties, listes pays …)



Mise en forme des données collectées auprès de l'établissement (KYC, opérations …)

Enrichissement des données brutes, calcul des agrégats et des métriques de risque



Segmentation du portefeuille par profils types et modélisation des liens entre clients par graphes

Restitution des résultats dans l'interface pour investigation

Fonctionnalités de filtrage et de recherche avancées, mise en exergue des profils de risque, visualisation des liens entre clients

Préparation | Ingestion | Investigation

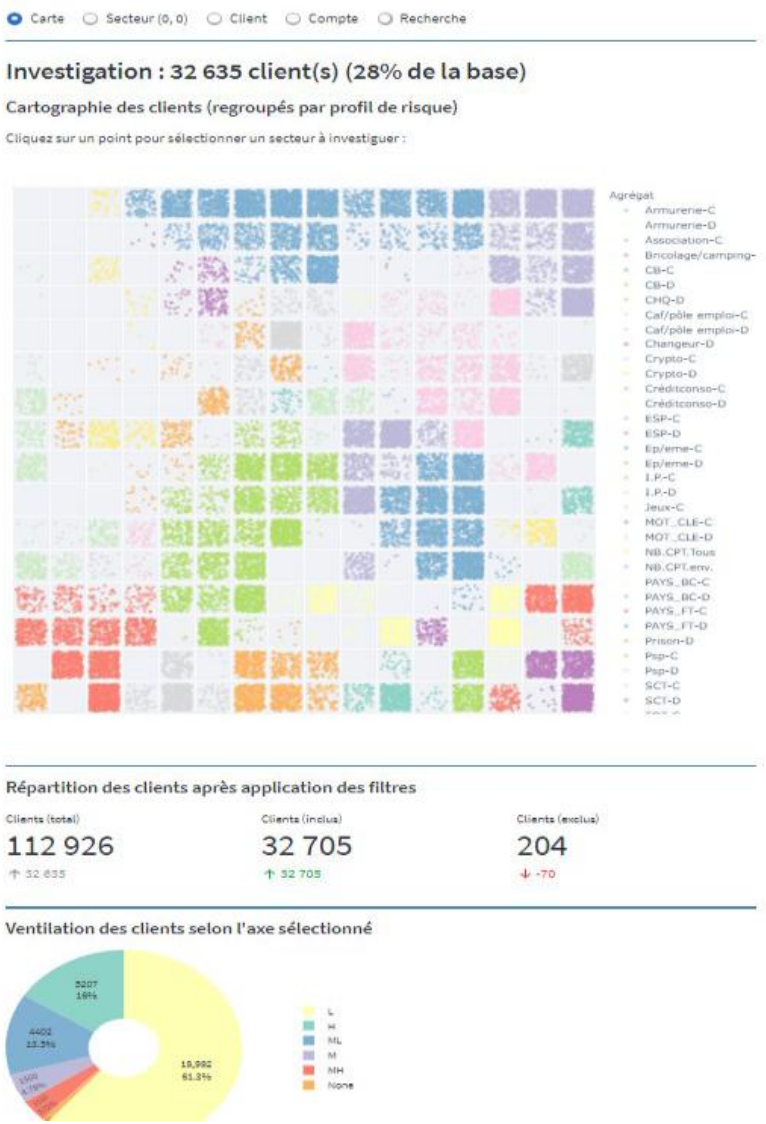
LA SOLUTION LUCIA

Parti pris méthodologique fondamental

- Exploiter les données remises par l'établissement et des sources d'information accessibles et publiques (rapports TRACFIN, appels à vigilance, open data, presse …)

Une approche en « entonnoir »

- Vision consolidée du portefeuille et des typologies comportementales de la clientèle
- Possibilité de filtrer à partir de scénarios prédéfinis ou configurés à la volée
- Approfondissement de l'analyse sur un segment homogène de clientèle caractérisé par un profil de risque type
- Étude détaillée d'un dossier avec vision consolidée sur le client, les faits saillants de risque, son environnement (co-titulaires, mandataires …), ses comptes et ses opérations



LA SOLUTION LUCIA

Techniques de traitement du langage naturel pour enrichir les données d'opération ou la connaissance client

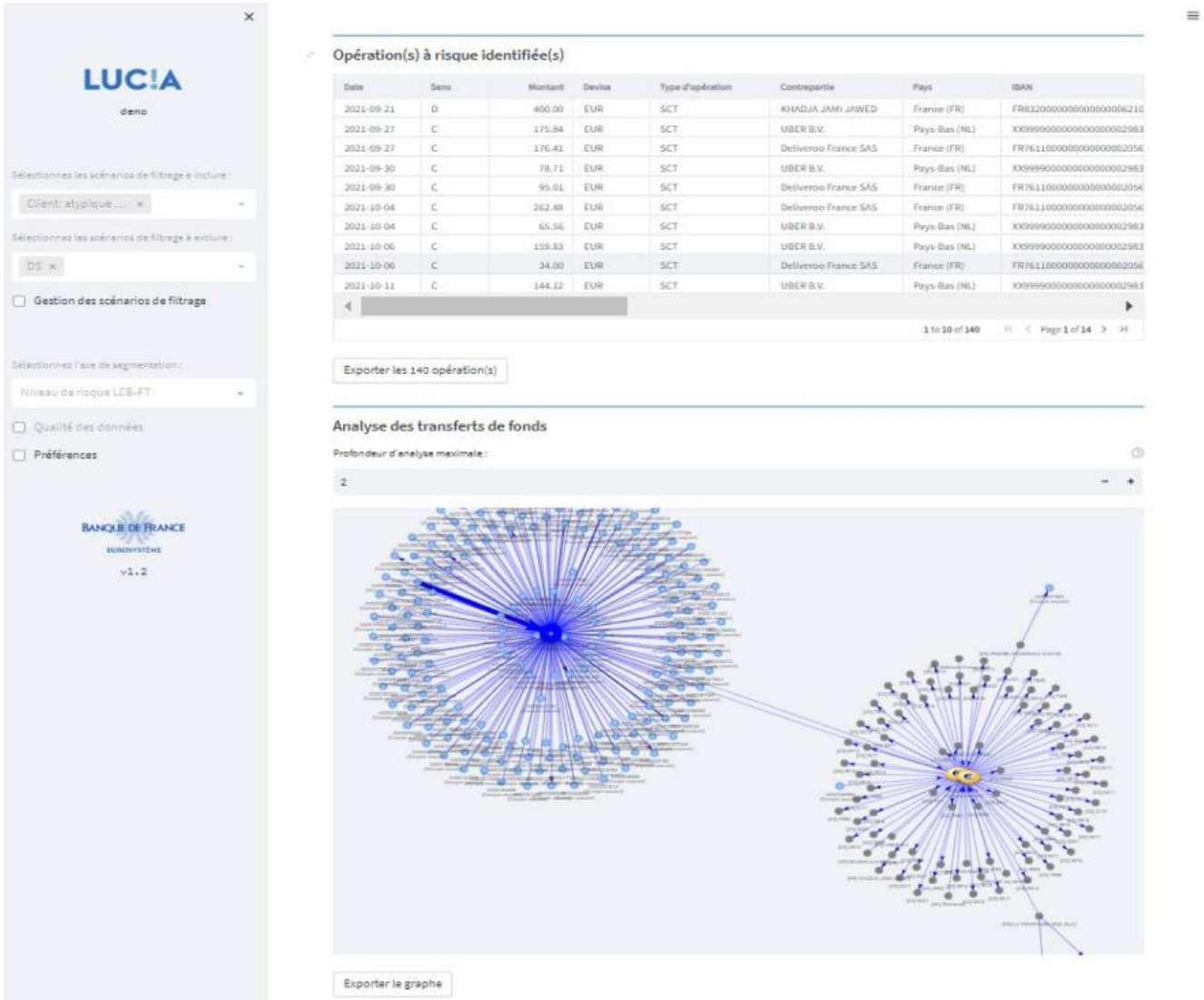
- détecter des contreparties ou opérations à risque
- analyser des adresses

Apprentissage non supervisé pour la détection d'anomalies et la segmentation automatique des profils de risque

- caractériser des comportements types à partir des données observées
- identifier les observations atypiques et construire des scores d'anomalie

Modélisation par graphes relationnels

- détecter des liens entre clients
- visualiser l'ensemble des flux et les relations avec les contreparties



LA SOLUTION LUCIA

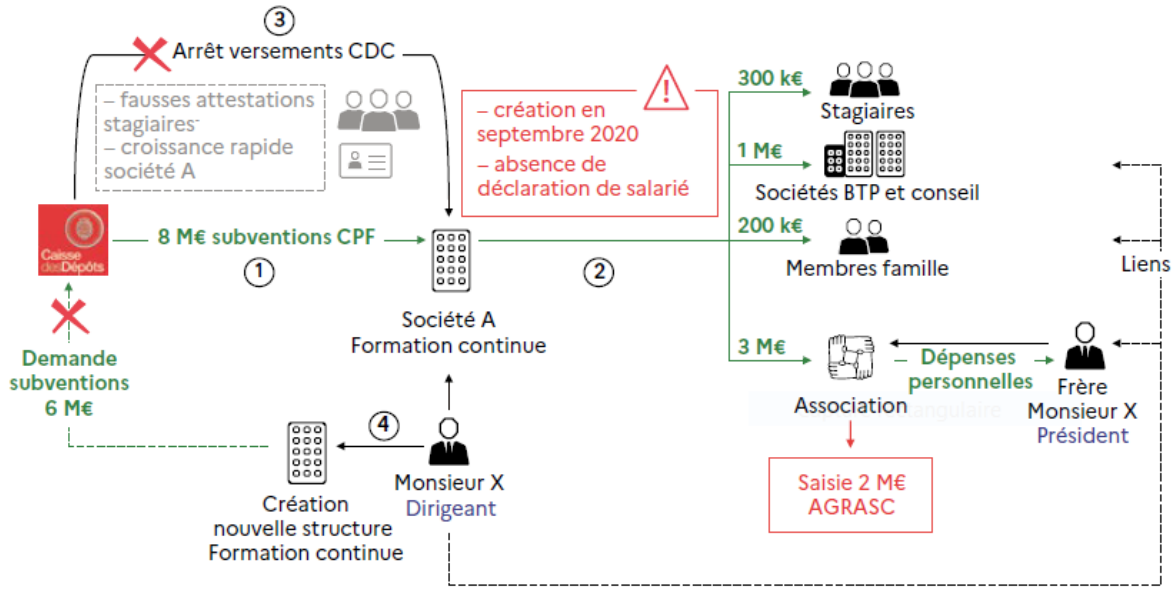
- **L'utilisation de sources de données externes permet d'améliorer l'identification des opérations atypiques :**
  - Ex : clients ou contreparties entreprises → challenger ou compléter/actualiser les données KYC de l'établissement à partir des données du site Pappers (identification des BE, secteur d'activité, effectifs, date de création, évènements, données financières) et identifier les contreparties
  - Prise en compte des informations péjoratives (Offshore Leaks, etc.) pour identifier des clients ou des contreparties de manière ad hoc ou à partir d'un score de risque
  - Données publiques ciblées correspondant aux typologies de BC-FT (ex : listes des délégataires CEE, OPCO vs flux CPF, etc.)

- **L'analyse des typologies de BC-FT issues des rapports TRACFIN permet d'approfondir l'approche par les risques et de mieux cibler les comportements atypiques :**
  - Analyser le portefeuille clientèle et ses caractéristiques pour identifier les zones de risques à investiguer
  - Identifier les typologies de BC-FT pertinentes (ex : blanchiment de fraude au CPF, de fraude au CEE, de fraude aux dispositifs d'urgence COVID19, recours à des sociétés taxis, fraudes fiscales ou sociales, etc.)
  - Compléter l'approche IA par une approche combinant scénarios de BC-FT et analyse relationnelle entre tiers (clients/contreparties)

LA SOLUTION LUCIA – ÉTUDES DE CAS

CAS TYPOLOGIQUE

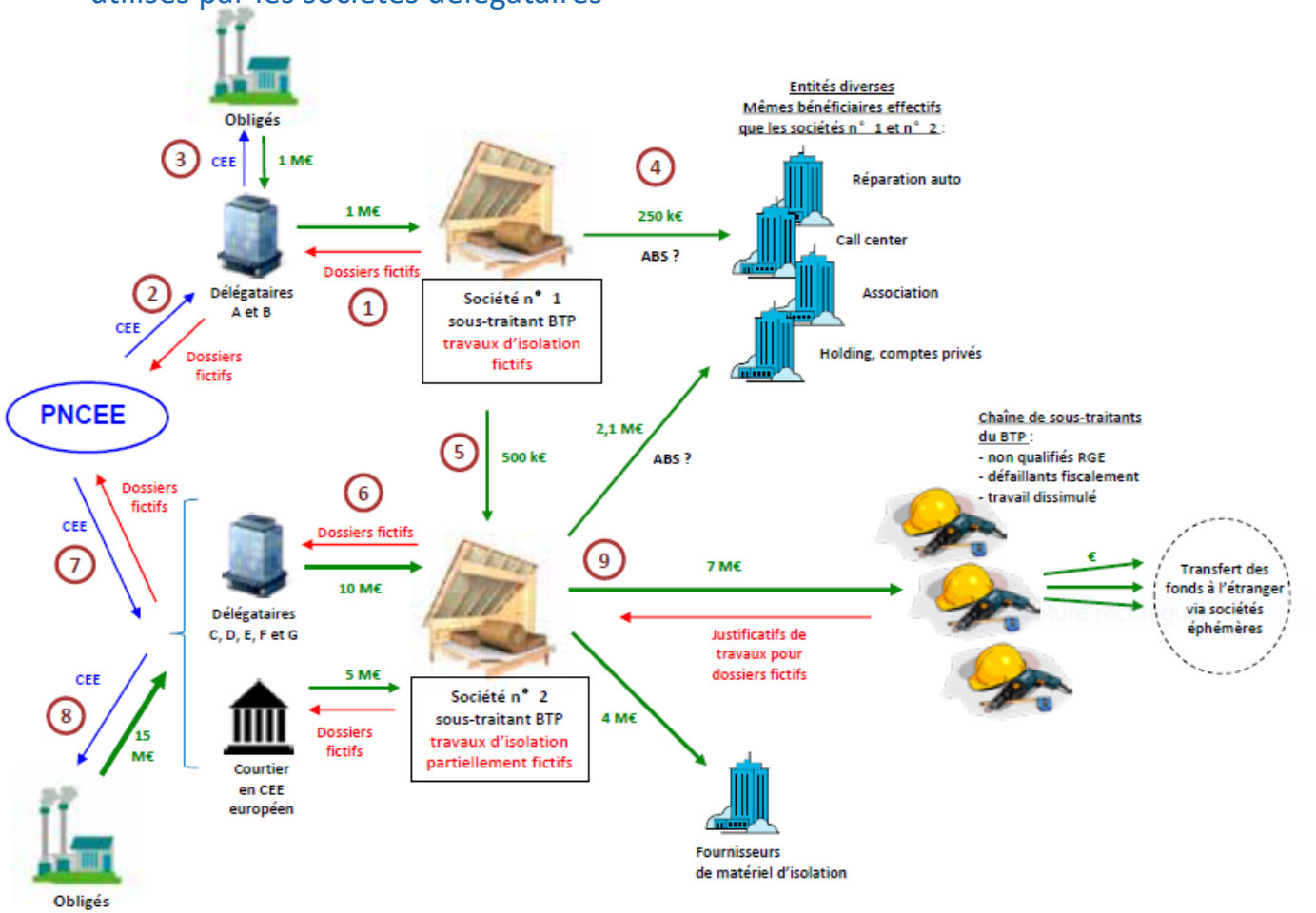
Escroquerie au CPF impliquant un réseau de blanchiment structuré



- **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.

LA SOLUTION LUCIA – ÉTUDES DE CAS

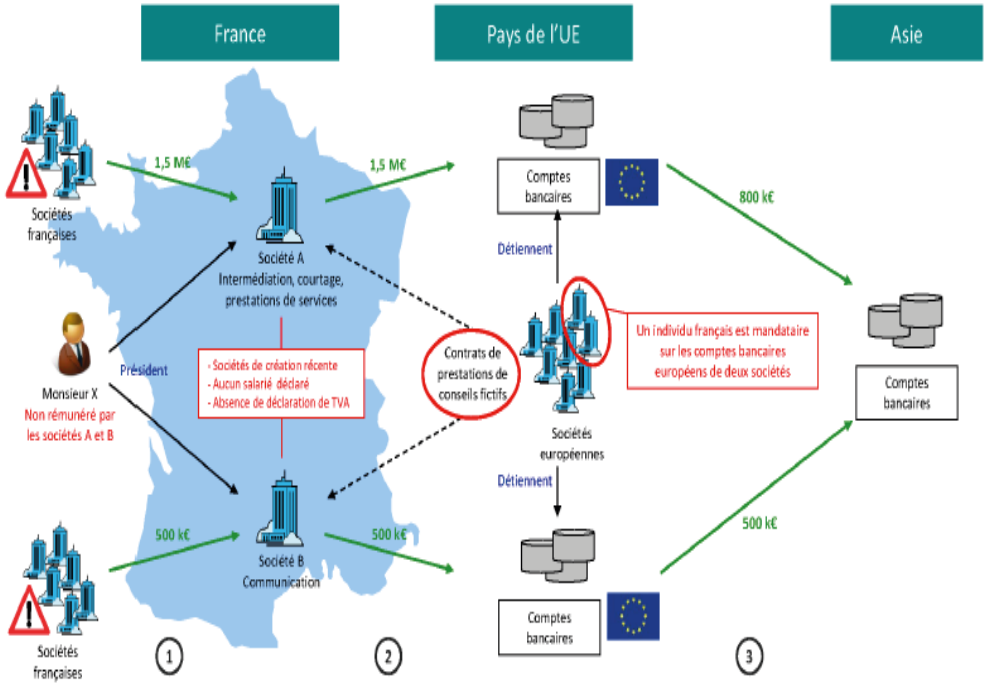
Blanchiment de fraude aux CEE via les chaînes de sous-traitants utilisés par les sociétés délégataires



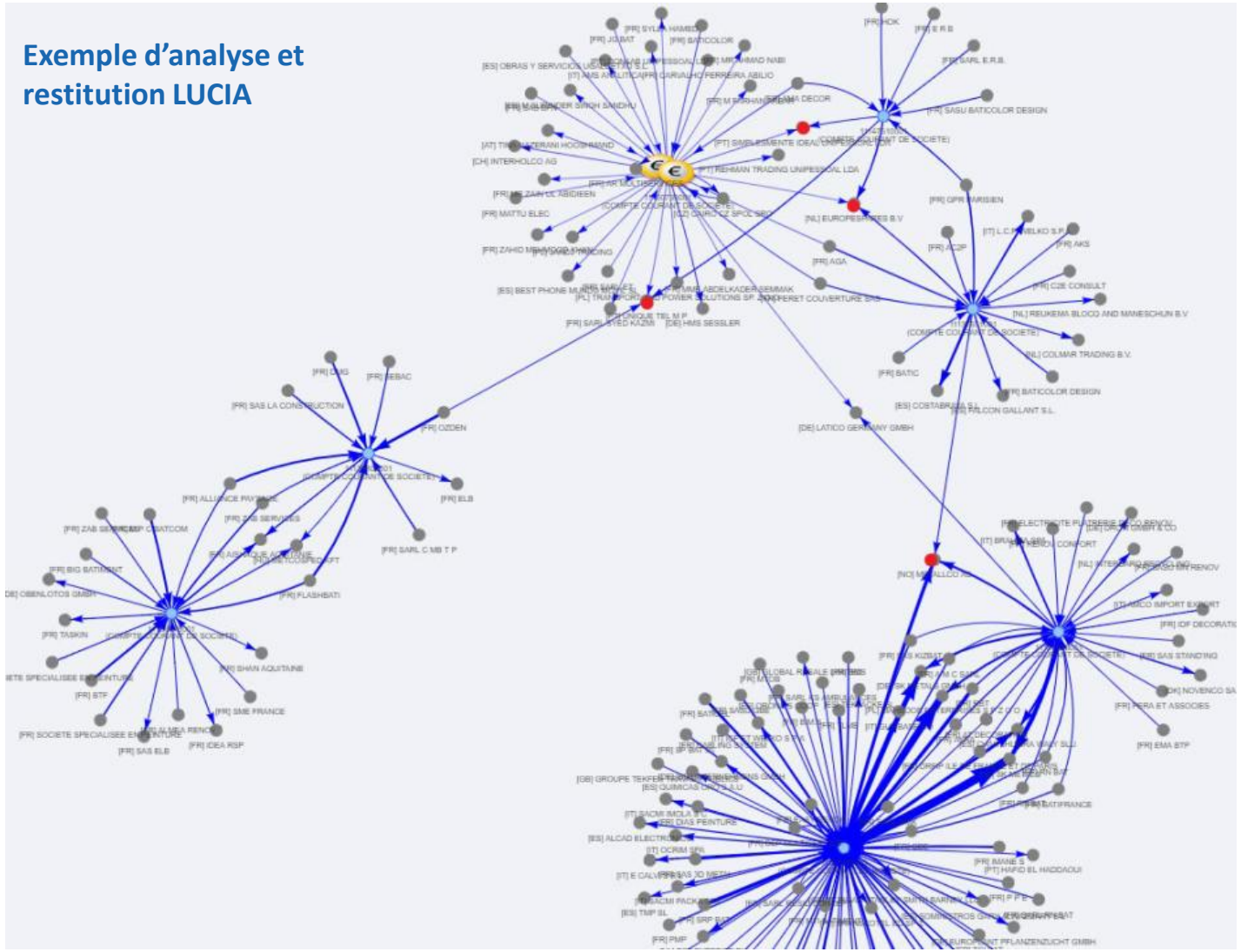
- **Mise en œuvre** : identifier les clients personnes morales ayant reçu des virements créditeurs en provenance des délégataires d'obligations d'économie d'énergie des périodes P4 et P5 dans le cadre des dispositifs de certificats d'économie d'énergie (CEE). L'identification des opérations a été réalisée 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.

LA SOLUTION LUCIA – ÉTUDES DE CAS

Blanchiment par l'intermédiaire d'un réseau de sociétés-taxis



Exemple d'analyse et restitution LUCIA



- **Mise en œuvre** : identification des clients présentant des caractéristiques communes (ex secteur d'activité, BE communs, dates de création proches) et liés par des contreparties communes.

CONCLUSION

- Les outils usuels de surveillance au fil de l'eau peuvent présenter des limites :
  - Modèles d'alertes axés sur la surveillance des types d'opérations/moyens de paiement avec des seuils en montants (unitaires ou cumulés) prenant en compte certaines caractéristiques des clients et la composante géographique
  - Prise en compte des données de connaissance clientèle insuffisante (revenus, patrimoine, caractéristiques clients)
  - Définition de véritables scénarios de BC-FT peu répandue
- Valeur ajoutée des sources d'informations publiques
  - Typologies de BC-FT et menaces identifiées par les autorités sur tous les segments (y/c les + récents comme les crypto-actifs)
  - Utilisation de sources de données externes pour approfondir l'approche par les risques et mieux cibler les comportements et transactions atypiques / à risques
- Combiner les méthodologies et les outils pour mettre en œuvre une approche par les risques sophistiquée et efficace
  - Définir des paramètres de surveillance en fonction des typologies de BC-FT pertinentes
  - Adapter les outils de surveillance aux zones de risques et favoriser les interactions entre les approches (ex : outil d'analyse transactionnelle vs surveillance des transactions fiat, analyse en réseau / relationnelle)

ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

QUESTIONS ?