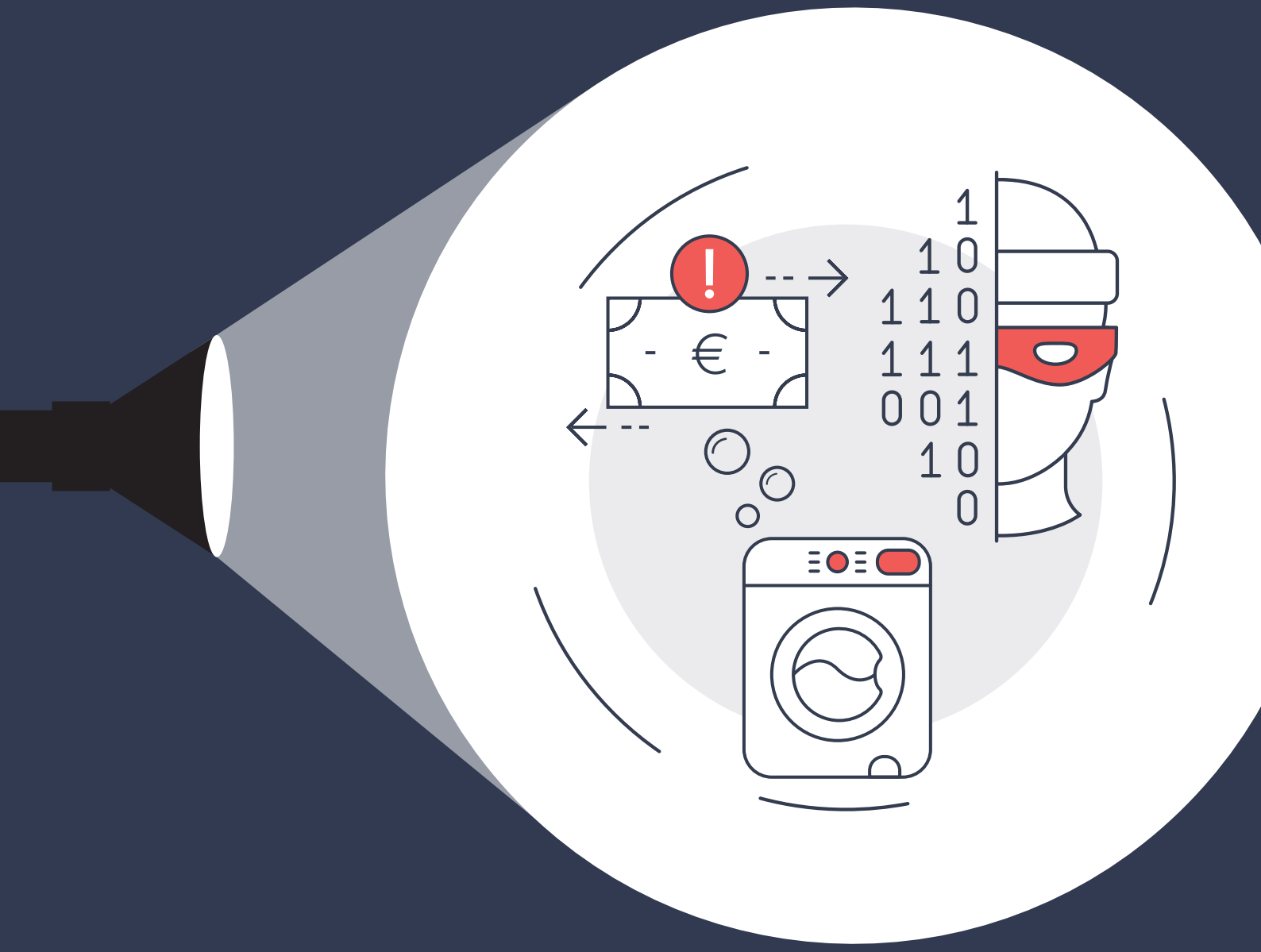
Les banques : gardiennes dans la lutte contre le blanchiment d'argent

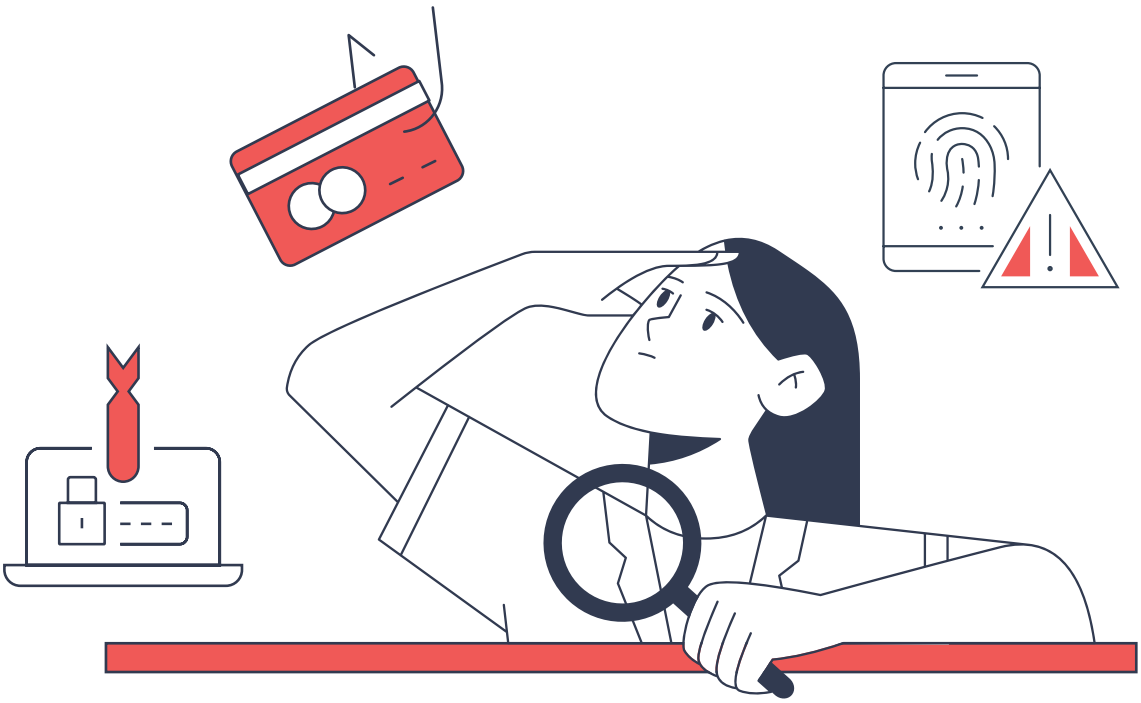


febelfin

Les banques assument leur responsabilité dans la détection des pratiques frauduleuses de blanchiment d'argent

L'argent circule. Il fait tourner l'économie. Les banques jouent un rôle crucial à cet égard, car elles rendent possibles les transactions financières et les paiements.
Mais il y a aussi un revers à la médaille : l'argent est parfois utilisé pour financer des activités criminelles telles que le terrorisme. Ou l'argent des milieux criminels est blanchi par des transferts successifs de compte à compte. Après maints transferts, l'argent criminel semble être complètement propre ou légal.

La lutte contre le blanchiment d'argent et le financement du terrorisme reste un défi, et les banques jouent aujourd'hui un rôle clé dans la détection de la fraude financière.
La présente brochure commente les efforts des banques en tant que gardiennes dans la lutte contre le blanchiment d'argent et le financement du terrorisme.



RESPECT ET SUIVI DES LÉGISLATIONS

Les banques sont soumises à la législation visant la lutte contre le blanchiment d'argent et jouent un rôle clé dans la détection de la criminalité financière. La législation belge est fondée sur des directives **européennes** (EU AMLD) et des **normes internationales** (GAFI/FATF), qui ont été encadrées de manière **encore plus stricte ces dernières années** (cf. EU AMLD III, IV, V, VI, etc.). Plus concrètement, cela signifie que :

- Le champ d'application a été élargi et que davantage d'institutions doivent se conformer aux obligations;
- des sanctions encore plus importantes (jusqu'à 10 % du chiffre d'affaires annuel de l'institution) ont été prévues en cas de non-respect de la réglementation;
- une approche basée sur les risques a été adoptée - pas une approche « cocher la case » - mais des évaluations de risque individuelles (= pas de standardisation possible);
- il a été prévu davantage d'inspections par les autorités de contrôle;
- il y a un risque de préjudice porté à l'image à chaque fois qu'un scandale survient.

Le **rôle de gardiennes dans la lutte contre le blanchiment d'argent ne s'arrête pas au contrôle préalable de la carte d'identité du client** mais nécessite **un devoir de vigilance continu** tout au long de la relation d'affaires, avec de **nombreuses obligations** :

- Know your customer « KYC »
- Know your transaction « KYT »
- Vérification de l'origine des fonds
- Approche fondée sur le risque
- Respect des embargos financiers
- Restriction quant à l'utilisation de l'argent liquide
- Obligation de déclaration à la CTIF (soupçons de blanchiment d'argent)
- Obligation de déclaration au Trésor (embargos)
- ...

Know your customer

La lutte contre le blanchiment d'argent a un impact majeur sur la relation entre la banque et sa clientèle. Un ou une client/e qui souhaite ouvrir un compte dans une banque doit d'abord s'identifier. Grâce à la bonne volonté de ce ou cette client/e qui accepte de partager son identité et d'autres données, la banque peut évaluer correctement sa relation avec lui ou elle et éventuellement prendre des mesures appropriées pour lutter contre la criminalité financière. Afin d'expliquer comment tout cela fonctionne, Febelfin a rédigé **la brochure « Lutte contre le blanchiment : savez-vous pourquoi votre banque vous pose des question ? »** que les banques peuvent utiliser pour informer leurs clients sur les raisons pour lesquelles elles demandent ces données et dans quel but.

La brochure commente entre autres les informations et documents que la banque doit rassembler avant de pouvoir offrir des services financiers. Plus précisément, cela signifie que :

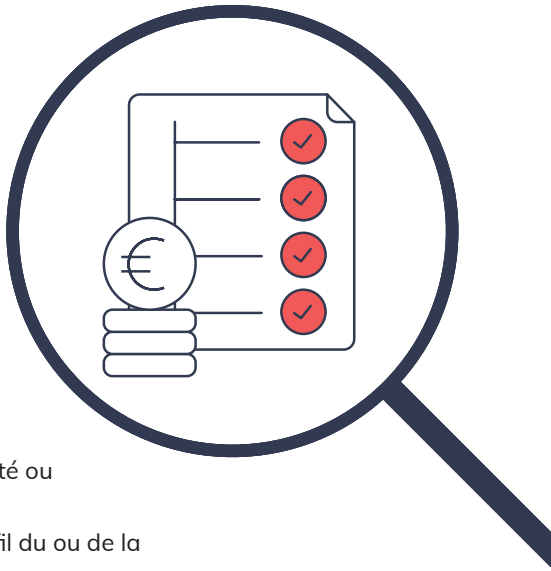
- Elle doit procéder à une identification et une vérification au moyen de preuves documentaires;
- Pour les **personnes physiques**, cela implique que, par exemple :
  - elle doit vérifier les données (nom, prénom, lieu de naissance, date de naissance, etc.) par lecture de la carte d'identité électronique (personnes physiques de nationalité belge) ou du passeport (personnes physiques ayant une autre nationalité)
  - elle doit vérifier si une personne a un « statut spécifique d'augmentation du risque » (par exemple, s'il s'agit de Personnes Politiquement Exposées, ...).
- Pour les **personnes morales**, des informations spécifiques sont requises, telles que :
  - mise à jour des statuts
  - clarté sur l'identité des administrateurs, des bénéficiaires effectifs (UBO)
  - dispositions relatives à la compétence d'engager une personne morale
  - identification claire des actions des mandataires (= titulaires de procuration, agents).

Ce processus doit être répété périodiquement (= vigilance continue). Cela signifie que les banques doivent à chaque fois assurer le suivi de différentes informations :

- Nouvelle adresse ?
- Nouveaux statuts ?
- Nouveaux bénéficiaires effectifs ? => L'entreprise doit identifier les bénéficiaires effectifs dans le registre UBO et en informer la banque. Pour plus d'informations : **Ce que vous devez savoir sur le registre UBO | Febelfin**
- La banque répète l'exercice afin de vérifier si le profil de risque et les mesures à prendre restent les mêmes ou doivent être adaptées.
- ...

La liste ci-dessus n'est pas exhaustive et est soumise à une législation stricte et aux recommandations de la Banque Nationale de Belgique.

Know your transaction



Les banques doivent toujours vérifier si une transaction est conforme aux caractéristiques de leur client/e et à l'objet et à la nature de la relation. Elles doivent ainsi identifier les transactions « atypiques » sur la base de leurs caractéristiques objectives ou sur la base des caractéristiques de ce ou cette client/e, telles que :

- les opérations anormalement complexes
- les opérations pour un montant inhabituellement élevé
- les opérations intrinsèquement inhabituelles, sans légitimité ou justification économique apparente
- les transactions qui ne semblent pas correspondre au profil du ou de la client/e.

Risk Based approach
(une approche basée sur les risques)

Les banques doivent concentrer au maximum leurs efforts et leurs ressources en matière de lutte contre le blanchiment d'argent sur la réduction du risque d'utilisation abusive à des fins de blanchiment d'argent ou de financement du terrorisme. Cette approche basée sur les risques devrait permettre aux institutions financières de prendre des mesures moins poussées dans les situations où les risques sont faibles et d'utiliser les ressources ainsi libérées pour appliquer des mesures plus strictes aux situations où les risques sont plus élevés.

Si une banque constate qu'il existe certains facteurs augmentant le risque en matière de lutte contre le blanchiment, elle doit

- recueillir davantage d'informations en vue de vérifier les données,
- prévoir d'accorder une attention plus soutenue aux opérations et de renforcer le contrôle sur celles-ci,
- mettre à jour les données plus rapidement,
- et bien sûr : signaler à la CTIF tout soupçon de blanchiment d'argent et mettre fin à la relation si nécessaire.

***Conformément à la loi anti-blanchiment**, les banques doivent être en mesure d'appliquer à tout moment une approche entièrement fondée sur le risque. Cela signifie qu'elles doivent être capables **d'analyser et d'atténuer les risques de blanchiment d'argent** liés à **chaque client/e individuel/le**. Pour donner une idée de l'ampleur : en 2019, il s'agissait de suivre quelque 18.787.773 client/es , dont 94,3 % de personnes physiques et 5,7 % de personnes morales.*

Signaler les transactions suspectes

Grâce aux procédures précitées, les banques peuvent remplir de manière optimale leur **rôle juridique** en matière de lutte contre le blanchiment d'argent et **déclarer les transactions ou les faits suspects** à la Cellule de traitement des informations financières (CTIF). Ceux-ci peuvent ainsi faire l'objet d'une enquête approfondie et d'un signalement éventuel au parquet. Les chiffres de la **CTIF** montrent d'ailleurs que les **banques** sont **l'un des principaux acteurs** de la lutte contre le blanchiment d'argent. En 2020, les établissements de crédit ont déclaré 17.678 **opérations suspectes à la CTIF** et ont été à l'origine de **55%** (soit une augmentation de 12% par rapport à 2019) des dossiers de blanchiment transmis par la CTIF aux autorités judiciaires. Ce qui correspond à un montant de 1,9 milliard d'euros.

Pour se conformer à la législation et à toutes les obligations - y compris l'obligation de déclarer les transactions suspectes à la CTIF -, il va de soi qu'il y a lieu de réaliser des investissements importants dans les procédures de contrôle et d'enquête, dans le renforcement des organisations internes (la formation du personnel et le recrutement supplémentaire, ...), mais aussi dans une collaboration étendue entre les banques et avec d'autres organisations et les pouvoirs publics.

[1] Enquête de Febelfin réalisée en 2020 dans le cadre de laquelle les données portaient sur la situation au 31/12/2019 auprès de 18 banques dont les 4 grandes banques.
[2] Source : **Rapport annuel CTIF 2020**

INVESTIR DANS DES PROCÉDURES DE CONTRÔLE ET D'ENQUÊTE

Protéger la société contre le blanchiment d'argent et le financement du terrorisme est une priorité absolue pour les **banques belges**. Ces dernières années, les banques ont poursuivi leurs **investissements** dans leurs **procédures de contrôle et de détection** [1] :

- Les banques belges ont **investi plus de 93 millions d'euros dans leurs départements de conformité AML en 2019**.
- Les banques investissent aussi massivement dans des **outils permettant d'automatiser les processus d'onboarding, de contrôle et de suivi des transactions**. Ainsi, 95 % des « vérifications de noms » périodiques sont déjà automatisées.

RENFORCER L'ORGANISATION INTERNE

En outre, les banques ont **renforcé** leur **organisation interne** afin d'intensifier la lutte contre le blanchiment d'argent et d'assumer plus que jamais leurs responsabilités en tant que **gardiennes** :

- En Belgique, on estime que plus de **1.600 employé/es de banque** sont engagé/es au quotidien dans la lutte contre le blanchiment d'argent. Mais dans la pratique, c'est bien plus, et chaque employé/e de banque est constamment attentif/ve à cette mission. **Ce qui précède montre que la lutte contre le blanchiment d'argent n'est pas seulement suivie par les services de conformité mais par tous les services au sein de la banque, et en premier lieu par les employé/es qui sont en contact avec la clientèle.**
- **61% des banques prévoient des investissements supplémentaires en 2021** en vue de recruter **davantage de personnel** afin de lutter contre le blanchiment d'argent et le financement du terrorisme.
- **Presque toutes les institutions financières (94,4%)** organisent des **formations continues spécifiques pour leur personnel dans le cadre de la lutte contre le blanchiment d'argent**. Cela peut aller de l'apprentissage en ligne à des formations classiques ou à l'autoformation. En 2019, **44.000 employé/es de banque** (soit 89 % de tout le personnel bancaire en Belgique) avaient suivi **au moins une formation spécifique sur la lutte contre le blanchiment d'argent**.

[1] Enquête de Febelfin réalisée en 2020 dans le cadre de laquelle les données portaient sur la situation au 31/12/2019 auprès de 18 banques dont les 4 grandes banques.

Les banques, maillon essentiel d'un ensemble plus vaste

Il est clair que les banques constituent un maillon fondamental pour prévenir et détecter autant que possible le blanchiment d'argent. Cependant, elles ne sont qu'une partie d'un ensemble plus vaste. La lutte contre le blanchiment d'argent gagnerait probablement à ce qu'il y ait davantage de possibilités d'échange d'informations, non seulement entre institutions financières, mais aussi avec d'autres instances publiques.

COLLABORATION ENTRE BANQUES

Les banques échangent leur expertise et leur savoir-faire concernant les utilities « Know Your Customer » (KYC). Cela conduit à une simplification administrative supplémentaire pour le client comme pour la banque, mais aussi à une amélioration de la qualité des données KYC et incite les banques à faire appel aux nouvelles technologies (par exemple, la blockchain) pour automatiser et numériser les processus.

Febelfin suit ainsi différents projets visant à optimiser les services KYC, notamment pour l'identification des entreprises et des particuliers. À cet effet, Febelfin soutient la société Isabel Group dans le développement du système Kube, qui permet aux entreprises de s'identifier via un système utilisant la technologie blockchain pour vérifier l'identité des utilisateurs. Grâce à ce système, les clients des institutions financières peuvent être identifiés plus facilement, plus rapidement et plus précisément. L'enquête de Febelfin [1] a montré que la plupart des institutions financières étaient très favorables au recours à des utilitaires de partage de données (tels que Kube ou Itsme).

Mais les **banques ne sont pas autorisées à partager dans toutes les circonstances des informations sur des transactions ou des clients suspects avec d'autres banques**. Pour que cela soit possible, **un cadre juridique est nécessaire pour le partage sûr et légal des données**.

[1] Enquête de Febelfin réalisée en 2020 dans le cadre de laquelle les données portaient sur la situation au 31/12/2019 auprès de 18 banques dont les 4 grandes banques.

CONCERTATION ENTRE BANQUES ET AUTORITÉS PUBLIQUES

En 2020, suite aux « FinCEN Files », Febelfin a recommandé une concertation plus étroite entre le secteur financier et les autorités publiques (gouvernement, BNB, cellule anti-blanchiment, autorités judiciaires, FSMA, etc.) afin d'**échanger efficacement des informations et d'intensifier conjointement la lutte contre le blanchiment d'argent**.

Aujourd'hui, les **banques** individuelles **fournissent des informations au pouvoirs publics et à la cellule anti-blanchiment**, mais cela s'arrête souvent là. Elles ne peuvent échanger des informations entre elles que de manière très limitative et elles reçoivent peu d'informations en retour. Febelfin plaide dès lors pour une **plus grande collaboration entre le secteur financier et les instances publiques** (pouvoirs publics, cellule anti-blanchiment, autorités judiciaires, etc.) en vue d'échanger des informations de manière sécurisée, afin d'unir les forces de toutes les parties concernées et d'accroître l'efficacité de la lutte contre la fraude et le blanchiment d'argent.

> « Permettons aux banques et aux pouvoirs publics d'échanger entre eux des informations sur les transactions suspectes via un environnement sécurisé afin de pouvoir réagir plus rapidement et éviter le blanchiment d'argent sale. »
>
> - Karel Baert

De telles formes de collaboration entre tous les acteurs concernés ont déjà été mises en place dans d'autres **pays européens**, comme les Pays-Bas et le Royaume-Uni. Les banques sont très favorables à la mise en place d'une telle plate-forme en Belgique également.

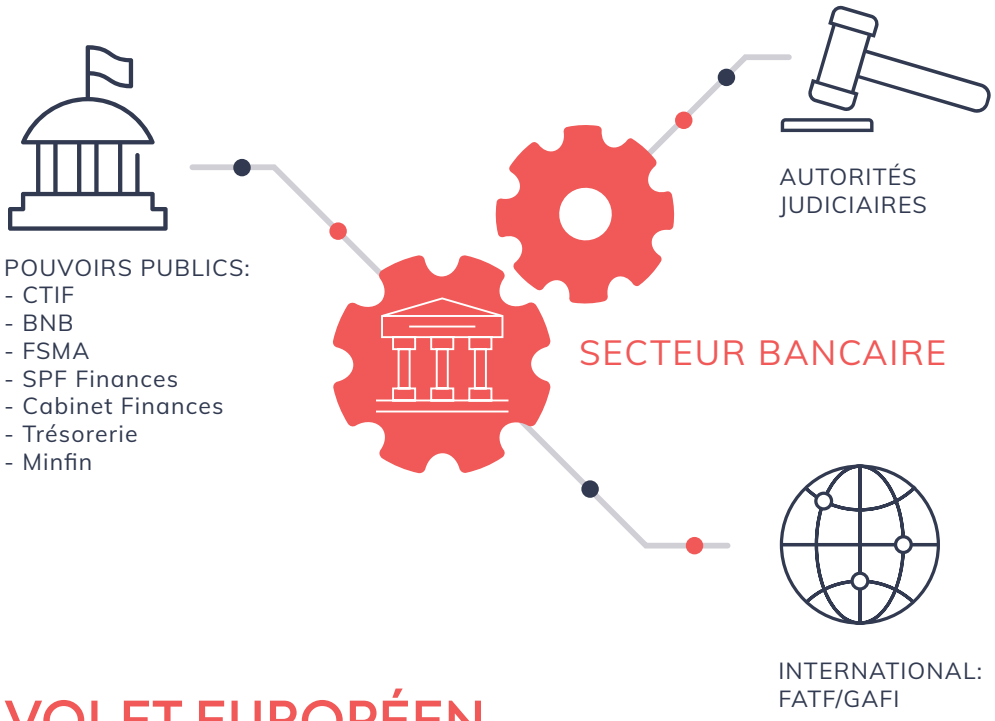
Ce plaidoyer a maintenant été entendu par les autorités et un partenariat privé-public comparable est en train d'être mis en place par analogie avec les exemples des pays voisins. Un protocole de collaboration a été rédigé pour créer et donner forme à cette plate-forme de concertation. Les partenaires de ce projet sont la CTIF, la BNB, le Cabinet des Finances, MinFin (Trésor), Assuralia, la FSMA et le secteur bancaire représenté par Febelfin. Les objectifs de la plate-forme sont :

- d'échanger des informations et de l'expertise sur les développements AML, les tendances, les risques émergents, les mécanismes et les typologies constatées ;
- de discuter de sujets relatifs à l'ALM/CFTP qui sont pertinents pour les différents participants ;

- de proposer des lignes directrices et fournir un retour d'informations sur l'application des obligations légales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, notamment en ce qui concerne la détection et la déclaration des opérations suspectes ;
- de rédiger des conseils ou proposer des initiatives pour promouvoir l'ALM/CFTP auprès des décideurs politiques ;
- d'étudier les possibilités de partager ou non les données dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme, qu'elles soient ou non spécifiques à un dossier, en tenant compte des dispositions légales en matière de secret professionnel et de traitement des données à caractère personnel et, si nécessaire, de proposer des solutions juridiques et technologiques pour l'échange de ces données par voie numérique.

Ce partenariat contribuera sans aucun doute à l'**élaboration d'un cadre juridique pour le partage sûr et légal des données.**

Les parties prenantes à la lutte contre le blanchiment d'argent en Belgique :



VOLET EUROPÉEN

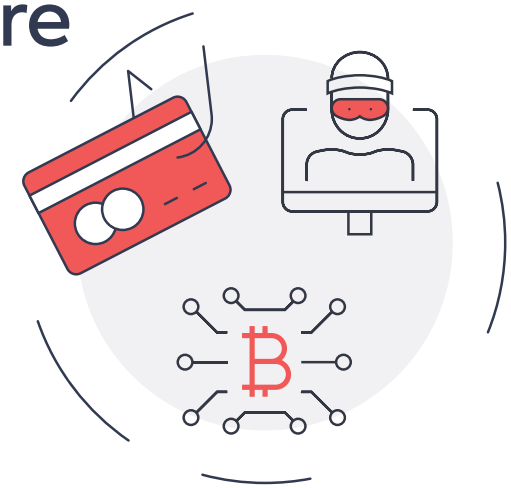
Le secteur suit également de près les travaux de l'**Union européenne** dans ce domaine. L'Europe est en train de réformer les règles anti-blanchiment et a l'intention d'élaborer un ***single rulebook*** pour **harmoniser les règles dans toute l'Union, par exemple en utilisant des règlements directement applicables**. L'harmonisation garantira une **application plus uniforme des règles et rendra la législation anti-blanchiment plus efficace**. Les propositions de loi européennes devraient également évoluer vers un régulateur européen de la lutte contre le blanchiment d'argent.

En collaboration avec la Fédération bancaire européenne (FBE), Febelfin a travaillé sur un certain nombre de recommandations pour une politique européenne efficace de lutte contre le blanchiment d'argent :

- un règlement européen au lieu de directives (ce qui est plus contraignant) ;
- une limitation des pouvoirs discrétionnaires des Etats membres ;
- des conditions de concurrence équitables au niveau mondial dans la lutte contre le blanchiment d'argent ;
- un renforcement du rôle de la **European Banking Authority (EBA)** dans un cadre réglementaire ;
- une harmonisation du contrôle (coordination transfrontalière); ceci s'applique également au travail des Financial Intelligence Units ;
- un renforcement du partage d'informations entre les banques et le secteur public/privé, dans les limites de la vie privée ;
- un enregistrement transparent et scrupuleux des UBO.

Nous pouvons attendre les premières propositions de la Commission européenne dans les semaines à venir, et elles seront examinées attentivement.

Tendances en matière de blanchiment d'argent et de financement du terrorisme [2]



La pratique du blanchiment d'argent est en constante évolution. Lorsqu'un mode opératoire est empêché, une autre manière créative de dissimuler l'origine criminelle des fonds et avoirs est trouvée. Cela reste un véritable jeu du chat et de la souris.

Si la crise du COVID-19 a eu un effet de ralentissement sur l'économie, elle n'a malheureusement pas eu d'impact significatif sur les fraudeurs et leurs activités. Au contraire, plusieurs nouvelles tendances de fraude ont été identifiées au cours de cette période, qui ont habilement tiré parti de l'actualité du moment et ont amené des défis supplémentaires pour le secteur bancaire en termes de lutte contre le blanchiment d'argent et le financement du terrorisme.

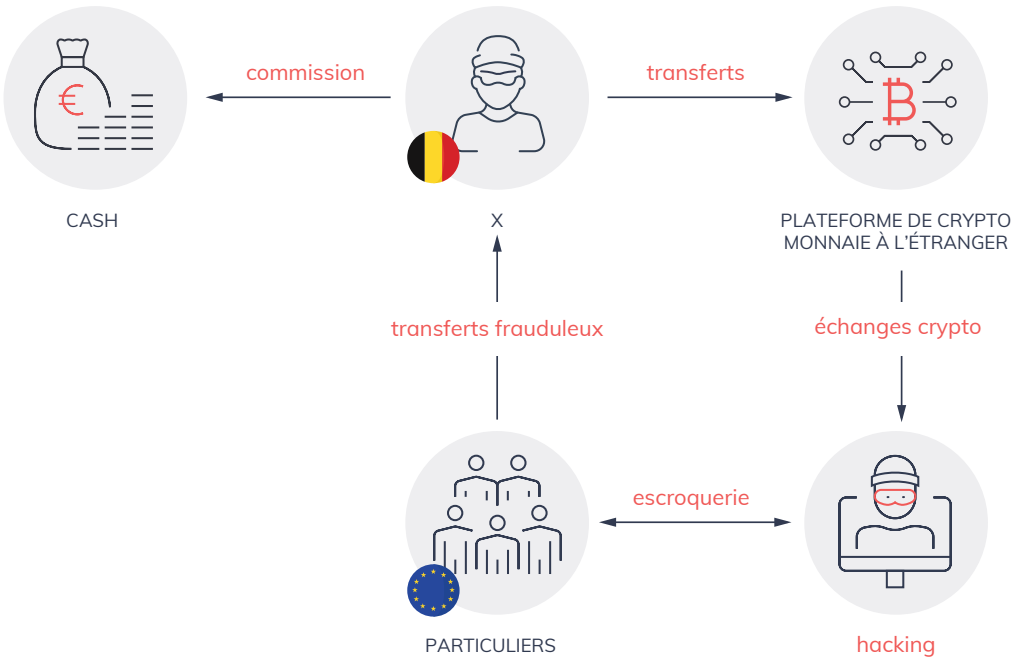
[2] Source : **Rapport annuel CTIF 2020**

Ainsi, le nombre de **courriels d'hameçonnage** dans lesquels des cyber-criminels, au nom d'une institution financière ou d'autorités, demandent à leur victime de mettre à jour les données de sécurité de sa carte - sous le prétexte de la situation exceptionnelle que nous connaissons - a considérablement augmenté et le « vivier » de victimes potentielles s'est encore agrandi.

Les **statistiques de Febelfin** montrent qu'en 2020, environ **67.000 transactions frauduleuses** ont été effectuées **via phishing**, pour un montant total net d'environ **34 millions d'euros**.
Ce qui est alarmant, c'est que **de plus en plus de mules** sont utilisées pour transférer rapidement et facilement l'argent dérobé par des moyens criminels d'un compte à un autre.

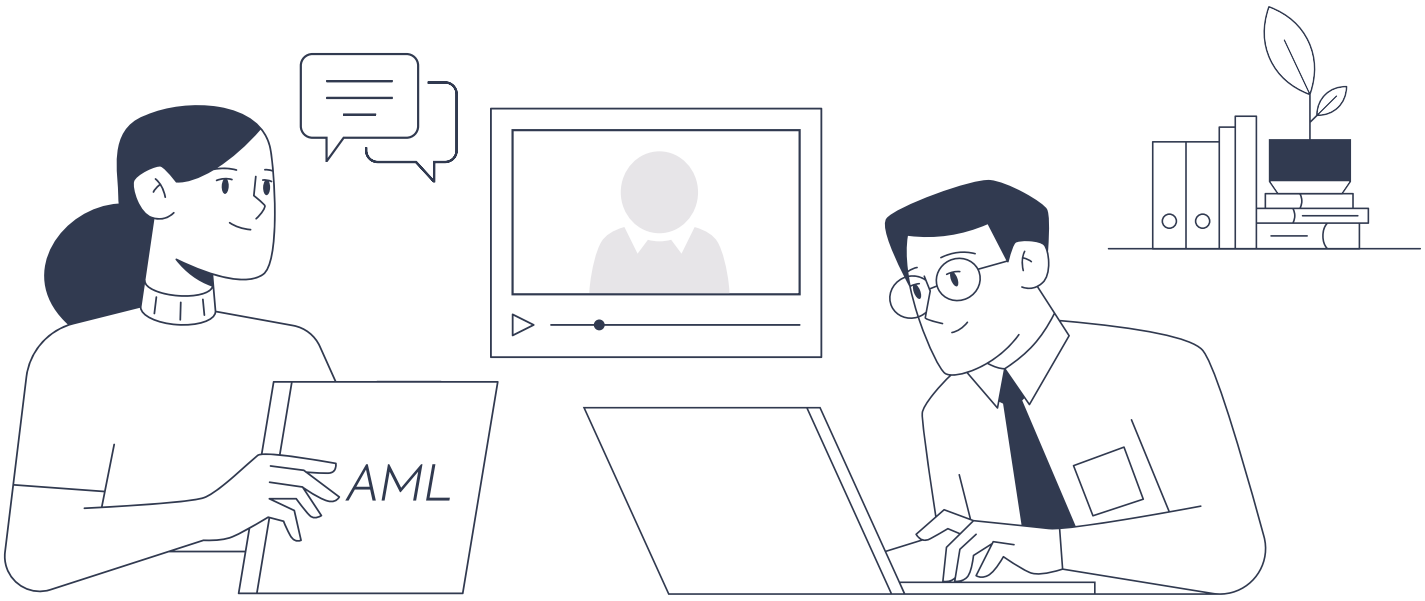
À l'heure actuelle, il n'est pas encore possible pour les banques d'échanger des données personnelles sur la fraude en raison de la législation (sur la vie privée). Les banques restent très prudentes dans ce domaine car elles sont liées par des réglementations très strictes par les autorités de contrôle et la législation. Febelfin étudie la possibilité de mettre en place un système d'échange de données d'identité de mules entre institutions financières sur une base légale.

La **fraude à l'investissement** (publicité en ligne pour de fausses formes d'investissement) et la **fraude via les cryptomonnaies** sont également en augmentation. La plupart des déclarations de fraude à l'investissement concernent les **boiler rooms, recovery rooms et options binaires**. Les **mules** jouent également un rôle majeur dans la fraude aux cryptomonnaies. Elles reçoivent de l'argent (obtenu par voie criminelle) déposé sur leur compte bancaire avec lequel elles doivent acheter des cryptomonnaies. L'illustration ci-dessous montre clairement comment tout cela fonctionne.



Exemple de fonctionnement des mules et du blanchiment via des cryptomonnaies : source CTIF

QUELQUES-UNS DES COURS PROPOSÉS PAR FEBELFIN ACADEMY



Febelfin Academy offre un large éventail de formations de base, avancées et spécialisées dans différents formats d'apprentissage (e-learning, classroom, blended), en cocréation avec différents partenaires. La nouveauté de cette année est qu'ils se concentrent également sur la manière d'appliquer la théorie/législation dans la relation quotidienne avec la clientèle.

Connaissances requises à l'entrée dans la profession

Chaque employé/e de banque/d'assurance/de crédits qui entre en contact avec un ou une client/e doit être en mesure de prouver ses connaissances. Ceci est basé sur des initiatives légales et inclut également l'AML. Cela signifie par exemple qu'une personne travaillant dans un garage doit avoir prouvé ces connaissances pour pouvoir proposer un prêt automobile.

- **Intermédiation bancaire (Loi Willems)**
- **Distribution d'assurances IDD**
- **Intermédiation en crédits**

FORMATION CONTINUE

Formations de base

Ces formations s'adressent à chaque employé/e qui, dans sa fonction quotidienne, est en contact avec la lutte contre le blanchiment d'argent.

Formation de base ayant pour objectif de donner une vue générale de la lutte contre le blanchiment d'argent : importance et impact : e-learning ou présentiel :

- **Lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT) : module général et applications**
- **Réglementation anti-blanchiment (AML V) obligations: une vision globale**

Application de la lutte contre le blanchiment d'argent dans la pratique et dans notre relation avec la clientèle : accent sur les compétences de négociation :

- **La prévention du blanchiment de capitaux (AML) et la connaissance du client (KYC) dans le cadre de la relation et des contacts avec les clients**

Formations avancées

L'accent est mis sur l'approfondissement des connaissances et l'application de la lutte contre le blanchiment d'argent dans l'organisation et ses processus. Ces formations s'adressent principalement aux employé/es qui traitent dans une large mesure des questions de blanchiment d'argent.

Formation avancée ayant pour objectif d'enseigner aux acteurs de terrain à reconnaître le financement du terrorisme et à agir en conséquence, ce, au départ de l'expérience pratique d'un commissaire fédéral chargé de la lutte contre le crime :

- **Prévention contre le financement du terrorisme**
- **Reconnaître des typologies anti-blanchiment**

Formation avancée offrant un historique approfondi et un cadre juridique général :

- **La prévention du blanchiment des capitaux: AML V**

Importance de la lutte contre le blanchiment d'argent dans le contexte des assurances

- **Recyclage assurance vie - Offre d'assurances vie : les obligations précontractuelles de la loi AML, du CDE et de l'IDD**

Formations d'experts

L'accent est mis sur l'impact de la lutte contre le blanchiment d'argent sur la politique de l'organisation dans ses différents aspects. Ces formations sont destinées aux membres du personnel qui contribuent à l'élaboration de la politique de l'organisation. L'accent est également mis sur l'avenir et l'impact stratégique.

AML et cryptomonnaies :

- **Investing in bitcoins or other cryptocurrencies: prudential framework**

Sanctions et embargos dans le cadre de la lutte contre le blanchiment d'argent :

- **AML: Sanctions et embargos**

AML et le rôle du Conseil d'Administration :

- **Executive program - The Board of Directors in the Financial Sector**

Que signifie la lutte contre le blanchiment d'argent pour notre vie privée et comment la gérer dans notre organisation ?

- **Developments for AML and challenges with Privacy: the perfect storm?**

Programme de certification en collaboration avec Deloitte Regulatory Services en vue de préparer l'examen de Certified Compliance Officer :

- **Trajet - Certified Compliance Officer**

Comment fonctionne l'évaluation des risques pour l'organisation ?

- **Evaluation des risques pour le compliance: organisation et approche**

Fédération belge du secteur financier

www.febelfin.be