Plan d'action de Febelfin contre la fraude en ligne

Résumé

Febelfin et ses membres partagent pleinement les préoccupations ambiantes concernant l'impact croissant de la fraude en ligne sur les consommateurs et la société dans son ensemble. Sous l'effet de la numérisation, de l'innovation technologique, de techniques d'ingénierie sociale de plus en plus sophistiquées et de l'industrialisation des réseaux criminels, la fraude en ligne est devenue un défi sociétal structurel en évolution constante.

Ces dernières années, le nombre de tentatives de fraude n'a cessé d'augmenter et les techniques utilisées sont devenues de plus en plus sophistiquées. En réponse, **les banques ont déployé des efforts importants et soutenus afin de renforcer la prévention de la fraude, sa détection et la protection des clients**. Ces efforts couvrent l'ensemble du cycle de la fraude : de la prévention et du suivi continu des transactions aux mesures de sécurité opérationnelles, en passant par la coopération avec les autorités policières et judiciaires, sans oublier les initiatives de sensibilisation continues destinées aux clients.

Ces efforts se sont considérablement intensifiés ces dernières années (capacité de développement informatique, effectifs dédiés à la fraude, etc.), ce qui atteste de l'engagement du secteur financier à renforcer davantage son rôle dans la lutte contre la fraude en ligne. Les banques continueront à élargir leur éventail de mesures de sécurité techniques et opérationnelles, à approfondir leur coopération entre elles et avec les autres acteurs concernés – avec le soutien politique et réglementaire nécessaire – et enfin à améliorer encore l'accompagnement des clients en cas de fraude. Parallèlement, le secteur reconnait que les banques ne peuvent pas relever ce défi seules.

La fraude en ligne ne peut être efficacement combattue par une approche centrée exclusivement sur les banques. Une réduction durable de la fraude nécessite **une approche intégrée et coordonnée dans laquelle tous les acteurs impliqués dans la chaîne de fraude assument leurs responsabilités**, les autorités publiques jouant un rôle clé de coordination et de facilitation. La fraude doit être traitée au plus près de sa source, notamment par une coopération renforcée avec les opérateurs de télécommunications et les plateformes de médias sociaux, ainsi que par des enquêtes et des poursuites efficaces afin de dissuader les réseaux criminels organisés. Comme dans certains pays voisins, une réponse collective et structurée est essentielle pour lutter contre cette forme de criminalité organisée. Ensemble, nous devons éviter de faire de la Belgique une destination attractive pour les fraudeurs.

Dans ce contexte, Febelfin et ses membres proposent un plan d'action global articulé autour de trois niveaux complémentaires.

Belgian Financial Sector Federation vzw/asbl
Boulevard du Roi Albert II 19 - 1210 Brussels
http://www.febelfin.be | T + 32 2 507 68 11 | F + 32 2 888 68 11
Governance Note FEB559746
Last saved on 9/07/2026 9:57:00 – 22 pages

1. **Les banques s'engagent individuellement à prendre des mesures de protection techniques et opérationnelles, visant à renforcer davantage les mécanismes de prévention, de détection de la fraude et de réaction. Cela implique l'introduction de certaines mesures de « slow banking », tout en maintenant un équilibre suffisant entre sécurité et confort d'utilisation.**

2. **Les banques renforceront la coopération interbancaire**, en évoluant vers une approche plus intégrée fondée sur le partage d'informations et de données, ainsi que sur des capacités technologiques communes. Le secteur financier s'engage également à adopter une gestion des clients plus harmonisée et centrée sur l'utilisateur, ainsi qu'à mener des actions de sensibilisation conjointes.

3. **Les banques plaident pour une approche globale de l'écosystème**, reconnaissant que la fraude prend souvent naissance en amont — via les opérateurs de télécommunications, les plateformes de médias sociaux et les canaux numériques — et qu'elle nécessite un engagement et une responsabilisation plus marqués des autres acteurs, ainsi qu'une application efficace de la loi.

Cette approche en trois niveaux, qui nécessitera une **large adhésion sociétale et un soutien réglementaire**, vise à renforcer la **protection des clients**, à améliorer l'efficacité opérationnelle et à s'aligner sur les évolutions du cadre réglementaire européen, notamment le Règlement sur les services de paiement (PSR). Elle met également en évidence la nécessité d'un **solide soutien politique** pour permettre le partage des données, assurer la responsabilisation intersectorielle et éviter la fragmentation réglementaire. En définitive, seul un **effort coordonné à l'échelle de tout l'écosystème** permettra de **réduire de manière durable et pérenne** la fraude en ligne.

Introduction : le paysage actuel de la fraude

Febelfin et ses membres prennent la lutte contre la fraude en ligne extrêmement au sérieux. Le secteur est pleinement conscient de l'impact financier, émotionnel et sociétal que la fraude a sur les victimes. Au quotidien, les banques investissent des ressources importantes pour prévenir la fraude, détecter les activités suspectes, bloquer les transactions frauduleuses, soutenir les victimes, récupérer les fonds lorsque cela est possible et coopérer étroitement avec les autorités publiques et les forces de l'ordre. Ces efforts sont continuellement adaptés aux nouveaux schémas de fraude et à l'évolution de la menace.

Malgré ces efforts soutenus, la fraude en ligne continue de causer des **dommages importants**. En 2025, les fraudeurs sont parvenus à soutirer 93 millions d'euros via des attaques de phishing, illustrant à la fois la persistance et la capacité d'adaptation des réseaux criminels.

Dans le même temps, il est important de replacer la fraude en ligne dans son contexte transactionnel global. Sur le volume total des transactions, les pertes nettes liées à la fraude représentent environ 0,004 % du montant total des opérations (2025). Ce chiffre montre que les transactions frauduleuses restent très limitées en termes relatifs, mais il souligne également l'impact significatif que la fraude peut avoir sur les victimes individuelles et la nécessité de poursuivre des efforts proportionnés pour renforcer la protection, chaque victime étant une victime de trop.

La fraude en ligne a connu une profonde évolution. **Il s'agit désormais d'un phénomène à l'échelle de l'écosystème, impliquant de multiples acteurs tout au long de la chaîne de fraude.** Les criminels opèrent de manière de plus en plus structurée et industrialisée, souvent à une échelle transfrontalière, en utilisant des kits de phishing, de faux sites web, des comptes de mules financières (passeurs de fonds), des centres d'appels, des fermes à fraude, des publicités sur les réseaux sociaux, des outils d'accès à distance et l'intelligence artificielle. Les opérateurs de télécoms, les plateformes de médias sociaux, les plateformes de vente en ligne et d'autres canaux numériques sont fréquemment utilisés en amont pour identifier, contacter et manipuler les victimes.

À l'inverse, les banques interviennent principalement en aval. Elles exécutent et surveillent les opérations de paiement, mettent en œuvre des contrôles visant la prévention et la détection, bloquent les instruments de paiement si nécessaire, lancent des procédures de récupération et accompagnent les clients après la survenue de la fraude. Ce rôle en aval est essentiel, mais il signifie également que **les banques ont un contrôle limité sur les premières étapes de la chaîne de fraude**, où les victimes sont au départ contactées, manipulées et préparées avant qu'un paiement ne soit initié.

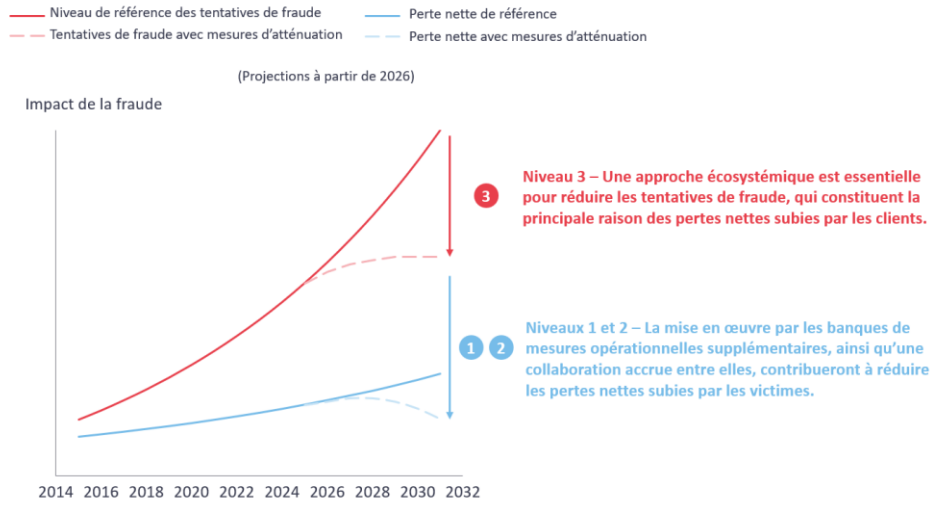
Les banques ont déjà **mis en place un vaste et solide ensemble de mesures opérationnelles et techniques** pour protéger les clients contre la fraude en ligne. Ces mesures couvrent l'ensemble du cycle de la fraude et peuvent être appréhendées à travers leur impact distinct mais complémentaire sur la dynamique de la fraude. Les mesures de **prévention** (telles que l'authentification forte du client,

itsme® et la vérification du bénéficiaire) contribuent à limiter la fraude en rendant les tentatives plus difficiles à exécuter. Les **mesures de détection et d'atténuation** (notamment le suivi des transactions, le blocage des transactions suspectes, les alertes et les procédures de récupération) réduisent principalement l'impact financier de la fraude en limitant les pertes lorsqu'une tentative a réussi.

Ces mesures ont déjà porté leurs fruits en renforçant la protection des clients. Grâce à une amélioration constante des capacités de prévention, de détection et de réaction, les banques ont considérablement accru leur capacité à identifier les transactions suspectes, à intervenir en temps réel et à limiter les pertes financières pour leurs clients. Les banques restent pleinement déterminées à intensifier encore ces efforts, notamment par le biais de garanties opérationnelles supplémentaires, de l'innovation technologique et d'une coopération accrue au sein du secteur. Ces investissements continus contribueront à réduire davantage l'impact financier de la fraude et à améliorer la protection des victimes.

Toutefois, l'évolution de la dynamique de la fraude (voir le graphique ci-dessous), montre que ces mesures influencent principalement l'**impact de la fraude une fois qu'elle se produit**, plutôt que le **volume global des tentatives de fraude**. Même avec des améliorations supplémentaires au niveau des banques, leur capacité à réduire structurellement le nombre d'attaques reste intrinsèquement limitée, la fraude étant en grande partie initiée en amont via des canaux situés en dehors du secteur bancaire.

Une réduction durable et significative de la fraude dépend donc largement d'actions efficaces de l'ensemble de l'écosystème — notamment les opérateurs de télécoms, les plateformes de médias sociaux, les fournisseurs de services numériques et les autorités chargées de l'application de la loi — afin de prévenir, détecter et entraver les activités frauduleuses à leur source. Le renforcement des mesures bancaires est nécessaire, mais seule une approche coordonnée à l'échelle de l'écosystème peut infléchir de manière significative la trajectoire des tentatives de fraude.



L'évolution de la fraude est étroitement liée aux tendances numériques plus larges. L'adoption rapide de la banque numérique et mobile, des paiements instantanés et des comportements « digital-first » des clients a renforcé la commodité pour les consommateurs, mais a également créé de nouvelles vulnérabilités. Les fraudeurs exploitent ces vulnérabilités en passant d'attaques de phishing de masse à des attaques plus personnalisées, en utilisant des techniques avancées de collecte de données, l'intelligence artificielle, le clonage vocal et des messages de phishing multilingues particulièrement convaincants.

De plus en plus souvent, les fraudeurs ciblent directement les clients, en exploitant la confiance, en créant un sentiment d'urgence et en manipulant leurs victimes pour les inciter à divulguer leurs identifiants, à approuver des transactions ou à augmenter elles-mêmes les plafonds de transfert. Dans ces cas, la banque ne perçoit pas immédiatement une « fraude » au moment de l'exécution, mais plutôt une transaction qui semble autorisée par le client. Ces tentatives de fraude, où les victimes sont manipulées pour valider elles-mêmes des transactions, prennent une importance croissante car elles permettent de contourner les mesures de sécurité techniques traditionnelles. Cette évolution est essentielle pour comprendre à la fois les limites techniques des contrôles bancaires et la nécessité d'une approche plus large et intégrée pour traiter la fraude à sa source (voir pièce jointe pour deux exemples du « processus de la fraude » correspondant aux modes opératoires les plus fréquents).

Ce paysage met clairement en évidence la nécessité d'une réponse à plusieurs niveaux. Les banques doivent continuer à renforcer leurs propres contrôles, mais une approche centrée uniquement sur les banques ne sera pas suffisante. **La fraude doit être combattue tout au long de la chaîne**, grâce à une prévention renforcée en amont, un meilleur partage des données, une clarification des responsabilités des autres secteurs, une application renforcée de la loi, une coordination accrue et une approche nationale cohérente.

Dans ce contexte, Febelfin propose un plan d'action ambitieux mais réaliste sur le plan opérationnel, dans lequel les banques prennent des engagements supplémentaires significatifs tout en appelant explicitement à une approche coordonnée et intégrée à l'échelle de l'ensemble de l'écosystème. **L'objectif est de renforcer encore la protection des clients, d'améliorer l'efficacité de la prévention et de la réponse à la fraude, et de garantir une pleine conformité avec le cadre réglementaire européen actuel et futur,** notamment la DSP2 (PSD2), le Règlement sur les paiements instantanés et le futur Règlement sur les services de paiement (PSR). Les initiatives nationales doivent rester cohérentes avec ce cadre européen et il convient d'éviter la surréglementation (« gold-plating »).

Plan d'action de Febelfin – Niveau 1 : Mesures opérationnelles et techniques mises en place et renforcées par les banques individuelles

Les banques ont déjà **mis en œuvre un vaste et solide ensemble de mesures opérationnelles et techniques** afin de protéger les clients contre la fraude en ligne.

Au cours des dernières années, les efforts des banques ont été continuellement renforcés par le biais d'une consolidation des **ressources humaines et technologiques**. Les banques ont élargi à la fois leurs capacités de développement informatique et leurs équipes spécialisées dans la lutte contre la fraude, reflétant la nature structurelle de la menace et la nécessité d'une adaptation constante à l'évolution des schémas de fraude.

S'appuyant sur les mesures déjà mises en œuvre par les banques individuelles en fonction de leurs bases de clientèle respectives et de leurs évaluations des risques, **les banques s'engagent à renforcer davantage leurs dispositifs individuels au moyen d'un ensemble de mesures opérationnelles alignées**. L'objectif est d'établir **un socle commun à l'échelle du secteur, composé d'un ensemble minimal de mesures opérationnelles** auxquelles les banques s'engagent. Les banques mettront en œuvre ces mesures et continueront en outre de les compléter en fonction de leur propre profil de risque ainsi que des caractéristiques spécifiques de leur clientèle, en tenant compte du timing visé pour chaque mesure.

Les mesures proposées visent non seulement à **renforcer la protection technique**, mais également à **introduire délibérément des moments de pause et de réflexion** dans le processus de transaction là où cela peut contribuer à **perturber les scénarios de fraude**. En **ralentissant** certaines étapes à haut risque — par exemple au moyen de mécanismes de « cooling down » — et en renforçant la sensibilisation des clients par des alertes et confirmations ciblées, les banques cherchent à **rompre la chaîne de fraude aux points critiques**.

Ces mesures répondent aux principales caractéristiques de la fraude moderne — urgence, manipulation et transferts à forte valeur — tout en cherchant à maintenir un équilibre proportionné entre sécurité, confort d'utilisation et autonomie des clients.

Le plan d'action de Febelfin prévoit les mesures opérationnelles suivantes, mises en œuvre par les banques individuelles, visant à :

Prévenir la fraude en ligne :

1. **Abaissement du plafond standard (5.000 EUR/jour) pour les virements à partir des comptes de paiement des clients particuliers**
2. **Période de ralentissement (« cooldown ») (> 4 heures) pour l'augmentation des plafonds**
3. **Notification en cas d'augmentation du plafond**
4. **Signature contextuelle**[1]
5. **Choix du client entre virement instantané et virement standard**
6. **Limitation des transactions frauduleuses sur les comptes d'épargne**

Détecter et traiter la fraude en ligne :

7. **Renforcement de la détection de la fraude et du monitoring des transactions**
8. **Détection des logiciels malveillants et des outils d'accès à distance (Remote access tool - RAT)**

Prévenir la fraude en ligne :

1. Abaissement du plafond standard (5.000 EUR/jour) pour les virements à partir des comptes de paiement des clients particuliers – limitation de l'exposition financière

Nombre de banques qui appliquent déjà aujourd'hui la limite standard inférieure (sur la base d'un échantillon de 10 banques de détail, 4/10)

Les banques **abaisseront les plafonds standards des virements au départ des comptes de paiement des clients particuliers à un maximum de 5.000 EUR par jour**. Un plafond par défaut plus bas **réduit l'exposition financière maximale par cas de fraude**, en particulier lorsque les pertes sont liées à des transactions unitaires de montant élevé. En diminuant les plafonds standards, le montant que les fraudeurs peuvent détourner sans relever les limites est fortement réduit. Les clients pourront toujours demander une augmentation de ces plafonds, mais celle-ci sera soumise à des processus

[1] La signature contextuelle garantit que les détails de la transaction affichés pour le signataire légitime (y compris le montant et l'IBAN complet du bénéficiaire) correspondent à ceux de la transaction exécutée. Cela inclut les moyens de signature directement liés à un appareil, tels que la reconnaissance faciale / l'empreinte digitale sur mobile et les passkeys.

contrôlés et à des mesures de sécurité supplémentaires (voir période de ralentissement et notifications).

Le plafond standard de 5.000 EUR/jour constitue un maximum. Une banque peut toujours choisir d'appliquer un plafond par défaut plus strict (par exemple 4.000 EUR/jour ou 5.000 EUR/semaine). Il est également important de noter que le client peut lui aussi réduire davantage ses limites personnelles en dessous du plafond standard fixé par la banque.

Timing visé : T1 2027

2. **Période de ralentissement (> 4 h) pour l'augmentation des limites – introduction d'un délai pour perturber les scénarios de fraude**

Nombre de banques qui appliquent aujourd'hui déjà la période de ralentissement
(sur la base d'un échantillon de 10 banques de détail, 5/10)

Les banques **introduiront une période de ralentissement (d'au moins 4 heures)** pour les augmentations des limites de virement. Dans le cadre de cette mesure, une demande d'augmentation de la limite de virement d'un client via des canaux numériques ne prendra pas effet immédiatement. Au contraire, la limite inférieure précédente restera active pendant au moins 4 heures. Cette mesure vise à **perturber les scénarios de fraude** qui reposent sur l'urgence et l'exécution immédiate après une augmentation de limite.

Timing visé : T4 2026, avec un calibrage soigneux afin de limiter autant que possible les frictions pour les paiements urgents légitimes.

3. **Notification en cas d'augmentation de la limite – une deuxième ligne de défense permettant une détection rapide**

Nombre de banques qui appliquent aujourd'hui déjà la notification en cas d'augmentation de la limite
(sur la base d'un échantillon de 10 banques de détail, 7/10)

Les banques mettront en place des **notifications systématiques en temps réel en cas d'augmentation des limites de virement** (et lorsque la période de ralentissement prend fin). Cela constitue une protection supplémentaire en alertant immédiatement le client d'un changement qui pourrait avoir été initié sous manipulation. Les notifications doivent être claires, pratiques et orientées vers l'action (ce qui a changé, quand, et que faire si le client n'est pas à l'origine de la demande).

Timing visé : T2 2027

4. Signature contextuelle – réduction du risque de fraude

Nombre de banques qui appliquent aujourd'hui déjà la signature contextuelle
(sur la base d'un échantillon de 10 banques de détail, 4/10)

Les banques renforceront encore les modalités de confirmation des transactions par les clients en veillant à ce que ces derniers voient des informations claires et spécifiques à la transaction au moment de l'approbation (telles que le montant et les coordonnées du bénéficiaire). Cela aide les clients à **comprendre exactement ce qu'ils autorisent** et réduit le risque qu'ils approuvent, à leur insu, une transaction frauduleuse sous manipulation.

La mise en œuvre se fera **progressivement au cours de la période 2026-2027**. Cette mesure s'accompagne de l'abandon progressif des lecteurs de cartes non contextuels, tout en maintenant la possibilité pour les clients qui le souhaitent de continuer à utiliser ces lecteurs de cartes.

5. Choix du client entre virement instantané et virement standard – réduction du risque de fraude

Nombre de banques qui offrent aujourd'hui déjà au client le choix entre virement instantané et virement standard
(sur la base d'un échantillon de 10 banques de détail, 10/10)

Les banques veilleront à ce que les clients conservent **toujours la possibilité de choisir entre un virement instantané et un virement standard.** Depuis octobre 2025, toutes les banques en Europe sont tenues de proposer les paiements instantanés à leurs clients. Les paiements instantanés, qui permettent de transférer des fonds au bénéficiaire en quelques secondes, gagnent en popularité en raison de leur rapidité et de leur praticité. Toutefois, cette immédiateté peut être exploitée par des fraudeurs pour transférer très rapidement des fonds hors des comptes de leurs victimes une fois la manipulation effectuée.

Pour répondre à ce risque, **les banques continueront à offrir aux clients la possibilité d'effectuer un virement standard,** dans le cadre duquel les fonds ne sont pas crédités au bénéficiaire instantanément. Ce délai supplémentaire peut contribuer à perturber les scénarios de fraude reposant sur l'urgence et la pression, et permettre de détecter ou de réévaluer des situations suspectes avant qu'un préjudice irréversible ne survienne.

Ce **choix offert au client** peut être mis en œuvre via différentes modalités opérationnelles, en fonction du modèle de service de la banque :

- la banque peut proposer le virement standard comme option par défaut, le client optant explicitement pour un paiement instantané s'il le souhaite ;
- la banque peut proposer le paiement instantané comme option par défaut, tout en permettant au client de passer à un virement standard ; ou

- la banque peut exiger que le client choisisse activement entre un virement instantané et un virement standard pour chaque transaction.

Dans tous les cas, le client conserve un contrôle total et peut décider en connaissance de cause quelle option de virement correspond le mieux à ses besoins. Cette mesure vise à concilier praticité et protection, en introduisant un **choix délibéré et éclairé** pouvant aider à **ralentir les scénarios de fraude et briser la chaîne de fraude**, tout en maintenant un équilibre proportionné entre rapidité, sécurité et confort d'utilisation.

Timing visé : immédiatement (T2 2026)

6. Limitation des transactions frauduleuses sur les comptes d'épargne – réduction du risque de fraude

Nombre de banques qui prennent déjà des mesures pour limiter les transactions frauduleuses sur les comptes d'épargne
(sur la base d'un échantillon de 10 banques de détail, 2/10)

Les banques prendront des mesures supplémentaires afin de limiter les transactions frauduleuses sur les comptes d'épargne. Elles pourront ainsi :

- proposer aux clients particuliers la possibilité de limiter et/ou de bloquer les virements en ligne depuis leurs comptes d'épargne réglementés vers leurs comptes à vue — dans le cadre d'une approche « slow banking » — combinée à une alternative sécurisée (par exemple un traitement en agence ou une période de réflexion complémentaire) pour autoriser ce type de transactions ; et/ou
- mettre en place une option dynamique de « mise en attente » (« on hold ») basée sur la surveillance des transactions.

Timing visé : T3 2027

Détecter & traiter la fraude en ligne :

7. Renforcement de la détection de la fraude et du monitoring des transactions

Les banques renforceront encore leurs mesures visant à détecter et à prévenir les transactions frauduleuses en **améliorant leurs capacités de détection de la fraude et de surveillance des transactions**. Des mécanismes de monitoring avancés permettent aux banques d'identifier des schémas suspects et, le cas échéant, d'intervenir en temps utile en bloquant ou en suspendant des transactions potentiellement frauduleuses avant qu'un préjudice irréversible ne se produise.

Dans le même temps, il est essentiel de **disposer d'un cadre approprié pour traiter les éventuels obstacles juridiques ou réglementaires** susceptibles de limiter l'utilisation d'outils efficaces de détection de la fraude, tels que le monitoring comportemental des transactions basé sur des

techniques analytiques avancées. L'innovation technologique peut constituer un instrument puissant dans la lutte contre la fraude en ligne et devrait être encouragée, pour autant qu'elle soit déployée de manière responsable et proportionnée.

Les banques soulignent dès lors l'importance de permettre cette innovation dans un **cadre clair et juridiquement sécurisé**, qui respecte pleinement les règles applicables en matière de protection de la vie privée et des données. Assurer le juste équilibre entre une prévention efficace de la fraude, le progrès technologique et la protection des droits fondamentaux est essentiel pour renforcer la protection des clients et perturber les scénarios de fraude tout au long de la chaîne de transactions. La mise en œuvre se fera **progressivement au cours de la période 2026-2028.**

8. **Détection des logiciels malveillants et des outils d'accès à distance (RAT) – ciblage des techniques de fraude les plus avancées**

Nombre de banques qui utilisent aujourd'hui déjà la détection de logiciels malveillants et/ou de RAT
(sur la base d'un échantillon de 10 banques de détail, 4/10)

Les banques exploreront plus avant des mécanismes (par ex. la détection de logiciels malveillants et d'outils d'accès à distance) afin d'identifier les sessions clients compromises (par ex. lorsqu'un appareil client est manipulé à distance). Il s'agit d'un domaine important pour lutter contre les techniques de fraude les plus avancées. Cela nécessite un développement et un calibrage soigneux, notamment afin de limiter les faux positifs et de garantir une expérience client proportionnée. **La mise en œuvre sera progressive sur la période 2026-2028.**

En outre, la fraude en ligne est un phénomène évolutif qui doit faire l'objet d'un suivi permanent, impliquant l'identification, l'évaluation et la mise en œuvre continues de bonnes pratiques lorsqu'elles s'avèrent efficaces contre la fraude en ligne. Une source d'inspiration peut, à cet égard, aussi être trouvée à l'étranger, où des instruments ou des mesures sont parfois introduits, sans toujours reposer sur la réglementation européenne. Febelfin s'engage, par le biais du benchmarking, à identifier et évaluer de nouvelles fonctionnalités, et à recommander à ses membres de les mettre en œuvre lorsqu'elles se révèlent efficaces et qu'elles bénéficient d'un soutien au sein du secteur.

Lors de la mise en œuvre des mesures précitées, il convient de tenir compte du fait que l'ensemble de ces adaptations techniques et opérationnelles, qui introduisent une forme de « slow banking », ont un impact sur le client : bien que ces mesures améliorent la protection, elles peuvent également entraîner des étapes supplémentaires ou des délais pour certaines transactions. Febelfin insiste dès lors sur l'**importance d'un large soutien sociétal et politique**. Des mesures de protection renforcées ne peuvent être efficaces et durables que si les clients, les décideurs politiques et les régulateurs reconnaissent qu'un niveau de sécurité plus élevé peut nécessiter certains ajustements en termes de rapidité, de commodité et d'expérience utilisateur.

Plan d'action Febelfin niveau 2 – Collaboration interbancaire

Des mesures au niveau de chaque banque sont nécessaires, mais elles ne suffisent pas. La fraude en ligne implique souvent plusieurs banques tout au long de la chaîne de transactions, en particulier lorsque les fonds sont transférés via des comptes de mules financières ou déplacés rapidement entre établissements et juridictions. Un **renforcement de la collaboration interbancaire** est donc essentiel pour détecter la fraude plus tôt, bloquer les fonds plus rapidement, améliorer leur récupération et apporter aux victimes une expérience plus cohérente et centrée sur le client.

Le plan d'action de Febelfin prévoit les mesures suivantes en matière de collaboration interbancaire, visant à :

Prévenir la fraude en ligne :

1. **Fraudstop**
2. **Campagnes de sensibilisation**
3. **Itsme®**

Détecter et traiter la fraude en ligne :

4. **Plateforme de partage des données sur la fraude**
5. **Charte de communication – engagement du secteur bancaire à traiter les dossiers de fraude dans un délai de 15 jours bancaires ouvrables**

Prévenir la fraude en ligne :

1. Fraudstop : un point de signalement unique et accessible 24 heures sur 24 et 7 jours sur 7

Les victimes sont souvent confrontées à de l'incertitude dans les premières minutes suivant la découverte d'une fraude : qui appeler, quelle procédure suivre et quelles actions entreprendre en priorité. C'est pourquoi le secteur a développé Fraudstop, un **point de signalement unique** avec un **numéro unique (078 170 170)**, accessible à tout moment, jour et nuit. Ce service permet d'orienter rapidement les victimes vers la banque concernée et de déclencher immédiatement des mesures de protection (y compris le blocage des moyens de paiement si nécessaire).

Cette initiative s'appuie sur la solidité et la notoriété du service sectoriel existant Card Stop, disponible 24 heures sur 24 et 7 jours sur 7, et vise à simplifier et accélérer la prise en charge des victimes. Parallèlement à ce nouveau point de signalement, chaque banque reste joignable via ses canaux habituels dédiés à la fraude. **Timing : lancement le 22 juin 2026**

2. Campagnes de sensibilisation – communication récurrente à destination du public

Dans un premier temps, les banques continueront à investir dans des campagnes de sensibilisation. Étant donné que le comportement humain et l'ingénierie sociale sont au cœur de nombreux scénarios de fraude en ligne, la prévention repose également sur le **renforcement de la résilience des clients**. Les initiatives de sensibilisation doivent être récurrentes, ciblées et adaptées aux modes opératoires de fraude ainsi qu'aux canaux de communication pertinents. Idéalement, les actions de sensibilisation devraient être menées conjointement par l'ensemble de l'écosystème afin d'en renforcer l'impact et d'en élargir la portée. Les banques sont favorables au déploiement de vastes campagnes de sensibilisation s'inscrivant dans l'esprit des célèbres « campagnes BOB ».

Timing visé : sur une base récurrente.

3. Itsme® renforcera ses mesures de prévention de la fraude

Au cours des 8 dernières années, itsme® n'a cessé d'ajouter des points de données ainsi que des mesures d'atténuation spécifiques, en étroite concertation avec les banques, afin d'améliorer la résistance à la fraude. Certaines de ces innovations sont mises en œuvre via une intégration directe avec les banques et les signaux qui y sont échangés ; d'autres sont assez visibles pour les utilisateurs eux-mêmes et créent une prise de conscience instantanée et contextuelle.

Dans le cadre de ces initiatives, des **couches de sécurité supplémentaires seront ajoutées via itsme® et des innovations dans les applications mobiles**. Cela réduira le risque de prise de contrôle de comptes et empêchera les fraudeurs de confirmer des identifiants de connexion ou un paiement au nom de leurs victimes. Seul l'utilisateur légitime correspondant à la photo figurant sur sa carte d'identité belge pourra agir en tant que titulaire du compte, ce qui constitue une barrière supplémentaire que les fraudeurs ne pourront pas franchir.

Timing visé : T1 2027

Détecter et traiter la fraude en ligne :

---

4. Plateforme de partage de données sur la fraude – une intelligence basée sur le réseau

Une initiative importante consiste à développer une **plateforme de partage de données sur la fraude via Isabel et itsme®.**

Les banques souhaitent partager plus rapidement et de manière plus structurée les signaux liés à la fraude, afin de détecter et d'interrompre plus tôt les schémas suspects. L'objectif est de passer d'une détection isolée à une **intelligence fondée sur le réseau**. En partageant des indicateurs de fraude pertinents, les banques peuvent détecter plus rapidement les activités des mules financières, éviter de nouvelles transactions frauduleuses et coordonner leurs actions de manière plus efficace. Dans ce contexte, le développement en continu de la plateforme de partage de données sur la fraude sera déterminant, notamment via l'intégration d'indicateurs de fraude supplémentaires, tels que des signaux provenant des appareils mobiles des citoyens. À court terme, la plateforme reposera sur la

mise en place d'un partage de données relatives aux comptes des mules financières. À moyen et long terme, l'ambition est d'élargir le périmètre en intégrant des signaux multi-sources (télécoms, appareils, itsme®).

Cette initiative s'inscrit dans les priorités nationales ainsi que dans l'orientation du futur cadre réglementaire européen, qui reconnaît de plus en plus l'importance du partage d'informations liées à la fraude. De telles initiatives nécessitent toutefois une **sécurité juridique** et un cadre approprié, notamment afin de garantir que l'échange de données soit sécurisé, proportionné et conforme à la réglementation. Le soutien politique, ainsi que l'implication active des autorités de contrôle (par ex. l'Autorité de protection des données), sont donc essentiels pour permettre une coopération efficace et éviter des failles exploitables par les criminels. Il reste crucial à cet égard que les banques soient en mesure d'évaluer une (nouvelle) relation client avec le(s) fraudeur(s) identifié(s), conformément à la législation applicable (AML, PAD, etc.).

En effet, les banques plaident depuis des années pour un partage accru des données relatives à fraude. À ce jour, seules les banques directement impliquées dans un cas de fraude sont autorisées à échanger des informations sur une base bilatérale (notamment concernant les comptes de mules financières). Ces informations ne peuvent pas être transmises à d'autres banques, ce qui complique considérablement la lutte efficace contre les fraudeurs et les réseaux de mules financières. Un renforcement de la coopération permettra ainsi de rendre la lutte contre la fraude encore plus efficace.

Timing visé : phase pilote T1 2027

5. Charte de communication – engagement du secteur bancaire à traiter les dossiers de fraude dans un délai de 15 jours bancaires ouvrables

Une autre priorité concerne **l'harmonisation de la communication avec les clients et du traitement des dossiers**. Le secteur s'engage à traiter les cas de fraude dans un délai maximum de **15 jours bancaires ouvrables**[2]. Cette démarche sera soutenue par des processus dédiés au traitement de la fraude, des délais standardisés ainsi que leur intégration dans une charte de communication sectorielle. Cette mesure est également alignée sur le futur cadre réglementaire PSR.

La charte de communication traduira ces engagements en une expérience client claire et cohérente. Ses objectifs fondamentaux sont d'agir rapidement, de garantir une accessibilité 24 heures sur 24 et 7 jours sur 7, de protéger en priorité le client, de tenir celui-ci informé, d'accompagner la victime étape par étape, de collaborer avec la police et d'assurer une assistance cohérente quel que soit le canal de signalement. Par cette charte, les banques entendent s'engager à veiller à ce que leurs clients victimes de fraude en ligne reçoivent les informations appropriées ainsi que l'accompagnement nécessaire, tout en accordant une attention particulière à leur dossier individuel. **Timing visé : T4 2026**

[2] Toutefois, lorsque la récupération des fonds implique des banques étrangères, ce délai de 15 jours peut être dépassé.

Plan d'action Febelfin niveau 3 – Approche écosystémique

Dans ce contexte, il est important de souligner que les mesures bancaires seules — qu'elles soient prises au niveau individuel ou sectoriel — ne peuvent produire des résultats durables en l'absence **d'une approche écosystémique pleinement opérationnelle**. Sans action efficace d'autres acteurs publics et privés **en amont et en aval de la chaîne de fraude**, les mesures de sécurité bancaires supplémentaires risquent de n'avoir pour seul effet que de limiter les conséquences plutôt que de s'attaquer aux causes profondes de la fraude. Nous nous référons à des exemples concrets, comme ceux du Royaume-Uni ou des Pays-Bas.

Par ailleurs, une approche écosystémique coordonnée est essentielle pour éviter l'apparition d'asymétries réglementaires ou opérationnelles susceptibles de faire de la Belgique une cible attractive pour les fraudeurs. Si la fraude n'est pas traitée d'une même manière tout au long de la chaîne ou entre juridictions, il existe un réel risque que l'activité criminelle se déplace vers le maillon le plus faible. Les banques sont prêtes à renforcer davantage leurs propres mesures, mais cela ne pourra être efficace que si l'ensemble des acteurs — publics et privés — prennent des initiatives complémentaires et cohérentes afin de lutter contre la fraude à chaque étape de la chaîne.

Febelfin appelle le gouvernement à prendre les mesures suivantes :

1. **Renforcer le rôle du CCB en tant que coordinateur central**
2. **Accroître la responsabilité des entreprises de télécommunications et des plateformes de médias sociaux**
3. **Renforcer l'action des forces de l'ordre (police et justice)**
4. **Renforcer l'authentification forte du client (dite « SCA » - Strong Customer Authentication) pour les transactions en ligne (« soft decline »)**
5. **Le gouvernement comme facilitateur : adapter le cadre juridique si nécessaire**
6. **Assurer l'harmonisation européenne et éviter la fragmentation et la surréglementation (« gold-plating »)**
7. **Soutenir les campagnes communes de sensibilisation**

1. Renforcer le rôle du CCB en tant que coordinateur central

Febelfin plaide pour une véritable approche écosystémique, coordonnée par les autorités publiques et impliquant l'ensemble des acteurs publics et privés concernés. Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité compétente en matière de cybersécurité dans notre pays. Pour rendre cette approche réellement efficace, deux priorités devraient être poursuivies :

- **L'élaboration d'un plan national de lutte contre la fraude**, auquel les banques contribueront activement. Un tel plan est nécessaire pour aligner les priorités, éviter la fragmentation et garantir une approche cohérente de la prévention, de la détection, du signalement, des enquêtes et de l'application des mesures.
- Le renforcement du rôle du CCB en tant que coordinateur central, notamment en assurant la présidence d'une plateforme de coordination centralisée réunissant l'ensemble des acteurs publics et privés concernés, afin de piloter la mise en œuvre du plan national de lutte contre la fraude et de garantir une coopération efficace.

2. Accroître la responsabilité des entreprises de télécommunications et des plateformes de médias sociaux

Les opérateurs de télécoms et les plateformes de médias sociaux jouent un **rôle central dans les premières étapes de la fraude en ligne** et doivent à ce titre assumer (davantage) leurs **responsabilités.** Les canaux de télécommunication sont fréquemment utilisés pour des appels et messages frauduleux, tandis que les plateformes de médias sociaux et les environnements publicitaires servent à diffuser des annonces frauduleuses, usurper l'identité d'acteurs de confiance et recruter des mules financières. Ces acteurs détiennent des données signalétiques essentielles et disposent de capacités de prévention pour lutter contre la fraude en amont. Leurs responsabilités doivent dès lors être clarifiées et renforcées, dans le cadre d'une approche globale de « responsabilité partagée ».

Pour les plateformes de médias sociaux et les grandes entreprises technologiques (Big Tech), cela implique notamment une détection et une suppression plus rapides des publicités, comptes et contenus frauduleux, ainsi qu'une responsabilité claire conformément au Digital Services Act et au futur cadre réglementaire PSR. La possibilité de désigner des signaleurs de confiance (ou « trusted flaggers ») pour rapporter les publicités frauduleuses devrait également être examinée dans le cadre juridique existant.

Pour les plateformes de médias sociaux et les opérateurs de télécoms, une coopération renforcée devrait également inclure la mise en place de mécanismes permettant de partager avec les banques des informations pertinentes liées à la fraude, conformément au futur PSR. À cet égard, des initiatives législatives supplémentaires ou des clarifications pourraient être nécessaires afin de fournir une base juridique solide à ces échanges de données, garantir la sécurité juridique entre secteurs tout en respectant les principes de protection des données et en permettant une action coordonnée efficace contre la fraude.

En particulier, l**es opérateurs de télécoms pourraient jouer un rôle clé** en développant des interfaces d'échange de données avec les banques et itsme®, permettant le partage de signaux pertinents pour la fraude, tels que des indicateurs de SIM swap, des signaux de ligne occupée, des numéros suspects ou certaines métadonnées de communication. Ces échanges devraient avoir lieu dans un cadre clair, proportionné et juridiquement robuste. Le renforcement de cette collaboration améliorerait

considérablement la détection précoce au stade de la transaction et la visibilité sur l'ensemble de la chaîne de fraude.

Une **supervision et des exigences plus strictes** pour les opérateurs de télécoms et les plateformes de médias sociaux sont nécessaires pour assurer le respect de leurs obligations, par exemple :

- Il est assez incompréhensible qu'une personne parvienne à acheter des centaines de cartes SIM avec la carte d'identité d'un membre de sa famille. De tels faits peuvent indiquer une fraude et doivent donc être traités avec fermeté par les opérateurs de télécoms, conformément aux exigences d'identification des utilisateurs finaux imposées par la législation belge.
- Des préoccupations analogues émergent dans le contexte du processus actuel de portage sortant (port-out). Auprès de certains opérateurs, un fraudeur peut s'approprier le numéro de téléphone d'une autre personne en se basant uniquement sur le numéro client lié au compte télécoms de cette personne, lequel peut être relativement facile à obtenir par phishing. Le fraudeur peut ensuite demander un échange de carte SIM et faire livrer une nouvelle carte SIM à une adresse de son choix. De telles lacunes illustrent la nécessité d'une supervision plus stricte et de contrôles renforcés, car elles facilitent non seulement la fraude, mais soulèvent également de sérieuses préoccupations en matière de KYC et d'identification des clients.
- Des rapports montrent que les plateformes de médias sociaux fondent leur modèle économique sur des publicités frauduleuses[3]. Ces plateformes devraient supprimer les sites web frauduleux conformément au Règlement européen sur les services numériques (Digital Services Act).

3. Renforcer l'action des forces de l'ordre (police et justice)

Les banques attendent également une **collaboration plus forte et structurée avec la police et la justice**, ces acteurs jouant un rôle décisif au bout de la chaîne de fraude. Si les banques peuvent prévenir, détecter, bloquer des transactions et initier des actions de récupération, seules les autorités policières et judiciaires peuvent **enquêter sur les réseaux criminels, poursuivre les auteurs et démanteler les structures organisées**. Cela est d'autant plus crucial que la fraude est de plus en plus organisée, transfrontalière et industrialisée, les fonds transitant souvent par des comptes de mules financières, différentes banques, des crypto-actifs ou des juridictions étrangères.

Febelfin appelle dès lors à un **renforcement de la coordination nationale** avec la police, les procureurs et les tribunaux, soutenu par des ressources adéquates, une expertise spécialisée et des flux d'information plus rapides entre banques et forces de l'ordre. Une telle coopération devrait dépasser le traitement isolé des cas individuels et permettre une approche plus stratégique, axée sur l'identification des schémas, le traçage des flux financiers et le ciblage des organisations criminelles de haut niveau à l'origine des fraudes. Une collaboration pilote avec le parquet, par exemple, pourrait contribuer à orienter les efforts vers le démantèlement des réseaux de fraude organisés plutôt que de

[3] https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

se limiter aux incidents individuels. La police et le ministère public devraient avoir accès à la (future) plateforme de partage de données sur la fraude et devraient également l'alimenter. Ce renforcement de la réponse judiciaire et policière est essentiel pour compléter les mesures préventives des banques et garantir que la lutte contre la fraude en ligne non seulement vise à protéger les victimes, mais s'attaque aussi à la source criminelle du problème.

Febelfin attend du gouvernement qu'il investisse les ressources nécessaires dans la police et la justice. Une politique de poursuite laxiste, due à un manque de moyens, entraîne une impunité pour les auteurs et constitue un facteur d'attraction pour les fraudeurs et criminels potentiels. Ceci est crucial non seulement pour dissuader les criminels, mais également pour réduire l'impression chez les victimes que ceux-ci agissent en toute impunité.

4. **Renforcer l'authentification forte du client (dite « SCA » - Strong Customer Authentication) pour les transactions en ligne (« soft decline »)**

Les banques prendront l'initiative (via un accord sectoriel et/ou une demande à l'autorité de régulation) pour rendre **l'authentification forte (SCA) obligatoire pour certaines transactions en ligne** (les transactions dites SCA-CNP (card not present), en accord avec la mesure française).

La directive PSD2 prévoit des exceptions à l'utilisation de la SCA dans les transactions en ligne. Par exemple, pour des bénéficiaires connus ou des montants faibles présentant un risque limité, la SCA n'est pas requise. Ces exceptions sont souvent à l'origine de nombreux cas de fraude (souvent pour des montants relativement faibles). Ce problème peut être en grande partie résolu en appliquant le mécanisme du « soft decline » (la demande de paiement sans SCA est refusée, mais le commerçant/vendeur peut soumettre à nouveau la demande avec SCA).

5. **Le gouvernement comme facilitateur : adapter le cadre juridique si nécessaire**

Certaines mesures bancaires ne peuvent être mises en œuvre que si la **législation pertinente** est effectivement appliquée et/ou adaptée dans un délai raisonnable :

- Partage de données relatives à la fraude : échange de données sur les mules financières entre banques (nom, numéro de registre national).
- Échange de métadonnées des opérateurs de télécoms (p. ex. si l'appel est en cours, durée de l'appel…).
- Utilisation de données biométriques dans le monitoring comportemental des transactions (profilage individuel) dans le cadre de la détection de fraudes.
- Les plateformes de médias sociaux doivent supprimer plus rapidement les publicités frauduleuses et être tenues légalement pour responsables conformément au EU DSA (Digital Services Act) et au PSR.
- Il faut évaluer qui peut être désigné comme signaleur de confiance (« trusted flagger ») dans ce cadre juridique pour soumettre des signalements fiables de publicités frauduleuses.
- Les opérateurs de télécommunications doivent respecter les exigences d'identification des utilisateurs finaux imposées par la législation belge.

6. **Assurer l'harmonisation européenne et éviter la fragmentation et la surréglementation (« gold-plating »)**

Cette approche en trois niveaux vise à renforcer la protection des clients tout en restant **cohérente avec le cadre réglementaire européen** en évolution. Le secteur souligne l'importance de l'alignement avec les règles de l'UE ainsi que la nécessité d'éviter la surréglementation nationale ou des initiatives fragmentées qui réduisent la sécurité juridique et l'efficacité opérationnelle.

7. **Soutenir les campagnes communes de sensibilisation**

Les campagnes de sensibilisation constituent un élément essentiel de la **prévention de la fraude**. Le secteur bancaire s'engage en faveur d'une approche de communication commune et développera une campagne visant à maintenir un niveau élevé de sensibilisation à la fraude dans l'opinion publique et à encourager les clients à adopter des comportements concrets et réfléchis réduisant leur exposition à la fraude. Le secteur continuera d'investir dans ce domaine afin de renforcer la résilience des consommateurs et ainsi prévenir la fraude. Il est important que le gouvernement (comme pour les « campagnes BOB ») et les autres parties prenantes soutiennent et facilitent ces campagnes. Une telle approche coordonnée peut générer un effet de levier important, renforcer davantage la prévention de la fraude et accroître la résilience des citoyens.

Conclusion

La fraude en ligne est devenue un défi sociétal structurel et évolutif qui ne peut plus être résolu par des mesures isolées ou par un seul groupe d'acteurs. **Le secteur bancaire reconnaît pleinement sa responsabilité et a déjà pris, et continue de prendre, des initiatives de grande ampleur pour renforcer la protection des clients, améliorer la détection de la fraude et soutenir les victimes.** Au travers du présent plan d'action, les banques s'engagent à poursuivre le renforcement de leurs efforts, tant au niveau individuel que sectoriel, notamment par des garanties opérationnelles supplémentaires, une coopération accrue et une sensibilisation renforcée des clients.

Dans le même temps, ce plan d'action démontre clairement que les seules mesures bancaires ne suffisent pas à assurer une réduction durable de la fraude en ligne. Même les initiatives les plus robustes, au niveau des banques et interbancaire, ne permettront de traiter qu'une partie du problème si la fraude continue d'apparaître et d'évoluer ailleurs dans la chaîne. **Un impact durable nécessite une approche écosystémique pleinement coordonnée, dans le cadre de laquelle l'ensemble des acteurs publics et privés concernés assument leurs responsabilités** et agissent de manière cohérente et complémentaire.

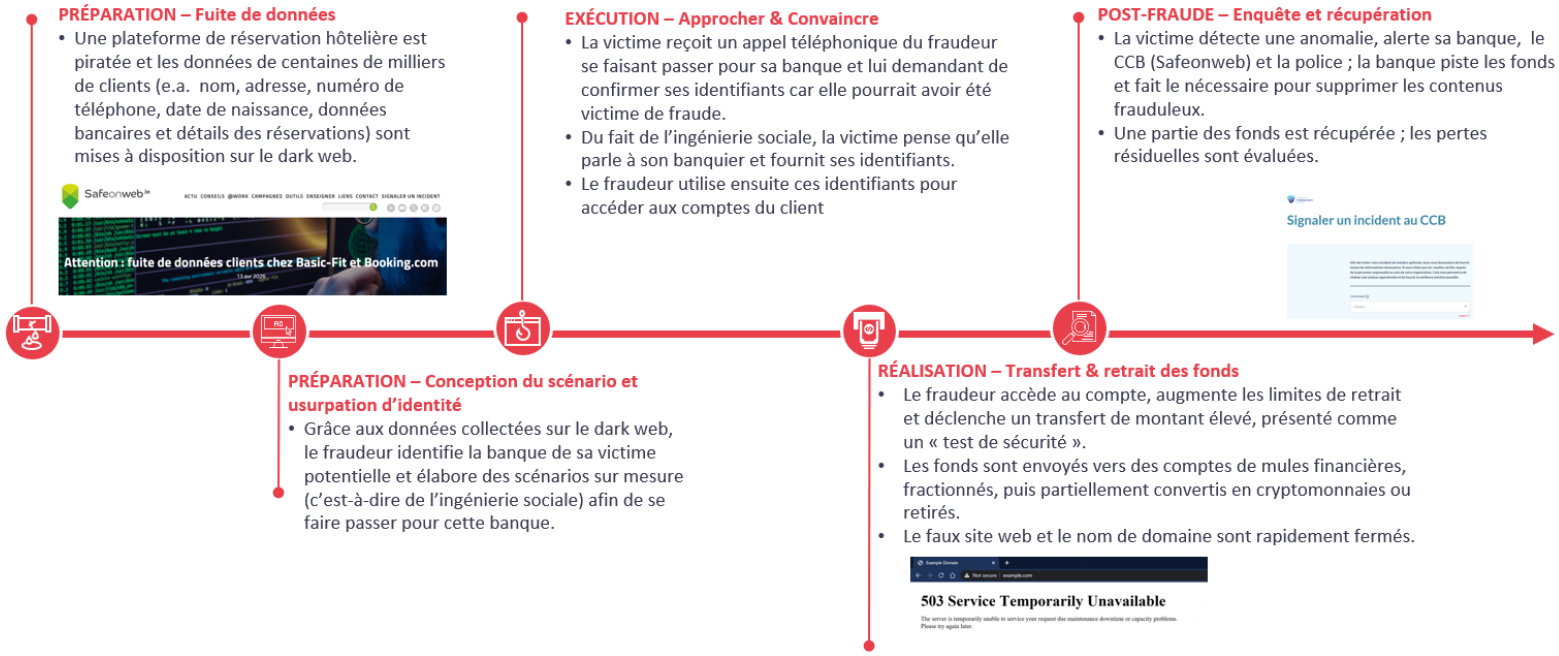
Les banques sont prêtes à en faire plus et à continuer d'investir dans la prévention, la détection et dans la protection des clients. Cependant, ces efforts ne pourront être efficaces que s'ils sont soutenus par des actions décisives en amont et en aval de la chaîne de fraude — y compris de la part des plateformes en ligne, des opérateurs de télécoms, des forces de l'ordre et des pouvoirs publics. À défaut d'un tel alignement, il existe un risque réel d'effets de déplacement, la fraude se déplaçant vers le maillon le plus faible. **Éviter une telle fragmentation est essentiel pour garantir que la Belgique ne devienne pas une cible attractive pour la fraude en ligne organisée.**

Ce plan d'action appelle dès lors à un soutien politique fort, à une coordination claire et à un cadre juridique facilitateur permettant l'innovation, le partage d'informations et une application efficace, tout en respectant pleinement les droits fondamentaux. Seule une approche partagée, équilibrée et intégrée permettra de s'attaquer à la fraude en ligne à sa source, de renforcer durablement la protection des clients et de préserver la confiance dans l'écosystème financier numérique.

Document joint : exemples de processus de fraude

Les banques interviennent principalement en aval du parcours — pendant et après la transaction — tandis que le phishing est généralement initié via les médias sociaux et des sites web frauduleux

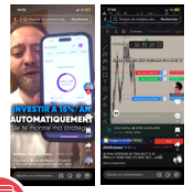
Processus de fraude – **Phishing**



Les fraudes à l'investissement sont intrinsèquement facilitées par les médias sociaux et les canaux de télécommunications, qui agissent comme des chambres d'écho, tandis que les banques n'interviennent qu'au stade de la transaction[45].

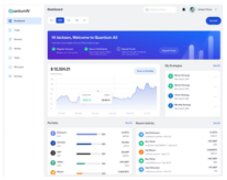
Processus de fraude – **Fraude à l'investissement**

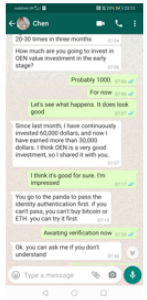
PRÉPARATION – Création de la plateforme
- Une ferme à fraude basée à l'étranger met en place une fausse plateforme de cryptomonnaie hébergée via Cloudflare, en utilisant des identités volées et en créant des publicités sur TikTok.



EXÉCUTION – Approche
- La victime clique sur une publicité sponsorisée « investissement en cryptos à haut rende-ment » sur TikTok et est rapidement contactée par un « conseiller financier » via WhatsApp.

EXÉCUTION – Convaincre
- L'escroc instaure un climat de confiance en présentant de faux tableaux de bord affichant des profits.
- Il appelle sans cesse afin de créer un sentiment d'urgence et d'inciter à investir davantage.





RÉALISATION – Transfert & retrait des fonds
- La victime transfère des fonds depuis ses comptes bancaires, puis suit des instructions pour effectuer des paiements supplémentaires et convertir les fonds en cryptomonnaies via une plateforme d'échange.
- Les fonds transitent par des comptes de mules financières, sont convertis en cryptomonnaies puis retirés ; le domaine hébergé via Cloudflare est ensuite fermé par les escrocs.

POST-Fraude – Enquête et récupération
- La victime contacte sa banque et dépose plainte auprès de la police belge.
- Le CCB est informé et la plateforme est signalée.
- Quelques semaines plus tard, la banque parvient à récupérer une partie des fonds grâce à la collaboration avec les forces de l'ordre et les institutions bancaires du pays étranger.

[4] "Dans la jungle des néobanques : arnaques, trafics et clients lésés" – Arte
[5] Extrait de presse de la BBC