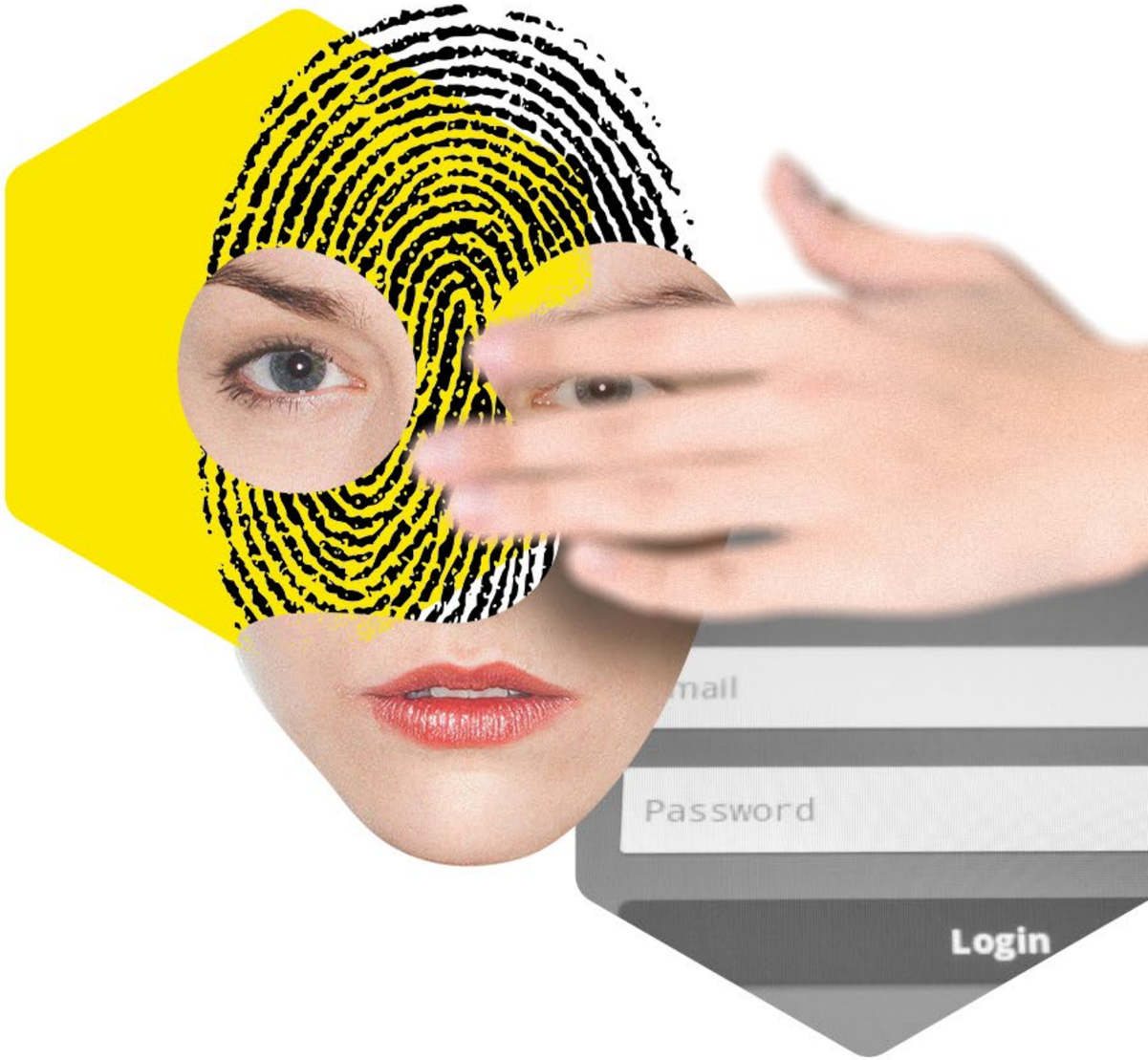
Livre blanc

Lutte contre la fraude et expérience client

Le refus du dilemme



France FinTech

onfido

Édito

La crise sanitaire a été un véritable catalyseur de la transformation digitale des entreprises. Celle-ci s'est accélérée d'environ 7 ans selon une étude de McKinsey*. 55 % des interactions avec les clients ont désormais lieu sur les médias numériques en Europe, ce qui représente un bond en avant de 3 ans par rapport aux prévisions pré-crise. Le secteur des services financiers, qui accusait jusqu'à maintenant un certain retard, a connu l'accélération la plus forte.

L'évolution des comportements, que ce soit en BtoC ou BtoB, est phénoménale et le retour en arrière semble difficile. Les clients désireux d'éviter le contact physique en agence se sont habitués aux services en ligne par la force des choses et sont devenus très vite beaucoup plus exigeants. En conséquence, les acteurs des services financiers doivent non seulement être en capacité d'offrir tous leurs services en ligne, mais ils doivent également proposer une expérience aussi simple, fluide et instantanée que celle offerte par les nouveaux acteurs du secteur financier, sous peine de perdre leurs clients.

Or si les usagers se sont rapidement adaptés aux services en ligne, ils ne sont malheureusement pas les seuls. Les fraudeurs ne sont pas en reste. L'étude annuelle d'Onfido sur l'état de la fraude à l'identité** à travers le monde montre ainsi à la fois une accélération de la croissance de la fraude et une professionnalisation des techniques des fraudeurs. Si cette tendance affecte tous les secteurs, le e-commerce et les services financiers sont les plus affectés.

Pour les acteurs assujettis à la réglementation LCB FT (Lutte contre le blanchiment d'argent et le financement du terrorisme), la lutte contre la fraude était une priorité en 2020, elle

Préface

C'est bien connu, "les voleurs courent souvent plus vite que les gendarmes »... Ils entretiennent d'ailleurs une relation dialectique, l'un rendant l'autre toujours plus intelligent, ce qui explique que la course n'a jamais de fin.
Il est également bien connu que l'argent attire plus que tout autre chose les voleurs et fraudeurs et ce, depuis la nuit des temps. Les services financiers sont donc un de leurs terrains de jeu favoris. La fraude dans ce domaine revêt de nombreuses formes : détournement et recyclage d'argent criminel notamment.
La numérisation des opérations et la technologie en général ont à la fois permis de développer des outils de prévention et de détection des fraudes, mais aussi ouvert la voie à toutes sortes de tentatives délictueuses nouvelles.
Les acteurs se sont engagés dans « une course à l'armement » qui s'accélère, à due concurrence de la numérisation toujours plus poussée des services, de la pression des régulateurs et par-dessus tout de l'exigence de sécurité des consommateurs.
De ce point de vue, la recherche algorithmique, la robotisation, l'intelligence artificielle et la blockchain sont autant de leviers mobilisables par le secteur.
La sécurité et le respect de la loi et du règlement ne sont pas une option pour les acteurs de cette industrie. Ils sont en effet les fondations de la confiance qui est consubstantielle à leur raison d'être. Le vocabulaire financier reflète d'ailleurs cet état de fait; crédit, fiduciaire, etc trouvent leur racine latine dans ce concept.
Un « accident de parcours » en terme de fraude peut considérablement porter atteinte à la réputation d'un établissement, petit ou grand, lui faire encourir des pertes d'exploitation considérables et des amendes qui ne le sont pas moins (rappel : dans le monde, les banques ont payé 312 milliards de dollars d'amende entre 2008 et 2016[1]).
C'est donc un thème d'innovation et de réflexion particulièrement intéressant.
C'est à lui que France FinTech et Onfido, deux entités fortement engagées dans la lutte contre la fraude, s'attaquent dans ce nouveau livre blanc, avec le soutien de notre superviseur (ACPR), Olivier Fliche, directeur du pôle FinTech Innovation, et Timothée Dufour, chargé de mission au pôle FinTech Innovation que je remercie chaleureusement.
Puisse sa lecture nous inciter tous à encore davantage de coopération qui est toute l'ambition de cet opuscule.

Alain Clot,
Président France FinTech

1 Source : Bloomberg (2017)

le restera en 2021. Leur défi sera de savoir comment déterminer son seuil de risque et comment concilier expérience client optimale et efficacité de la protection. Dans un contexte complexifié par les évolutions, il nous a paru pertinent de partager les réflexions des acteurs concernés et les solutions qu'ils mettent en œuvre.

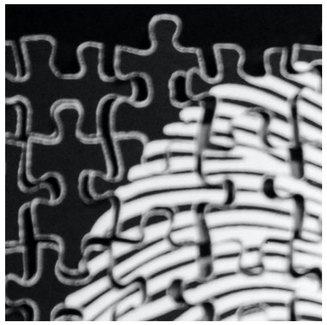
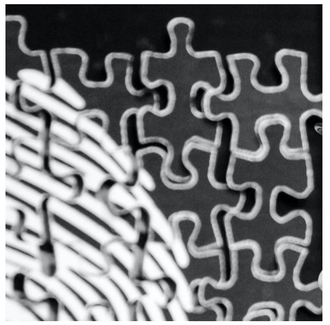
Onfido et France FinTech se sont donc associés afin d'interroger les entreprises du secteur financier, mais aussi le régulateur, sur les évolutions et les enjeux de la gestion de la fraude dans la cadre de l'entrée en relation avec les clients, ainsi que sur les solutions permettant de minimiser les risques et maximiser la conversion. Plus de 60 décideurs de grands groupes et de FinTech ont partagé leur expérience et leurs réflexions au sein de ce livre blanc sur la « lutte contre la fraude et expérience client : Le refus du dilemme ». A partager sans modération !

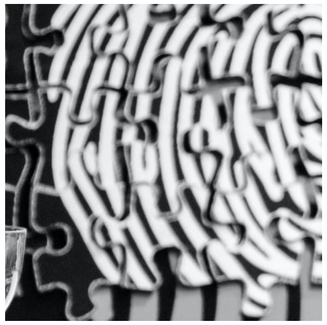
Très bonne lecture !

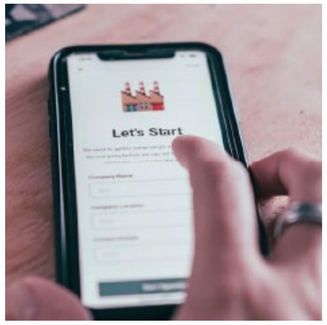
Gimena Diaz - VP SEMEA Onfido

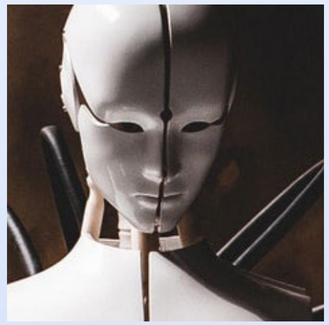
*McKinsey Global Survey of executives July 2020 - https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

**Onfido Identity Fraud Report 2020 - https://onfido.com/resources/fr/fraude-a-l-identite-rapport-2020





Principaux enseignements

Malgré la diversité de leurs activités, de leur dimension et de leur historique, les avis des différents acteurs interrogés sur la lutte contre la fraude s'avèrent relativement consensuels.

Résumons-les en 6 points :

1. L'usurpation d'identité et la fraude documentaire sont aujourd'hui les principaux fléaux à combattre lors de l'entrée en relation.
2. Les solutions en place, combinant plusieurs outils, permettent de contenir la menace et leur impact sur l'expérience utilisateur est jugée acceptable.
3. L'évolution constante de la fraude, les opportunités technologiques et les attentes des clients incitent toutefois les entreprises à faire régulièrement évoluer leurs dispositifs.
4. Le contrôle d'identité biométrique et le recours au selfie vidéo sont plébiscités, bien que parfois suspendus aux futures certifications par l'ANSSI, en lien avec les exigences réglementaires, tandis que l'analyse de données prend une importance croissante.
5. Une majorité se prononce pour le maintien de dispositifs hybrides, intelligence artificielle et expertise humaine, qui offrent le meilleur compromis entre, d'une part, réactivité et coût maîtrisé et, d'autre part, efficacité maximale.
6. La mise en œuvre d'une identité digitale nationale, fortement désirée, soulève beaucoup d'espoirs pour l'amélioration de l'expérience client.

Méthodologie

- **Étude qualitative** sous forme d'entretien auprès d'acteurs clés des services financiers et de l'ACPR du 30 novembre 2020 au 31 janvier 2021.
- **Enquête en ligne** du 12 janvier au 3 mars auprès de banques, d'assureurs et FinTech, de sociétés de conseil et d'entreprises de services.

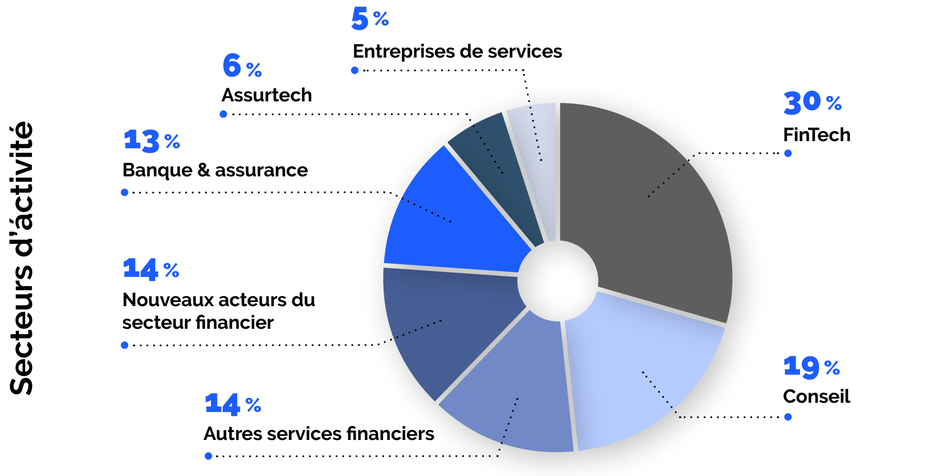
65 participants représentatifs de l'écosystème financier français

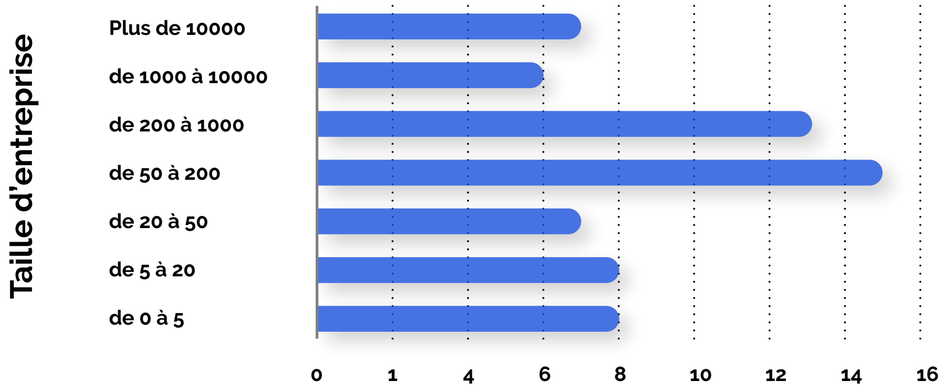
France FinTech, en partenariat avec Onfido, a réalisé une enquête qualitative sous forme d'interviews approfondies de 50 à 60 minutes auprès de 15 entreprises du secteur financier et de responsables du pôle FinTech-Innovation de l'ACPR.

Cette étude a été complétée par une enquête en ligne à laquelle 49 professionnels ont répondu.

75 % des répondants sont issus du secteur de la banque, de l'assurance et des services financiers avec la participation d'acteurs historiques (banque corporate) et de FinTech (nouveaux acteurs du secteur financier, assurtech et acteurs des paiements).

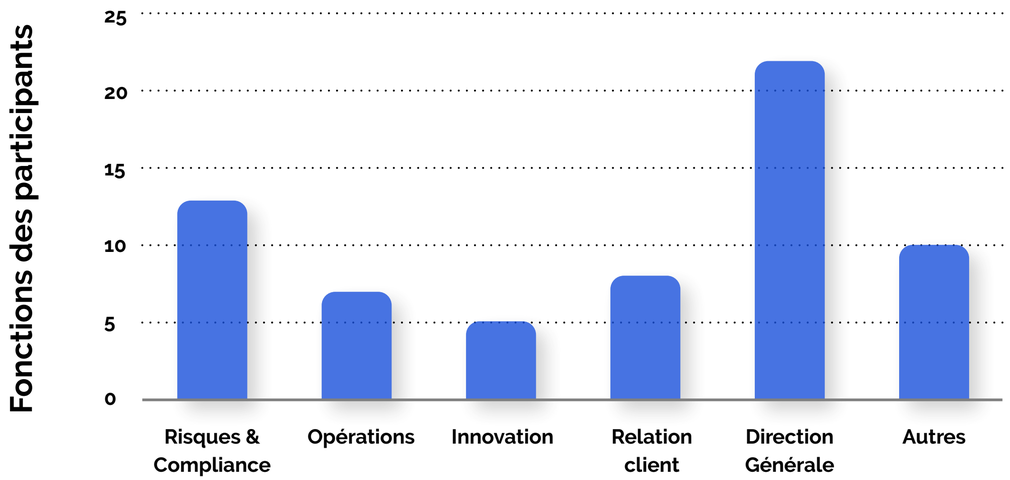
25 % des participants appartiennent à des sociétés d'audit et de conseil ou à des entreprises de services non financiers (e-commerce, gaming).

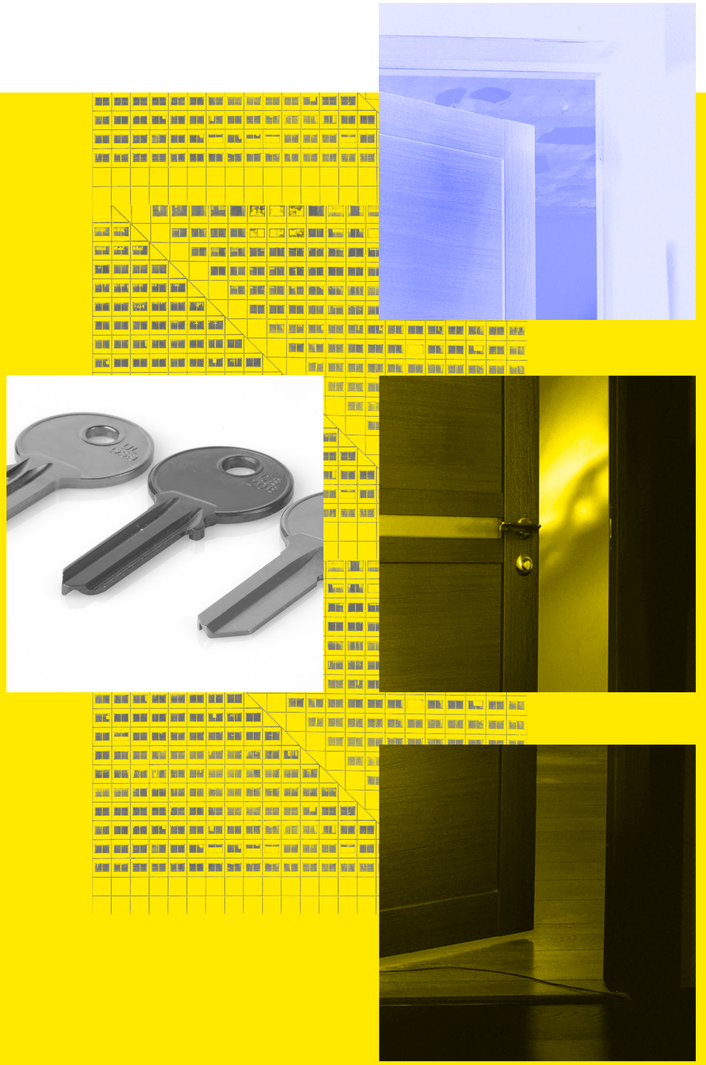




Des profils de participants de haut niveau

63 % des répondants occupent des postes de direction générale ou des fonctions de directeur de pôles concernant la gestion des risques & la conformité, les opérations, l'innovation ou la relation client.





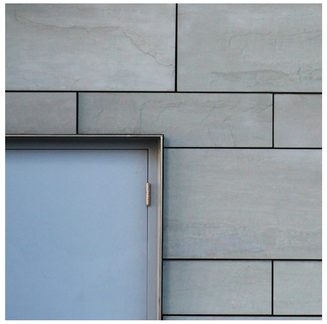
SOMMAIRE

Introduction

Depuis leur naissance jusqu'à aujourd'hui, les services financiers sont victimes d'une fraude toujours plus sophistiquée, profitant des progrès technologiques les plus pointus. Les acteurs du secteur sont donc engagés dans une course à l'armement, déployant sans cesse de nouvelles parades qui leur permettent de maîtriser la menace.

Pour la plupart des entreprises (85 % de notre échantillon), la bataille contre la fraude est une priorité stratégique et pour plus de 4 sur 10, elle figure en tête de leurs préoccupations.

Quelle est la situation de la fraude et de la lutte contre la fraude en 2021 dans le secteur financier ? Quelles sont les dernières tendances et évolutions pour lutter efficacement contre la fraude tout en garantissant la satisfaction des clients ? Que nous réserve l'avenir ? Voici quelques éléments de réponse recueillis auprès des premiers intéressés.

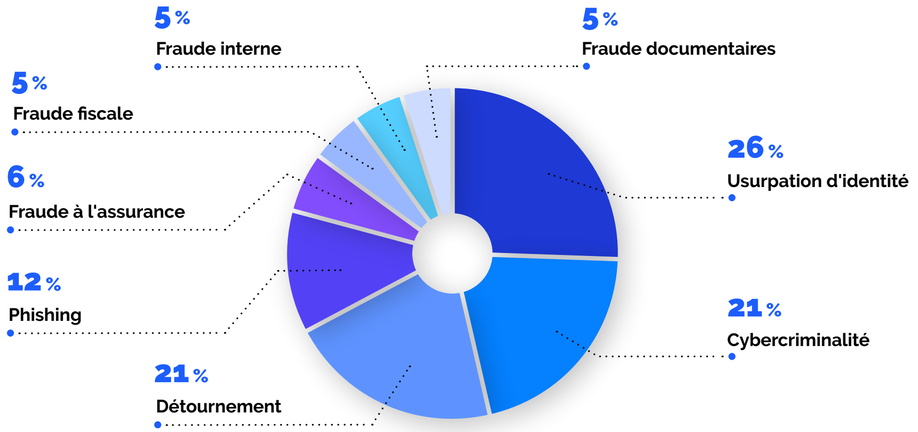


I

UN ÉTAT DES LIEUX DE LA FRAUDE

La fraude en général

Pour les entreprises interrogées, outre la fraude au paiement (y compris la fraude « au président »), qui reste un domaine préoccupant, notamment dans l'écosystème du e-commerce, la principale préoccupation concerne l'usurpation d'identité. Qu'elle soit exercée à une échelle individuelle, pour le gain personnel du fraudeur, ou qu'elle prenne une dimension quasi-industrielle, notamment dans le cadre de pratiques de blanchiment ou de financement du terrorisme, elle est la première source d'inquiétude de plus d'un tiers des répondants à notre enquête.



« L'usurpation d'identité et la fraude sur les paiements sont les principales menaces rencontrées par les banques. » (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

Historiquement très présente et très problématique dans l'univers du crédit, la fraude dite documentaire, qui consiste à falsifier des justificatifs (par exemple les feuilles de salaire) afin, par exemple, d'obtenir un prêt, tend désormais à céder le pas, tandis que les attaques par hameçonnage, visant collaborateurs ou clients, utilisées pour toutes sortes de malversations (et non uniquement la fraude), tendent à devenir le mal du XXIème siècle.

« En 2017, nous étions surtout confrontés à la fraude documentaire, mais, depuis 2018, l'usurpation d'identité est en recrudescence. » (Antoine Saudray, Younited Credit, Enterprise Risk Manager & DPO)

« La fraude ne se limite pas uniquement à la falsification documentaire, plus simple à détecter. Le risque majeur concerne l'usurpation d'identité avec des pièces authentiques.» (Jean-Baptiste Boix, Floa, Responsable fraude et cybercriminalité)

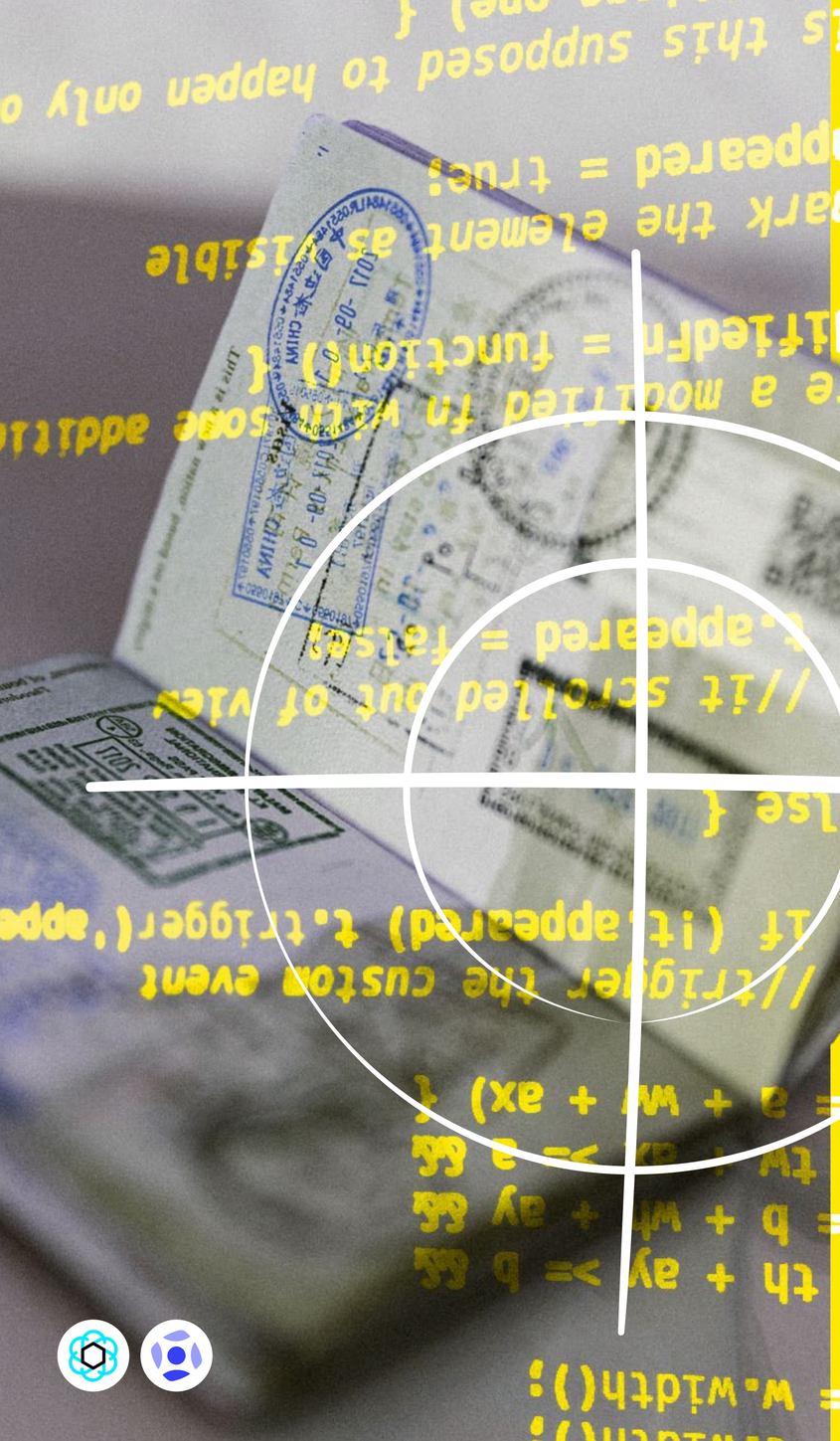
La professionnalisation de la fraude se fait fortement ressentir depuis quelques années. Ainsi, les contournements et autres ripostes aux moyens de défense mis en œuvre par les acteurs de la finance sont développés de plus en plus rapidement et les failles ou faiblesses détectées dans les systèmes sont exploitées immédiatement, à grande échelle.

L'impact de la pandémie

La crise sanitaire semble avoir engendré une augmentation significative des cas de fraude. Cependant, hormis, côté entreprises, l'exploitation de l'actualité à des fins d'attaque ciblée (détournement du dispositif de Prêt Garanti par l'État, blanchiment d'argent à travers la vente de masques de protection…), les techniques déployées n'ont pas fondamentalement évolué depuis l'apparition de la pandémie.

Selon toute vraisemblance, la croissance s'expliquerait d'abord par le recours massif aux interactions en ligne à l'occasion des mesures de confinement et de restriction des déplacements. Celles-ci ont démultiplié les opportunités d'offensives pour les cybercriminels, les usagers, souvent isolés, se trouvant plus vulnérables. Les efforts de communication des banques après la première vague ont heureusement permis de contenir le phénomène au cours du deuxième confinement.

« La fraude s'industrialise et se professionnalise. On enregistre davantage de cas d'usurpation d'identité en bande organisée, avec des schémas d'ingénierie sociale toujours plus élaborés. » (Jean-Baptiste Boix, Floa, Responsable fraude et cybercriminalité)



Focus sur l’ entrée en relation

Naturellement, les risques d’usurpation d’identité, de falsification de documents ou de déclarations mensongères sont particulièrement sensibles (et beaucoup plus élevés) lors de l’entrée en relation, surtout quand celle-ci se déroule entièrement à distance. Toutefois, des problématiques supplémentaires doivent être prises en compte. C’est le cas, par exemple, avec les précautions spécifiques à prendre vis-à-vis des « personnes politiquement exposées ».

« Notre risque principal à l’ouverture de compte concerne les faux documents d’identité. » (Nadège Pupier, Lemonway, Chief Compliance and Risk Officer)

Sans surprise, les professionnels sont peu diserts sur les préjudices qu’ils subissent. Parmi les quelques cas explicites, ce sont les fraudes à la carte, lors d’opérations d’approvisionnement de compte, qui sont le plus souvent évoquées. Dans l’ensemble, le poids des coûts directs est plutôt minimisé, la lourdeur des dispositifs de lutte, surtout les équipes qui y sont consacrées, étant parfois soulignée.

« Le coût concerne surtout nos opérations, soit les personnes dédiées à la lutte contre la fraude à temps plein. » (Evan Proux, Lydia, Head of Fraud Operations)

L'éclairage de l'ACPR (Olivier Fliche, directeur du Pôle FinTech Innovation et Timothée Dufour, chargé de mission au pôle FinTech Innovation)

L'Autorité de Contrôle Prudentiel et de Résolution (ACPR), adossée à la Banque de France, est chargée de la surveillance des banques et des assurances en France. Elle contrôle les dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), mais également, au titre plus général des dispositifs de contrôle interne, les moyens mis en œuvre pour lutter contre la fraude.

De fait, les obligations de connaissance et de vérification de l'identité des clients posées par la réglementation LCB-FT rejoignent logiquement une des principales préoccupations des institutions financières, exposées aux tentatives d'usurpation d'identité lors de l'entrée en relation.

Ce sujet fait l'objet d'une attention soutenue de la part de l'ACPR dans le contexte de la transition de nombreuses activités économiques sur les médias électroniques. Il est directement lié aux réflexions sur la notion d'identité numérique, aujourd'hui encadrée par le règlement européen eIDAS. Ce dernier constitue donc le socle sur lequel reposent les critères spécifiques élaborés pour la LCB-FT.

Avec l'arrivée d'acteurs aux approches disruptives (N26, Revolut…), un groupe de travail a été constitué en 2019, regroupant des experts d'horizons divers, afin d'évaluer les questions pratiques soulevées à l'époque par la réglementation française relative à l'entrée en relation à distance. Ce groupe de travail a préconisé quelques modifications réglementaires, facilitant notamment le recours à des solutions certifiées de vérification d'identité à distance. Cette certification repose sur un référentiel technique, dont la réalisation a été confiée à l'ANSSI.

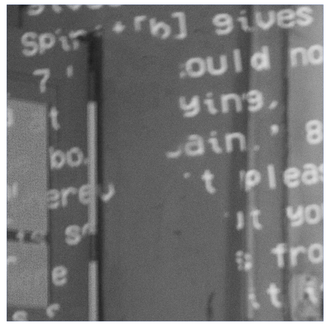
« L'ACPR ne délivre pas de label mais s'appuie sur l'expertise de l'ANSSI pour la validation technique des solutions. » (O. Fliche)

Le grand défi des autorités consiste à réaligner leur position au fil des évolutions constantes des risques de fraude et de blanchiment. Il s'agit d'abord d'adapter les mécanismes de protection à la sophistication croissante des menaces, notamment quand elles émanent d'organisations criminelles structurées. Les progrès technologiques rapides, par exemple, rendent possibles de nouvelles formes de fraude ou d'usurpation d'identité qui étaient auparavant considérées comme non rentables et, en conséquence, restaient ignorées.

« Il y a quelques années, la vérification de l'utilisateur à partir d'un selfie dynamique aurait pu sembler acceptable. Aujourd'hui, selon le référentiel de l'ANSSI, un contrôle vidéo est indispensable. » (O. Fliche)

A contrario, les mêmes avancées permettent aussi d'envisager de nouvelles approches de défense, plus performantes, moins complexes à déployer et moins coûteuses. Par exemple, l'ouverture d'un service de contrôle électronique des passeports permettrait de détecter plus facilement les documents falsifiés.

La publication du référentiel cette année devrait permettre aux institutions implantées dans l'Hexagone de développer rapidement des parcours d'entrée en relation à l'état de l'art. Mais elles devront rester agiles : les règles du jeu seront vraisemblablement appelées à changer fréquemment.



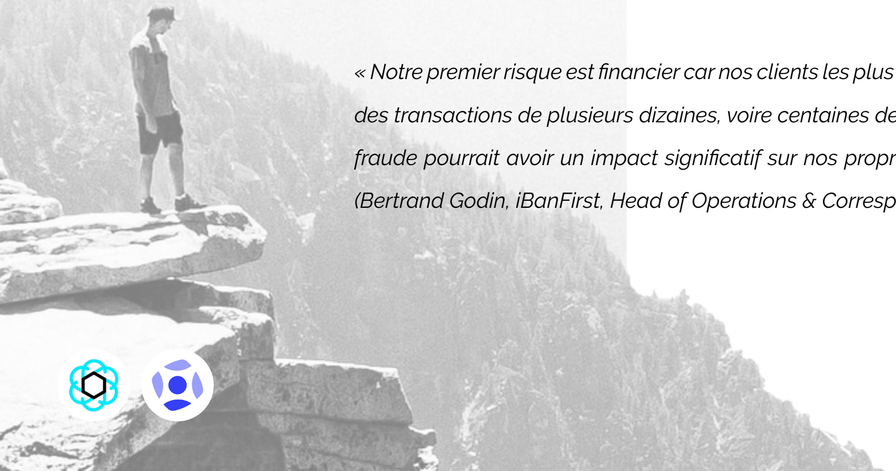
II

LES ENJEUX POUR LES SERVICES FINANCIERS

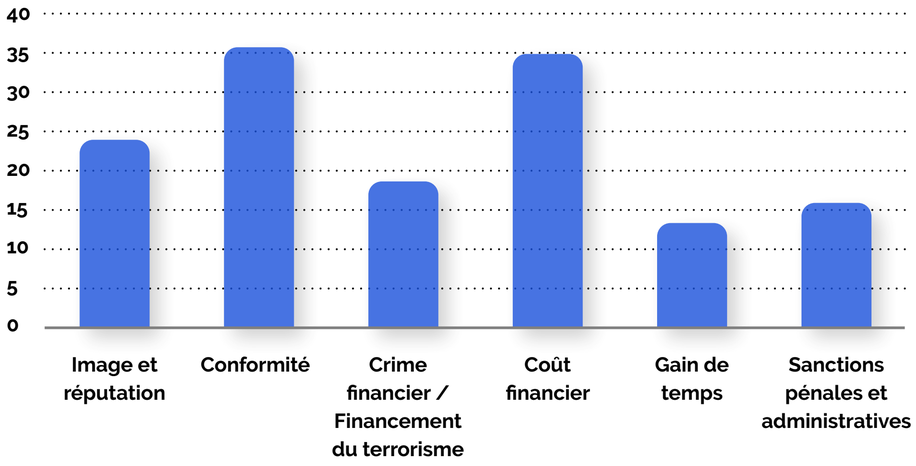
Face aux menaces, les institutions et start-up financières appréhendent des enjeux de natures différentes, avec des priorités qui diffèrent selon leur typologie.

Les jeunes pousses de la FinTech sont les plus sensibles au risque opérationnel : elles craignent par-dessus tout les pertes financières engendrées par la fraude, susceptible de représenter un danger existentiel si elle n'est pas maîtrisée.

« Notre premier risque est financier car nos clients les plus importants effectuent des transactions de plusieurs dizaines, voire centaines de millions d'euros. Une fraude pourrait avoir un impact significatif sur nos propres flux de trésorerie.» (Bertrand Godin, iBanFirst, Head of Operations & Correspondent Banking)



Quels sont les enjeux de la lutte contre la fraude pour votre société ?



En revanche, les banques, pour lesquelles les impacts des malversations sur les résultats sont peut-être moins sensibles, se disent davantage préoccupées par le respect des exigences réglementaires et les conséquences d'éventuelles sanctions, autant sur les montants potentiellement engagés que sur les conséquences indirectes en termes d'image.

« Notre objectif essentiel est d'être conforme à la réglementation. » (Jean-Eloi Rateau, Qonto, Head of regulatory and compliance)

Notons toutefois que, même s'il n'est placé en tête de leurs angoisses que par une minorité des organisations interrogées, le risque réputationnel « direct » est toujours présent à l'esprit des start-up, puisqu'un des défis majeurs qu'elles doivent relever dans leurs phases d'émergence et de croissance est de conquérir la confiance de leur clientèle.

« Nous avons un enjeu de réputation extrêmement fort car nous devons inspirer confiance aux parents qui équipent leurs enfants de notre solution. » (Amine Bounjou, Kard, Co-Founder & COO)

« En tant que FinTech nous devons conquérir la confiance des acteurs historiques du marché, pour ne pas être stigmatisés et bloqués par ces acteurs. » (Jean-Eloi Rateau, Qonto, Head of regulatory and compliance)

« Pour nous, l'enjeu réputationnel est très important pour attirer les investisseurs ». (Antoine Saudray, Younited Credit, Enterprise Risk Manager & DPO)

Sur le plan opérationnel, l'entrée en relation est également confrontée à des enjeux spécifiques en matière de lutte contre la fraude. La connaissance du client et de son « profil » (par exemple son domaine d'activité, pour une entreprise) et la compréhension des catégories de risque associées sont ainsi des prérequis essentiels.

En conséquence, se posent des questions critiques sur les mécanismes de vérification à activer, y compris pour des contrôles croisés, et sur les meilleures approches à retenir – quand déclencher la validation de l'identité, comment limiter les effets indésirables sur l'expérience utilisateur.

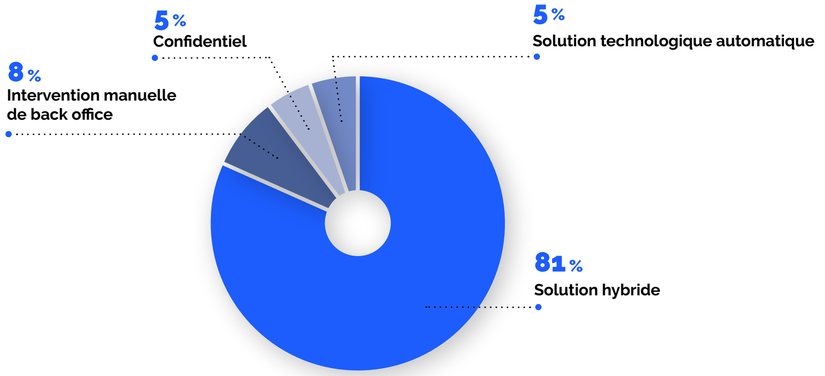
III

LES SOLUTIONS MISES EN ŒUVRE

Quelles solutions ?

Dans leur stratégie défensive, les entreprises interrogées déploient généralement un arsenal diversifié, qui leur permet à la fois d'adresser toutes les facettes des risques contre lesquelles elles doivent se prémunir et d'améliorer la fiabilité de leurs dispositifs grâce à la redondance et aux recoupements entre sources distinctes.

Moyens de détections de la fraude



« Nous avons opté pour une double mesure de vérification d'identité : un virement bancaire et le contrôle de la pièce d'identité (avec la solution d'Onfido). » (Bertrand Godin, iBanFirst, Head of Operations & Correspondent Banking)

« Nous avons une exemption au-dessous de 150 euros collectés. Afin de maximiser l'acquisition de clients, nous attendons donc le franchissement du plafond ou des signes de fraude pour déclencher une vérification d'identité. » (Evan Proux, Lydia, Head of Fraud Operations)

Les dispositifs mis en œuvre comprennent donc notamment des solutions de contrôle d'identité et de vérification de documents, électroniques ou imprimés, qui s'appuient sur des technologies variées : intelligence artificielle (machine learning) par exemple pour l'analyse comportementale, lecture automatique de documents, recours à des listes noires, accès à des plates-formes de données ouvertes ou publiques… Environ deux tiers des acteurs font appel à une solution externe pour ces services.

« Nous avons mis en place un système de KYC instantané : l'identité du client est vérifiée en temps réel, il peut alors commencer à traiter des opérations sans délai. » (Nadège Pupier, Lemonway, Chief Compliance and Risk Officer)

« Nous avons des bases de données officielles pour vérifier que nos emprunteurs ne sont pas sur des listes de sanction ou des listes de personnes politiquement exposées. » (Julien Ramezani, October, Head of Client Operations)

Les solutions d'analyse de données (« big data »), comprenant autant des outils de « business intelligence » relativement classiques (SAS, Qlik, Tableau et consorts) que des technologies d'intelligence artificielle, sont largement mises à contribution dans la lutte contre la fraude, dans toutes ses dimensions. Elles peuvent s'appuyer sur une multitude de sources d'informations facilement accessibles : présence des internautes et des entreprises sur les réseaux sociaux, caractéristiques des moyens d'accès au web (permettant une identification), répertoires publics de sociétés… jusqu'aux comptes bancaires auxquels une connexion est parfois demandée lors de l'entrée en relation.

Les approches biométriques, à savoir essentiellement les séquences vidéo de validation de la correspondance entre le client et les justificatifs d'identité fournis, sont appelées à prendre une place de plus en plus importante en 2021, en grande partie grâce aux avancées réglementaires en la matière.

« Les nouvelles méthodes, avec la vidéo à "preuve de vie" et la biométrie vont permettre un parcours en temps réel, au profit du client. » (Pierre Villeroy de Galhau, Boursorama, Directeur Stratégie & Innovation)

« La détection de documents falsifiés et la vidéo à "preuve de vie" permettent de réduire grandement les risques. » (Clément Mazeries, Mangopay, Compliance Officer)

Les processus combinent des moyens automatisés et humains, autant par conviction – d'une meilleure fiabilité et/ou des valeurs de proximité et d'ancrage local de l'établissement, jusqu'à imposer parfois un rendez-vous physique – que par anticipation des exigences réglementaires (cf. encadré). Cette approche hybride n'est guère remise en question à moyen terme : seuls 5 % des participants à l'enquête expriment leur préférence, dans l'idéal, pour une automatisation totale.

« Quand notre solution de vérification de justificatif d'identité rejette un document, nous recourons à une vérification manuelle. » (Nadège Pupier, Lemonway, Chief Compliance and Risk Officer)

« L'objectif n'est pas de remplacer l'humain dans les processus, mais d'automatiser les tâches qui peuvent l'être pour les rendre plus efficaces. » (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

« On ne peut pas se passer d'une vérification par un opérateur quand il y a une anomalie détectée : le cerveau humain reste nécessaire. » (Nadège Pupier, Lemonway, Chief Compliance and Risk Officer)

« Pour nous, l'idéal serait la vérification à 100 % automatique, mais nous n'y sommes pas encore tout à fait. » (Eric Mignot, +Simple, Founder and Chairman)

Les contours de la certification ANSSI pour un nouveau service de confiance

- L'ANSSI est l'Agence nationale de la sécurité des systèmes d'information. Rattachée au Premier ministre, son rôle est de faciliter la prise en compte des questions de cybersécurité en France.
- L'ANSSI a publié un référentiel d'exigences applicables aux PVID, Prestataire de vérification d'identité à distance, et vient de créer une certification afin d'établir un nouveau service de confiance.
- Ce référentiel apporte un cadre technique et réglementaire commun pour une protection accrue des utilisateurs et une sécurité renforcée lors de l'entrée en relation à distance. Elle représente une opportunité de faire évoluer les parcours digitaux pour les acteurs régulés afin d'améliorer l'expérience utilisateur.

Voici les points clés du référentiel d'exigences pour les PVID

- Le référentiel ANSSI formule des exigences applicables aux PVID, que ces services soient asynchrones, synchrones avec interaction humaine, synchrones sans interaction humaine, internes ou externes.
- Seule la **vérification d'identité à distance de personnes physiques** entre, à ce jour, dans le champ d'application du présent référentiel.
- Seuls les **services de vérification d'identité à distance hybrides** peuvent respecter les exigences du présent référentiel ;
- Le présent référentiel prévoit que les besoins en termes de disponibilité du service de vérification d'identité à distance soient identifiés par le service métier et définis contractuellement entre le prestataire et le commanditaire dans la convention de service.

Activités du service de vérification d'identité à distance

(extrait du référentiel d'exigences)

Le service de vérification d'identité à distance réalise les quatre étapes successives :

- l'acquisition des données d'identification,
- la vérification des données d'identification,
- la constitution du dossier de preuve,
- la transmission des résultats

1. **Acquisition des données d'identification**

   Cette étape consiste à acquérir les données d'identification relatives à l'utilisateur, à savoir et a minima, d'une part une vidéo du visage de l'utilisateur et d'autre part une vidéo du titre d'identité présenté par l'utilisateur ou les données d'identification relatives à l'utilisateur (dont la photo du visage de l'utilisateur) stockées dans le composant de sécurité du titre d'identité présenté par l'utilisateur. Les acquisitions de ces différents éléments peuvent être réalisées simultanément, ou dans un ordre indifférent. Le terminal utilisé pour acquérir les données d'identification peut être celui de l'utilisateur, celui du prestataire ou celui du commanditaire.

2. **Vérification des données d'identification**

   Sur la base des données d'identification acquises lors de l'étape précédente, cette étape consiste à vérifier à l'aide de traitements, à la fois automatisés et humains, que le titre d'identité présenté par l'utilisateur est authentique, que l'utilisateur est le détenteur légitime du titre d'identité. La vérification du fait que l'utilisateur est le légitime détenteur du titre d'identité comprend :

   - une vérification de l'authenticité du titre d'identité présenté ;
   - une détection du caractère « vivant » de l'utilisateur représenté dans la vidéo ;
   - une comparaison du visage de l'utilisateur extrait de la vidéo de l'utilisateur avec soit la photo de l'utilisateur extraite de la vidéo du titre d'identité soit la photo de l'utilisateur extraite du composant de sécurité du titre d'identité. Ces vérifications peuvent être réalisées simultanément, ou dans un ordre indifférent.

3. **Constitution du dossier de preuve**

   Cette étape consiste à créer un dossier de preuve comprenant les données d'identification acquises, les résultats détaillés issus des traitements automatisés et humains de la vérification des données d'identification ainsi que le résultat de la vérification d'identité transmis au service métier.

4. **Transmission du résultat de la vérification d'identité**

   Cette étape consiste à transmettre au service métier du commanditaire le résultat (échec ou succès) de la vérification d'identité, une synthèse des résultats des traitements automatisés et humains de la vérification des données d'identification, ainsi qu'un sous-ensemble des données d'identification.

Pour en savoir plus :

https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf

Quels résultats ?

Hormis quelques entreprises qui ne s'expriment pas car leur stratégie est en cours de transition, tous les répondants se déclarent satisfaits des solutions qu'ils exploitent et, plus particulièrement, de leur capacité réelle à maintenir les niveaux de fraude au plus bas. Ainsi, près de deux tiers des répondants à notre enquête indiquent observer un taux de fraude à l'entrée en relation inférieur à 1 %.

« Depuis trois ans nous avons des objectifs très ambitieux que nous avons atteints. » (Jean-Baptiste Boix, Floa, Responsable fraude et cybercriminalité)

Une moitié d'entre eux concèdent cependant qu'ils perçoivent quelques pistes d'amélioration restant à explorer. Le facteur d'inquiétude le plus fréquent est la vitesse d'évolution des menaces et la difficulté à suivre le rythme dans l'arsenal défensif.

« La fiabilité de notre solution de contrôle d'identité nous satisfait à 100 %, mais nous regrettons de ne pas pouvoir encore proposer une réponse immédiate ou en quelques secondes. » (Amine Bounjou, Kard, Co-Founder & COO)

Par ailleurs, bien que seuls quelques acteurs parmi les plus mûrs mesurent effectivement la contribution de chaque outil déployé à la réduction des risques, les coûts de mise en œuvre des dispositifs de lutte contre la fraude paraissent raisonnables, voire faibles, en comparaison des pertes, directes et indirectes, évitées.

« Nous disposons d'indicateurs qui nous permettent de mesurer, pour chaque étape du parcours, le volume de fraude évité et l'attrition client. » (Jean-Baptiste Boix, Floa, Responsable fraude et cybercriminalité)

« Les montants des investissements sont finalement assez faibles comparés aux risques encourus. » (Bertrand Godin, iBanFirst, Head of Operations & Correspondent Banking)

Le défi de l'expérience utilisateur

Les impacts sur l'expérience utilisateur suscitent, en revanche, des réactions plus contrastées. Ainsi, si tous les répondants sont confrontés au défi de trouver l'équilibre idéal entre le niveau de protection et les frictions engendrées sur le parcours du client, certains s'inquiètent des taux de rejet indus (par exemple en raison de documents déclarés illisibles par un logiciel mal calibré) tandis que d'autres considèrent que les nouveaux outils disponibles simplifient l'accès (un contrôle vidéo est mieux accepté que la numérisation et l'envoi de deux documents d'identité). Pourtant, l'optimisme est de rigueur, puisque personne ne doute de la possibilité à l'avenir d'atteindre un bon compromis entre sécurité et fluidité.

Aujourd'hui, la durée moyenne des parcours d'entrée en relation montre de grandes variations, dues pour une grande partie à des exigences réglementaires différentes selon les métiers. Pour presque la moitié des entreprises interrogées, à moins de 5 minutes, elle paraît optimale, mais une sur sept avoue dépasser une journée, ce qui laisse entrevoir un besoin d'accélération.

Les taux d'abandon révèlent également des écarts importants : s'il est maîtrisé selon la plupart des professionnels interrogés, il dépasse tout de même 50 % dans une fraction non négligeable de cas. La cause principale de l'attrition est imputée à la complexité des processus eux-mêmes (formulaires trop longs, justificatifs à fournir…), alors que les obstacles purement techniques (manipulation des outils) sont considérés beaucoup moins gênants.

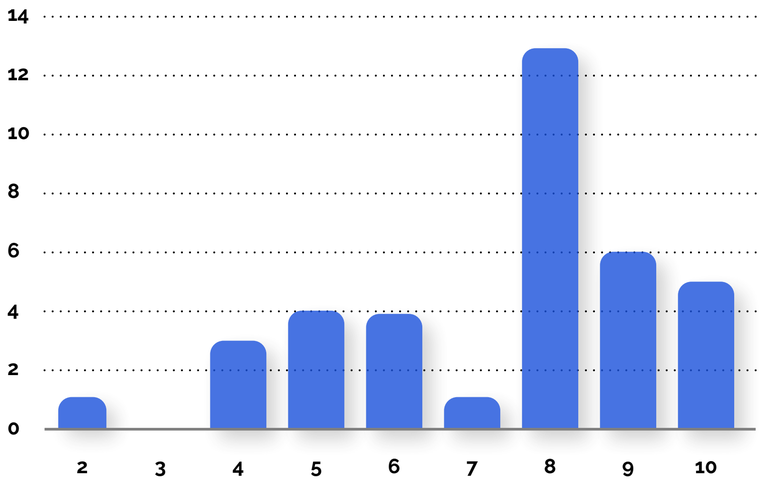
« Nous sommes constamment dans la recherche de l'équilibre idéal entre des mesures contraignantes et efficaces pour lutter contre la fraude et une dégradation minimale de l'expérience utilisateur par les contrôles.» (Evan Proux, Lydia, Head of Fraud Operations)

« Afin d'améliorer l'expérience client, en réduisant le nombre de questions posées au client, nos robots recherchent et exploitent un maximum d'informations disponibles en open data. » (Eric Mignot, +Simple, Founder and Chairman)

Le sentiment qui prédomine : qu'il s'agisse d'une obligation réglementaire ou de prudence opérationnelle, les contrôles sont indispensables et l'impact sur l'expérience utilisateur inévitable, ce que confirment trois quarts des répondants à notre enquête.

Les clients semblent d'ailleurs partager ce constat, puisque, pour les organisations interrogées les plus performantes, les taux d'abandon restent maîtrisés. Il est également vrai que, dans certains cas, la présence de méthodes de contrôle sophistiquées constitue un facteur de réassurance et de confiance pour les clients.

Impact de la solution sur l'expérience client



Nombreuses sont les entreprises qui considèrent que les solutions de contrôle modernes améliorent l'expérience utilisateur.

Le point de vue d'un éditeur logiciel (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

En tant qu'éditeur international de solutions logicielles à destination des institutions financières, Sopra Banking Software est à la fois au cœur de l'action dans la lutte contre la fraude, qu'il lui faut intégrer dans son offre, et à l'écoute permanente des défis rencontrés par ses clients.

Dans cette dernière position, Stéphane Berger observe une forte évolution dans nombre de banques historiques. En raison de craintes liées à la pandémie, leurs clients sont devenus plus réticents que jamais à se rendre en agence, préférant la sécurité d'une relation à distance, y compris pour des opérations importantes, qu'ils peuvent aussi traiter au téléphone ou en visioconférence avec leur conseiller.

« Dans la situation actuelle, une banque qui exige un passage en agence pour conclure un prêt immobilier peut perdre des clients. » (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

Face à cette demande pressante, les résistances tendent à s'estomper. Les établissements historiques, conscients de l'écart qui les sépare encore des nouveaux entrants, notamment en termes d'expérience client, sont désormais à l'affût des solutions qui leur permettront de s'aligner sur l'état de l'art définis par ces derniers.

Naturellement, les risques de fraude sont au premier plan des préoccupations dans cette transition vers des parcours 100 % digitaux. Aux côtés des attaques sur les moyens de paiement, l'usurpation d'identité lors de l'entrée en relation fait probablement partie des

plus inquiétantes pour les responsables de la lutte contre la fraude.

Stéphane Berger se veut pourtant rassurant. Les outils existants sur le marché permettent de répondre de manière très satisfaisante aux menaces. Certes, il n'existe pas une parade universelle et il peut s'avérer complexe d'assembler tout l'arsenal nécessaire pour une protection maximale, mais celle-ci est à la portée de tous les acteurs.

Sopra Banking Software en fait la démonstration avec son approche d'intégration de composants fournis par divers partenaires. Entre collecte et analyse de toutes sortes de justificatifs, accès aux sources publiques pour la vérification des adresses, détection des incohérences dans les bulletins de salaires, recherche de l'empreinte digitale des personnes (entre autres sur les réseaux sociaux), connexion aux services des impôts ou aux comptes bancaires..., toutes sources recoupées et corrélées, sa plate-forme réduit les risques à un niveau infime.

« La mise en œuvre des solutions disponibles aujourd'hui permet de répondre efficacement à la menace actuelle. » (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

Outre la nécessité d'ajuster les mesures de défense au fil des progrès accomplis par les fraudeurs, les banques ont tout à gagner à profiter des évolutions technologiques afin, entre autres, de relever le niveau de leurs défenses à coût réduit. Ainsi, la mise en œuvre de capacités de calcul de plus en plus puissantes couplées à des technologies d'intelligence artificielle, par exemple, rend économiques des protections auparavant inaccessibles.

Les banques qui adoptent l'ensemble de ces dispositifs en sont très satisfaites, autant en raison de leur efficacité dans la lutte contre la fraude que par l'optimisation de l'expérience client qu'ils autorisent, notamment en limitant le nombre de documents à transmettre et en accélérant les prises de décision.

Il subsiste tout de même des acteurs qu'effraie l'idée de confier un certain nombre de contrôles à des logiciels. Ceux-là doivent être rassurés, par exemple en expliquant qu'il n'est pas question d'écarter toute intervention humaine. Les outils proposés doivent être considérés comme une assistance, prenant en charge une partie des tâches afin de fournir au décisionnaire les moyens d'exercer au mieux son rôle.

Dans un parcours d'entrée en relation entièrement digital, l'expérience utilisateur est automatiquement améliorée par rapport à celui qui requiert une rencontre physique avec un conseiller. Pour aller plus loin et atteindre l'idéal de la signature en 5 minutes, il n'est pas inutile de s'inspirer des nouveaux acteurs du secteur financier : ajustement des contrôles selon les circonstances (et les risques), pré-acceptation assortie de limites (peu contraignantes) en attendant une validation définitive...

« Quand les banques traditionnelles imposent le même processus, le plus sécurisé et le plus contraignant, dans tous les cas, les nouveaux entrants ajustent leurs exigences selon les circonstances. » (Stéphane Berger, Sopra Banking Software, Head of Digital Product Strategy)

En conclusion, la plus importante piste d'amélioration à considérer en matière de lutte contre la fraude serait l'instauration d'un véritable système d'identité numérique, à l'échelle nationale. Sans être la réponse ultime à tous les risques, il représenterait une avancée significative à la fois pour la protection des banques (et de leurs clients) et pour la qualité de l'expérience utilisateur.

IV

DEMAIN, QUELLES ÉVOLUTIONS ?

Les évolutions les plus présentes à l'esprit des acteurs consultés concernent à parts égales l'amélioration de l'expérience utilisateur et le renforcement des protections, en particulier en regard de la sophistication et de la professionnalisation croissante des fraudeurs. Dans une moindre mesure, les ajustements réglementaires, qui collent à l'actualité des menaces, sont aussi surveillés attentivement.

> *« Les exigences évoluent en fonction des menaces et des technologies. »*
> *(Olivier Fliche, directeur du pôle FinTech Innovation, et Timothée Dufour, contrôleur des assurances)*

Les préférences vont d'abord aux technologies émergentes (validation biométrique, accès direct aux comptes bancaires – via les API DSP2 –, captation automatique d'information…), qui contribuent simultanément aux deux objectifs. L'accélération des processus est également citée, en réponse aux attentes de réactivité des clients. Enfin, pour certains, l'éducation des usagers et des employés mériterait encore des efforts.

« Sur les profils risqués, nous réalisons des analyses complémentaires à base de recherche ouverte sur internet pour des contrôles de cohérence. » (Jean-Eloi Rateau, Qonto, Head of regulatory and compliance)

Plusieurs personnes interrogées attendent beaucoup de la généralisation de l'identité numérique, qui pourrait résoudre un certain nombre des difficultés rencontrées aujourd'hui avec la vérification des documents.

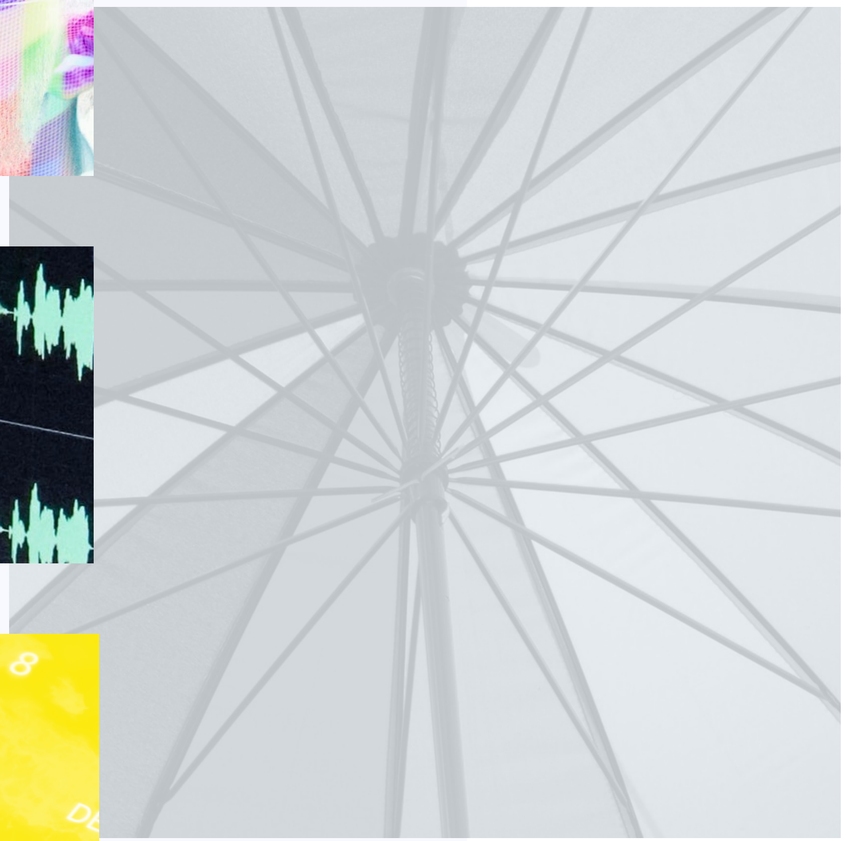
L'identité numérique

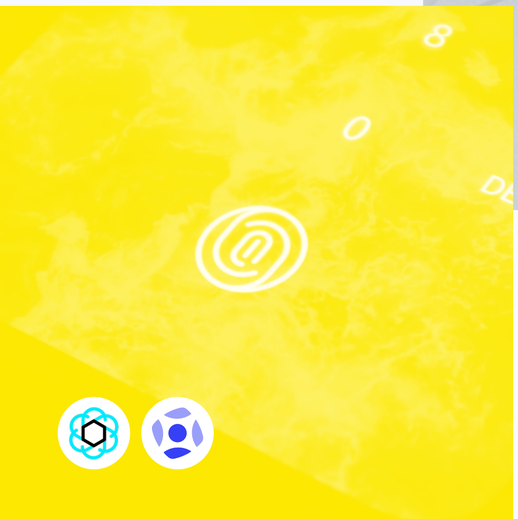
(Pierre Villeroy de Galhau, Boursorama, Directeur Stratégie & Innovation)

A l'avenir, chaque citoyen (et chaque entreprise) disposera d'une identité numérique, sorte de capsule virtuelle contenant une collection d'informations relatives à tous les domaines de la vie (banque, fiscalité, santé…) à laquelle son propriétaire peut donner accès en un clic, sélectivement, en fonction des besoins.

Ainsi, une souscription de crédit pourrait être soumise à la transmission d'un avis d'imposition ou de bulletins de salaire, tandis que la création d'un compte sur une boutique en ligne pourrait se contenter du nom et de l'adresse de l'individu…

Les données personnelles conservées dans ce coffre-fort digital seront authentifiées et certifiées, de manière à en faciliter l'usage. Pour ce faire, les mécanismes biométriques de contrôle, par selfie ou vidéo notamment, deviendront la norme.





Les pistes d'optimisation envisagées comprennent une longue liste de solutions, disponibles ou exploratoires, parmi lesquelles nous pouvons relever :

- Les techniques de vérification d'identité par interaction vidéo dynamique,
- Le concept d'« usine KYC », un espace centralisant la connaissance du client à l'échelle de l'entreprise ou de l'industrie, enrichi au fil de la relation,
- La connexion aux comptes bancaires de l'utilisateur, par exemple, pour confirmation d'identité,
- Les méthodes d'empreinte numérique, identifiant les caractéristiques de l'appareil connecté et, éventuellement, de son utilisateur, à des fins de détection de comportement suspect,
- L'analyse automatique de documents (statuts d'entreprise…) et contenus web, de manière à enrichir la connaissance du client.

« Nous utilisons également l'analyse audio couplée à l'intelligence artificielle pour détecter la fraude au téléphone. » (Jean-Baptiste Boix Floa, Responsable fraude et cybercriminalité)

Logiquement, les projets planifiés en 2021 s'orientent dans les mêmes directions, la vérification d'identité en vidéo étant particulièrement plébiscitée, dès que les derniers obstacles réglementaires seront levés.

« Nous anticipons les critères de certification de l'ANSSI. Nous allons intégrer notre propre solution et la faire certifier. » (Evan Proux, Lydia, Head of Fraud Operations)

Quelques répondants expriment leur intention de maintenir une veille active sur l'évolution de l'offre de lutte contre la fraude et, le cas échéant, d'expérimenter rapidement les nouvelles options qui apparaissent.

Des efforts spécifiques devraient en outre être consentis en matière de dispositif humain. Il est ainsi question, de manière récurrente, de renforcement des équipes, de formations approfondies, de fournir aux collaborateurs des outils plus performants pour les aider dans leur mission, d'adaptation des règles en vigueur…

« Nous souhaitons améliorer notre outil afin de prémâcher et accélérer la prise de décision de notre équipe. » (Antoine Saudray, Younited Credit, Enterprise Risk Manager & DPO)

« Notre principal effort vise d'abord à informer et partager les bonnes pratiques.» (Michael Benisti, Ledger, Head of Payment & Fraud Management)

« Sensibiliser tout le monde pour lutter efficacement contre la fraude. » (Julien Ramezani, October, Head of Client Operations)

A plus long terme, les cybercriminels et les fraudeurs étant toujours prompts à s'emparer des technologies les plus sophistiquées, l'arsenal devra se renforcer en permanence, soit par l'ajout de boucliers additionnels, soit par l'enrichissement des solutions en place.

Par exemple, les progrès de l'intelligence artificielle, qui aident à créer des identités synthétiques ou permettront bientôt de produire des « deep fakes » vidéo en temps réel, ou l'émergence de l'informatique quantique, avec ses lourdes implications prévisibles sur la cybersécurité (en particulier sa capacité à rendre obsolètes les algorithmes cryptographiques actuels), imposeront un surcroît de vigilance et de protection aux acteurs de la finance.

CONCLUSION

De l'avis général, il paraît aujourd'hui possible de réconcilier lutte contre la fraude et expérience utilisateur dans le secteur financier, sans fragiliser l'une ni dégrader la seconde. Pour ce faire, les acteurs n'hésitent pas à déployer les technologies les plus sophistiquées et les plus en pointe, de l'intelligence artificielle à la biométrie. Ils se montrent en outre relativement confiants pour l'avenir, misant sur les progrès des solutions disponibles et sur l'innovation permanente pour contrer l'évolution rapide de la cybercriminalité.

Cependant, notre étude révèle trois domaines dans lesquels une majorité des professionnels estime encore nécessaire d'explorer des pistes d'amélioration.

Il est d'abord question d'**inclusion numérique**. Quelle que soit la qualité des parcours d'entrée en relation mis en œuvre, une fraction conséquente de la population reste à l'écart des opportunités offertes, soit par défaut de l'équipement nécessaire, soit, plus fréquemment, en raison de réticences vis-à-vis des technologies. Pour ces personnes, la réponse apportée à l'heure actuelle, quand elle est possible, consiste à proposer l'aide d'un conseiller (humain). L'enjeu dépassant largement le secteur financier (il affecte notamment les services publics), peut-être une réflexion commune, à l'échelle de la société, devrait-elle être engagée autour de la littératie numérique…

Ensuite, la mise en œuvre du **cadre réglementaire** doit permettre à la France de rester compétitive par rapport au reste de l'Europe. A ce titre, il est primordial à l'avenir d'entretenir un lien fort entre innovation et régulateur et que ce dernier conserve une forte réactivité face aux prochains défis réglementaires.

Enfin, un axe de progrès, essentiel mais trop négligé, consisterait à **développer les collaborations** autour de la lutte contre la fraude, jusqu'à, peut-être, instaurer des solutions de place. La mise en commun, y compris au-delà du secteur financier (l'usurpation d'identité, par exemple, touche tous les domaines d'activité), des connaissances des pratiques des cybercriminels, des données compromises, des mécanismes d'attaque empruntés… permettrait de renforcer grandement l'efficacité des dispositifs de protection individuels.

REMERCIEMENTS

France FinTech et Onfido remercient tous les contributeurs au livre blanc :

Olivier Fliche et Timpothé Dufour du Pôle FinTech Innovation de l'ACPR; Pierre Villeroy de Galhau, Directeur Stratégie & Innovation, Boursorama; Jean-Baptiste Boix, Responsable Fraude et Cybersecurité, Floa Bank; Bertrand Godin, Head of Operations & Correspondent Banking, iBanFirst; Amine Bounjou, Co-Founder & COO, Kard; Michael Benisti, Head of Payment & Fraud Management, Ledger; Nadège Pupier, Chief Compliance and Risk Officer, Lemonway; Evan Proux, Head of Fraud Operations, Lydia; Clément Mazeries, Compliance Officer, Mangopay; Julien Ramezani, Head of Client Operations, October; Eric Mignot, Founder and Chairman, PlusSimple; Jean-Eloi Rateau, Head of Regulatory and Compliance, Qonto; Stéphane Berger, Head of Digital Product Strategy, Sopra Banking Software; et Antoine Saudray, Enterprise Risk Manager & DPO, Younited Credit»

À PROPOS

Onfido

Fondée en 2012 à Londres, Onfido fournit ses services de vérification et d'authentification d'identité en ligne à plus de 1 500 entreprises à travers le monde. Basée sur un mode hybride incluant à la fois l'intelligence artificielle et le recours à des experts humains, la technologie Onfido permet de vérifier qu'un internaute est bien celui qu'il prétend être, et ce sans altérer l'expérience client, la confidentialité des données ou la sécurité.

C'est ainsi qu'Onfido donne à des entreprises comme Nickel (groupe BNP Paribas), Europcar Mobility Group et Getaround (ex Drivy) l'assurance dont elles ont besoin pour intégrer les clients à distance et en toute sécurité. Onfido est soutenu par TPG Growth, Salesforce Ventures, M12 (Microsoft), Idinvest Partners et d'autres investisseurs auprès desquels l'entreprise a levé plus de 200 millions de dollars.

Pour plus d'informations : www.onfido.com/fr

France FinTech

Créée en 2015 à l'initiative des entrepreneurs, France FinTech fédère les sociétés utilisant des modèles opérationnels, technologiques ou économiques, innovants et disruptifs, visant à traiter des problématiques existantes ou émergentes de l'industrie des services financiers et représentant les principales composantes de la filière. L'association s'est donnée pour mission de promouvoir l'excellence du secteur en France et à l'étranger et de représenter les fintech françaises auprès des pouvoirs publics, du régulateur et de l'écosystème. France FinTech est aujourd'hui la plus grande association sectorielle de start-up en France et en Europe. Outre ses actions sur les terrains réglementaires et législatifs, ses nombreuses publications, ses ateliers et rencontres diverses, l'association organise chaque année l'événement de référence de l'écosystème, Fintech R:Evolution.

France FinTech est membre fondateur de l'EDFA (European Digital Finance Association).

Pour plus d'informations : francefintech.org