Fraude à l’identité : Rapport 2022

Le guide pour lutter contre la fraude

onfido

Sommaire

INTERPOL

> Nous devons de plus en plus nous adapter à l'utilisation numérique des documents d'identité, en plus des menaces qui pèsent sur les documents physiques.

Avant-propos

Par Interpol

Les documents frauduleux ouvrent la voie au crime organisé, dont le blanchiment d'argent et le financement du terrorisme. Par conséquent, le fait de ne pas les identifier dans des scénarios réels et en ligne constitue une menace pour l'économie mondiale, les pays et leurs citoyens.

Les objectifs d'Interpol en matière de documents d'identité et de fraude se concentrent sur l'examen et l'analyse des documents physiques, ainsi que sur le partage des connaissances et des compétences nécessaires auprès des agents publics pour leur permettre d'identifier les pièces d'identité frauduleuses.

Mais de plus en plus, nous devons nous adapter à l'utilisation numérique des documents d'identité, au-delà de leur seule utilisation physique. Et dans ce nouvel environnement, les entreprises et les gouvernements sont confrontés à des défis pour détecter la fraude.

Onfido, avec sa solution de vérification d'identité numérique, se trouve dans une position unique pour identifier et analyser ces menaces de fraude. Dans cette publication, l'équipe d'experts d'Onfido fournit un guide de référence utile sur les tendances émergentes en matière de fraude d'identité, ainsi que certaines des mesures que les professionnels peuvent prendre pour les prévenir.

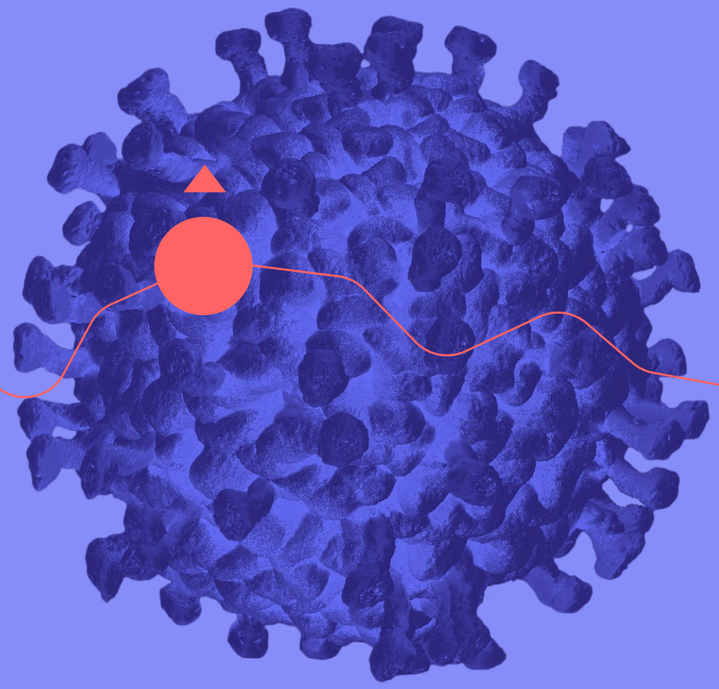
À propos de ce rapport

Onfido vérifie des millions d'identités chaque année pour ses clients. Pour ce faire, nous combinons la vérification de documents et la vérification biométrique. Cela nous donne un aperçu unique des tendances qui se dessinent en matière de fraude documentaire et biométrique.

Dans ce rapport sur la fraude d'identité, nous examinons nos données* de l'année précédente et analysons les tendances et les techniques frauduleuses qui ont émergées.

*Les données de ce rapport ont été collectées du 1er octobre 2020 au 1er octobre 2021 auprès des clients d'Onfido. Les données et les tendances reflètent l'état du secteur de la vérification et peuvent ne pas toujours refléter les tendances plus larges du marché. Onfido détient le droit de publier ces données.

Principaux enseignements de l'année écoulée



2020 a été une année tumultueuse pour les entreprises et les fraudeurs n'ont pas eu peur d'en profiter. Le COVID-19 est directement responsable de l'augmentation de la fraude à l'identité, car de nombreuses entreprises ont été contraintes de déplacer rapidement leurs opérations en ligne.

Dit simplement, plus d'activité en ligne signifiait plus d'opportunités pour les fraudeurs, et nos données le reflètent. Une nouvelle vague de fraudeurs « non professionnels » et opportunistes est entrée sur le marché, et nous avons vu les taux moyens de fraude d'identité passer de 4,1 % en octobre 2019 à 5,8 % en octobre 2020.

La pandémie a également encouragé les comportements frauduleux. Les fraudes sophistiquées sont devenues plus difficiles à détecter et les fraudeurs sont actifs sept jours sur sept.

Alors que la pandémie s'atténue, lesquelles de ces tendances de la fraude sont là pour rester, et de nouvelles sont-elles apparues ?

Les Tendances

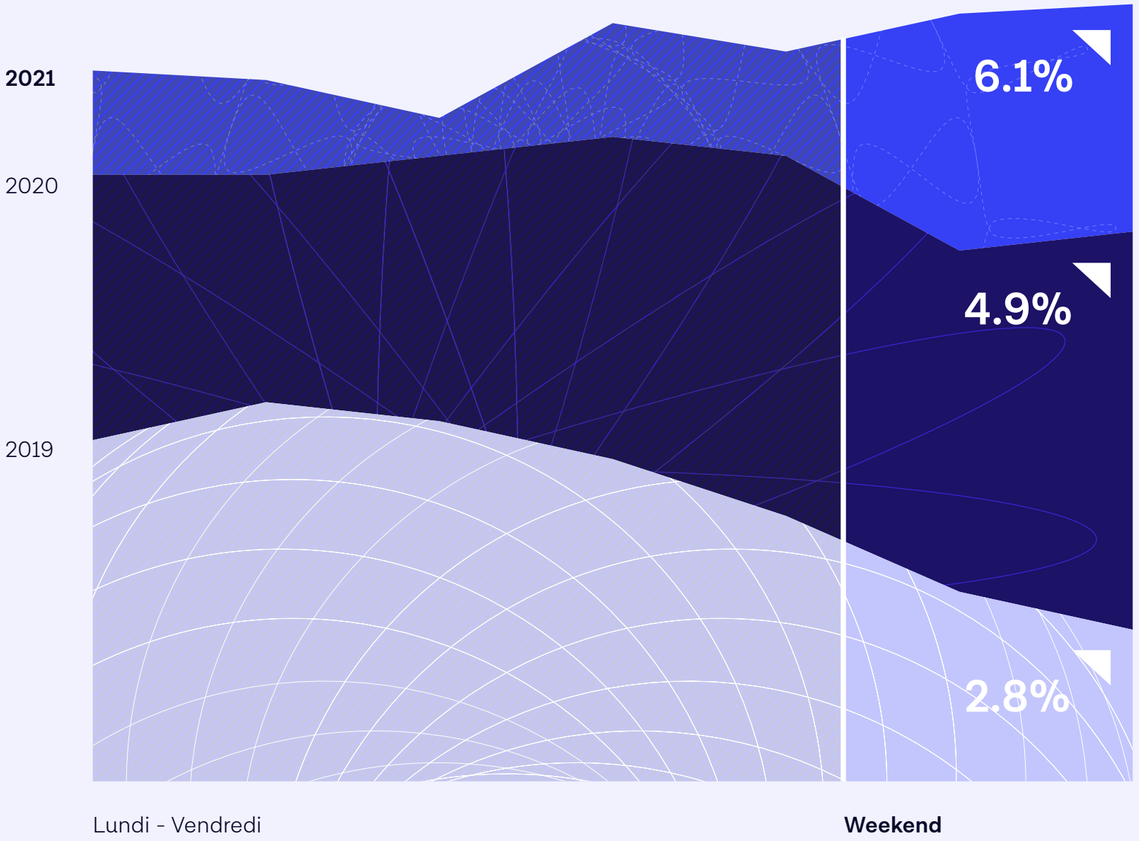
Le paysage de la fraude

La fraude à l'identité n'est pas encore revenue au niveau d'avant la pandémie

Il y a eu une augmentation de 44% des fraudes depuis 2019. Entre octobre 2020 et octobre 2021, le taux moyen de fraude à l'identité était de 5,9%, contre un taux moyen de 4,1% en 2019.

Malgré le fait qu'une grande partie du monde physique ait rouvert, la fraude n'est toujours pas revenue aux niveaux d'avant la pandémie. Le bond de la fraude qui était un résultat direct du COVID-19 semble être là pour rester. Comme les consommateurs sont devenus beaucoup plus à l'aise pour effectuer des transactions en ligne, les fraudeurs resteront en ligne avec eux.

Les horaires de travail des fraudeurs

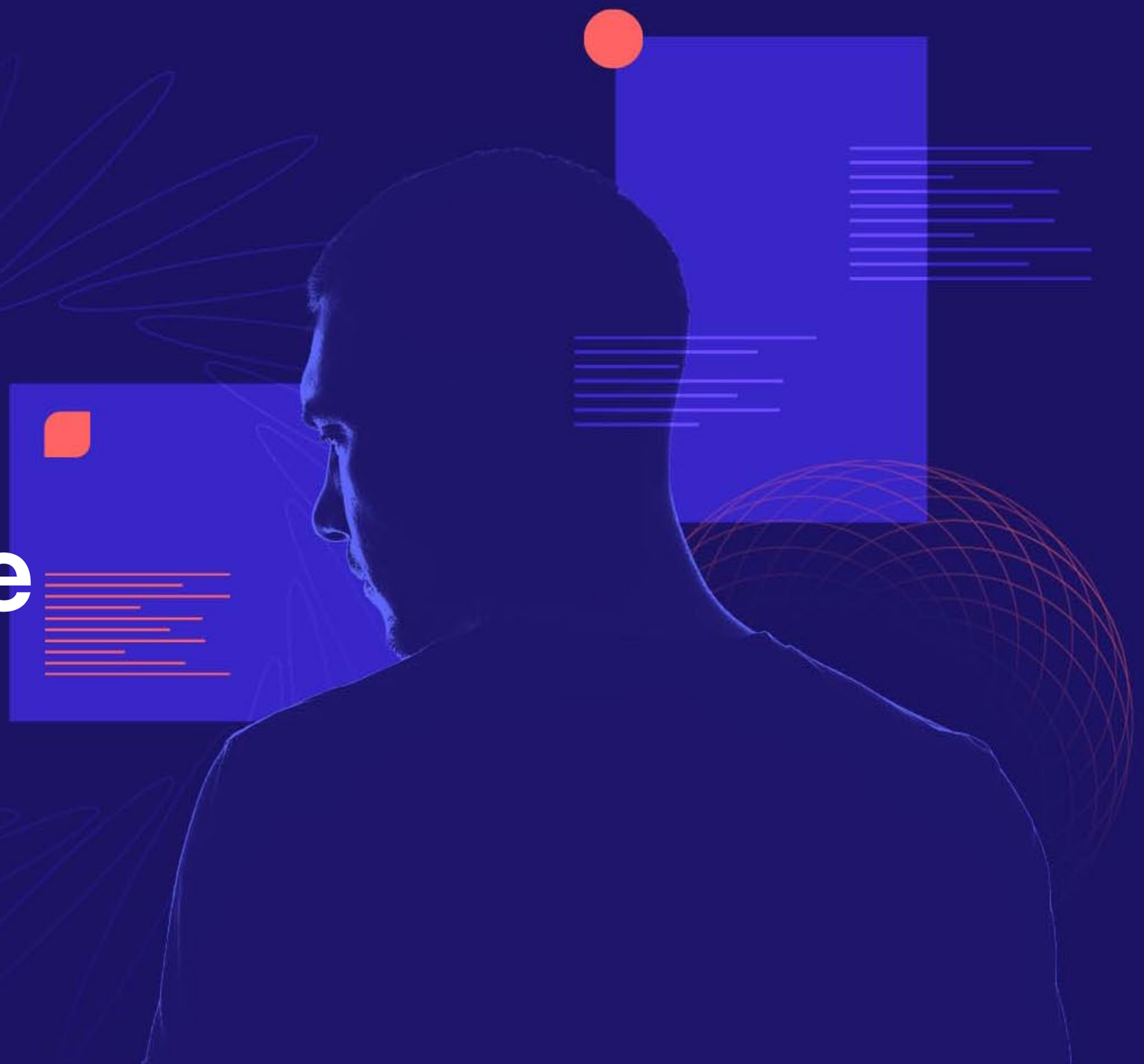


Les fraudeurs ont abandonné la journée de travail habituelle au profit des weekends.

La pandémie a également eu un impact à long terme sur le comportement des fraudeurs. Avant la pandémie, l'activité des fraudeurs suivait la semaine de travail habituelle (ils étaient plus actifs du lundi au vendredi). Mais maintenant, non seulement les activités frauduleuses augmentent tous les jours de la semaine, mais elles culminent le week-end.

En tant qu'entreprise, c'est quelque chose à surveiller. Il se pourrait que davantage d'amateurs se soient installés dans l'espace en tant que fraudeurs à temps partiel. Mais cela suggère également que les fraudeurs essaient de profiter des temps d'arrêt de votre entreprise, lorsqu'il y a moins d'employés disponibles pour signaler les problèmes ou détecter une activité suspecte.

Tendances de la fraude documentaire



Les types de fraude documentaire

Échec de la validation des données : le document ne contient pas de données valides à tous les endroits appropriés.

Échec de la cohérence des données : les données ne sont pas cohérentes dans toutes les zones du document.

Échec de l'authenticité visuelle : un document présente des critères de sécurité visuels compromis.

La plupart des documents frauduleux manquent de données valides

Globalement, la majorité des documents frauduleux (55%) échouent à un contrôle en raison d'erreurs relatives à la validation des données. Cela signifie que le document ne contient pas de données valides à tous les emplacements corrects ou contient des données incompatibles avec le type de document. Par exemple, une date de publication qui correspond à un autre format, telle qu'une version 2010 d'un document où la date de publication sur le document est 2021.

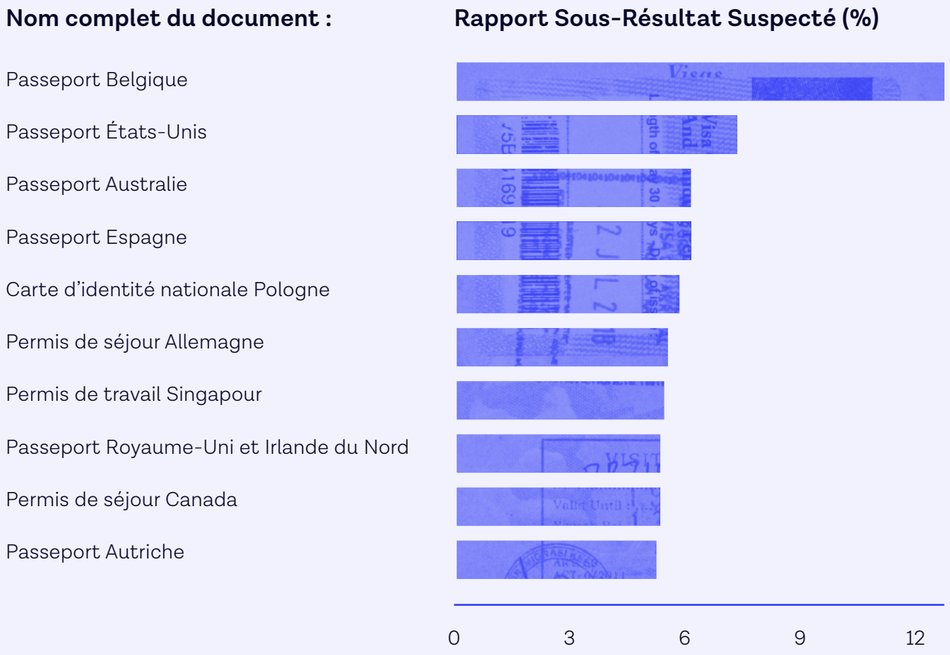
Cela indique un type de fraude moins sophistiqué, suggérant qu'une grande partie des fraudeurs ont une connaissance limitée des documents d'identité.

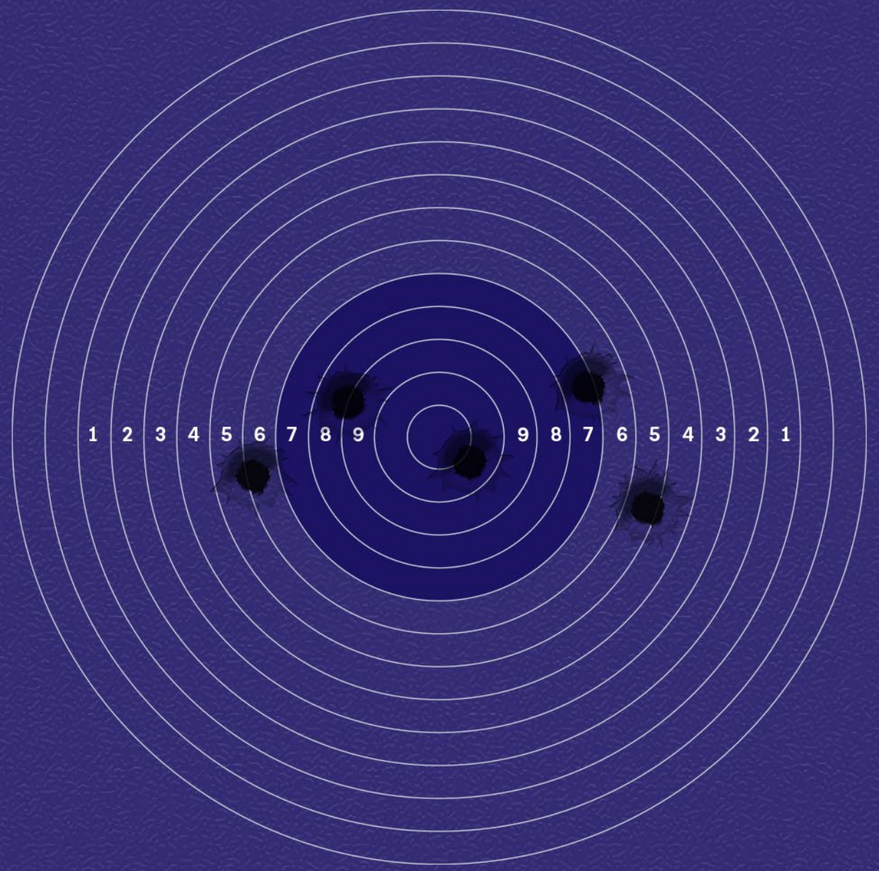
Les passeports sont les pièces d’identité les plus attaquées.

L’année dernière, les cartes d’identité nationales étaient le type de document le plus fréquemment attaqué. La moitié de nos dix documents les plus frauduleux étaient des cartes d’identité nationales. Nous considérerions les cartes d’identité nationales comme des documents d’identité « plus vulnérables » (elles n’ont jamais été conçues pour les voyages internationaux et ont donc moins de critères de sécurité). Cela les rend plus vulnérables à la fraude, de sorte que les fraudeurs les ciblaient traditionnellement davantage que d’autres types de documents.

Mais cette année, les passeports dominent notre liste des documents les plus fréquemment attaqués. Cela indique un changement dans le comportement des fraudeurs.

Les types de documents les plus frauduleux

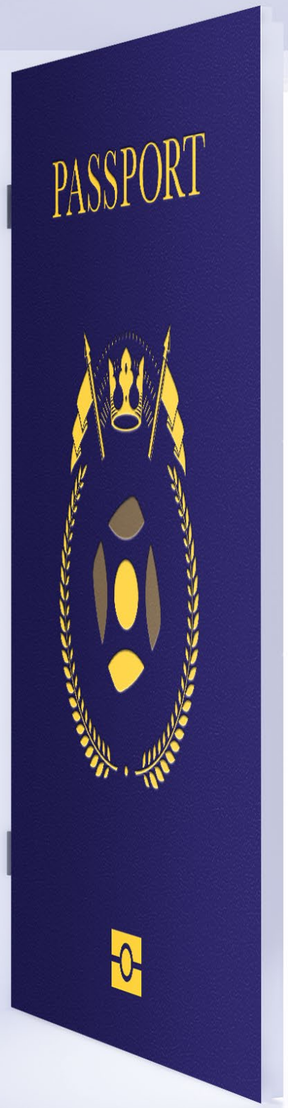




Les fraudeurs sont paresseux et choisissent de cibler les documents recto.

Un passeport est un document recto. En d'autres termes, il ne contient que des informations personnelles sur une seule page. En comparaison, une carte d'identité comporte des informations personnelles au recto et au verso du document. Lorsque nous effectuons un contrôle de vérification des documents, nous demandons à l'utilisateur de soumettre deux photos d'une carte d'identité nationale (une recto et une verso), mais une seule pour les passeports.

Ainsi, fabriquer un faux passeport demande moins d'efforts pour le fraudeur, car il n'a à modifier ou recréer qu'une partie d'un document. Il s'avère que les fraudeurs sont toujours à la recherche d'attaques qui nécessitent un minimum d'efforts.



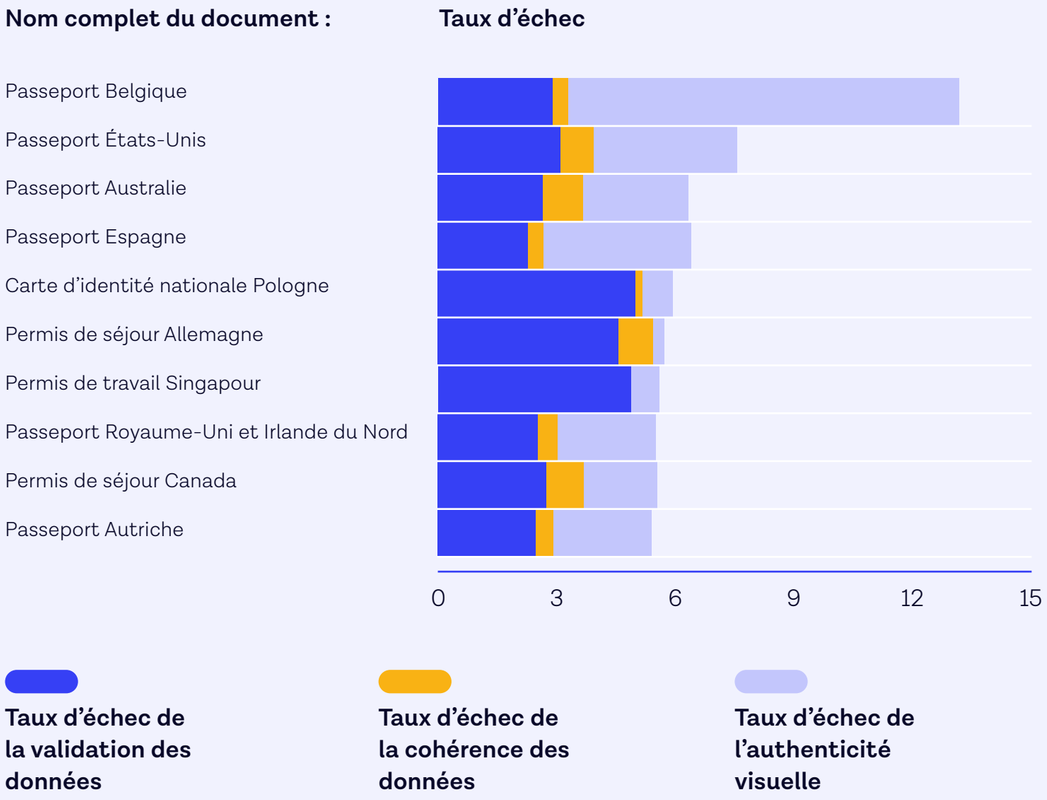
Les fraudeurs croient que la réputation d’un passeport est supérieure aux autres documents d’identité.

Beaucoup considèrent les passeports comme des preuves au niveau de garantie élevé en raison des procédures de délivrance. Vous avez souvent besoin d’une pièce d’identité nationale pour demander un passeport. Donc, si vous les mettez sur une échelle relative, les passeports sont considérés comme « supérieurs » et plus difficiles à frauder.

Cela nous donne un aperçu unique de la psychologie des fraudeurs. Ils choisissent de soumettre de faux passeports plutôt que d’autres documents d’identité, en espérant que la réputation d’un passeport aidera le faux à passer inaperçu.

Les fraudeurs utilisent une fraude moins sophistiquée pour cibler des documents plus vulnérables.

Type d’attaque le plus fréquent concernant les documents frauduleux



Il ne s’agit pas seulement du type de document, le pays d’origine joue également un rôle. Les documents d’identité délivrés dans un pays peuvent avoir plus de critères de sécurité ou des règles plus robustes en matière de données.

Ainsi, nous pouvons également appliquer les différents types de fraudes à notre liste de documents les plus fréquemment attaqués analysés par Onfido. Lorsque nous appliquons cette approche, cela nous donne une idée des méthodes les plus susceptibles d’être utilisées par les fraudeurs pour les attaquer.

Dans l’ensemble, les documents qui échouent davantage pour la validation et la cohérence des données ont des règles de données plus robustes. Par exemple, la répétition des données à caractère personnel dans le document.

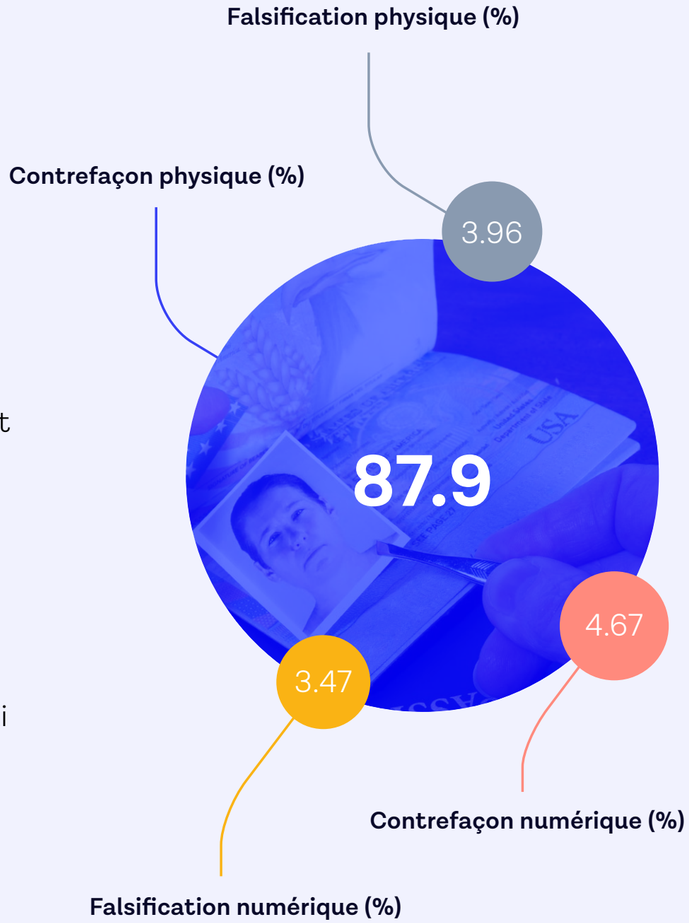
D’un autre côté, les documents qui échouent davantage pour l’authenticité visuelle ont tendance à avoir moins de protections des données. Cela laisse les signaux visuels comme principale méthode de détection de la fraude.

Les fraudeurs préfèrent « partir de zéro »

Plus de 90 % des fraudes d'identité que nous constatons impliquent des documents contrefaits. Une contrefaçon est une reproduction intégrale d'un document, par opposition à une falsification qui consiste à altérer un document original.

Le nombre élevé de contrefaçons pourrait être dû au grand nombre de fichiers modèles disponibles en ligne. Un fichier modèle est peu coûteux et les fraudeurs peuvent les modifier avec peu d'effort. De plus, de nombreux documents d'identité modernes contiennent de nombreux critères de sécurité. Cela rend toutes les modifications, comme ce que vous verriez sur un faux, facilement détectables même à l'œil non averti.

La plupart de ces documents contrefaits sont des reproductions physiques, ce qui signifie qu'un fraudeur utilise un document réel. Nous voyons beaucoup moins de fraudes numériques (lorsqu'un fraudeur manipule l'image d'un document), car notre produit est conçu pour l'empêcher. Beaucoup de nos clients utilisent nos kits de développement logiciel (SDK) natifs qui obligent les utilisateurs finaux à capturer une photo de leur document en direct. Cela empêche les fraudeurs de créer ou de modifier des images de documents à l'avance, puis de les télécharger.



Documents contrefaits
Une contrefaçon est une reproduction complète d'un document original.

Documents falsifiés
Les falsifications sont des altérations de documents originaux. Par exemple, un fraudeur peut changer un chiffre sur un document, ce qui peut créer une identité totalement nouvelle et fausse.

Fraude numérique
Les fraudeurs utilisent un logiciel pour manipuler l'image d'un document.

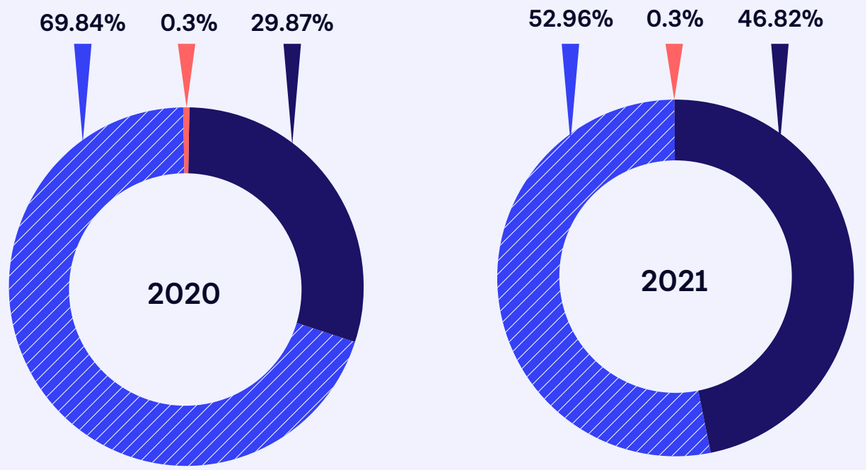
Fraude physique
Les fraudeurs modifient le document réel que l'on voit sur l'image, ou partent de zéro.

Le crime organisé est lié à plus de fraudes moyennes

Par rapport à l'année dernière, nous constatons beaucoup plus de fraudes « moyennes ». Cette année, 46,82 % de toutes les fraudes documentaires que nous avons constatées ont été classées comme « moyennes ». Par rapport au chiffre de l'année dernière, cela représente une augmentation de 57 %.

L'une des raisons à cela est que cette année, nous avons assisté à une augmentation des activités frauduleuses organisées. Ces groupes organisés tenteront de créer des comptes « vérifiés » avec de faux documents, avant de les revendre.

niveau de complexité de la fraude



Facile

Lorsque les éléments du document sont clairement erronés, par exemple, les documents ont la mauvaise police de caractères ou une photo visiblement attaquée.

Moyenne

Erreurs moins évidentes, telles que des polices incorrectes moins visibles, une mauvaise photo technique d'impression, ou des éléments de sécurité imités.

Difficile

Cas nécessitant une connaissance approfondie de la fabrication des documents (par exemple, les éléments de sécurité, l'impression et les erreurs délibérées) pour détecter les anomalies.

Tendances de la fraude biométrique

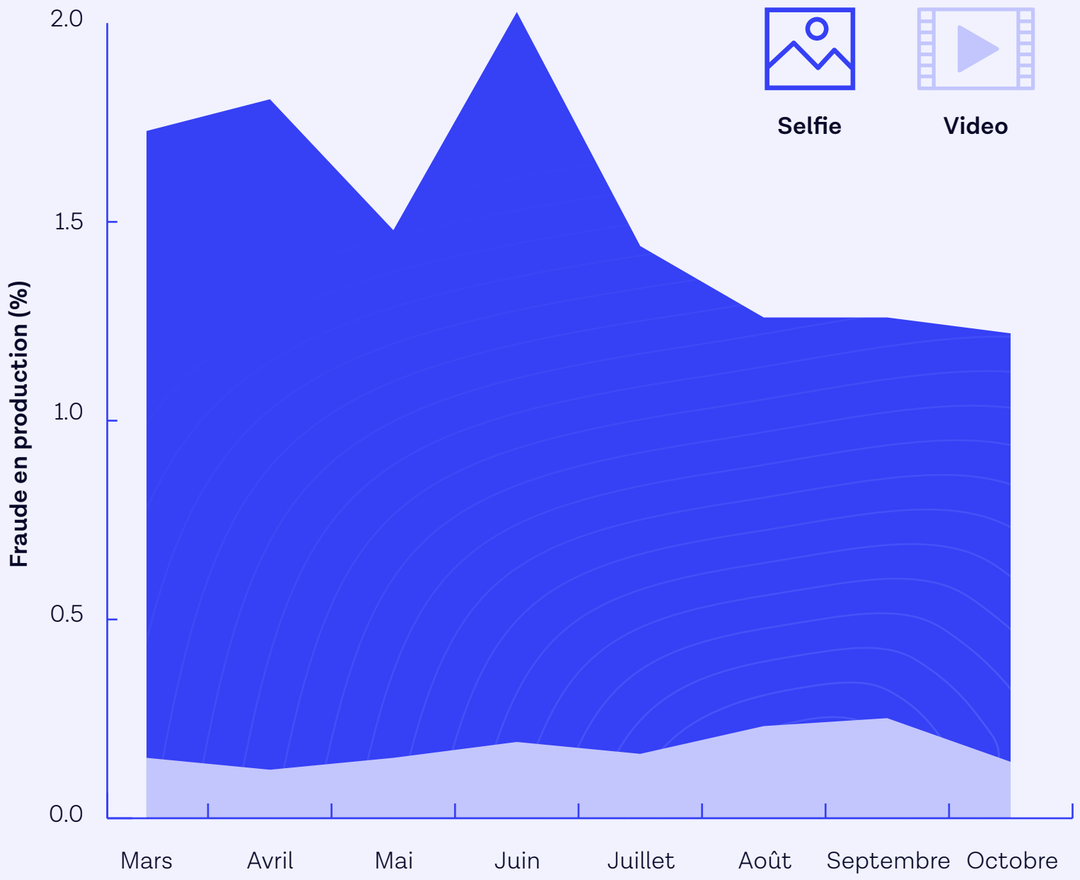
La biométrie est un grand moyen de dissuasion contre la fraude

Dans l'ensemble, nous voyons beaucoup moins de fraudeurs tenter d'attaquer un contrôle biométrique (à la fois selfie et vidéo) par rapport à un contrôle de document. Le taux moyen de fraude documentaire pour 2021 était de 5,9 %, contre 1,53 % pour les selfies et 0,17 % pour les vidéos.

Ceci est directement lié à notre produit. La vérification biométrique offre plus de protection contre la fraude que la vérification de document seule (et une vérification vidéo offre plus de protection qu'une vérification par selfie). L'expérience utilisateur vidéo en elle-même agit comme un moyen de dissuasion naturel contre la fraude, car il s'agit d'une expérience active hautement aléatoire. Cela rend presque impossible de frauder le système.

Étant donné qu'au cours des six derniers mois, les usurpations vidéo ont représenté une fraction (0,17%) de tous nos contrôles vidéo, cela en fait une excellente mesure de sécurité pour les entreprises soucieuses de faire de la prévention de la fraude une priorité.

Le taux de fraude biométrique



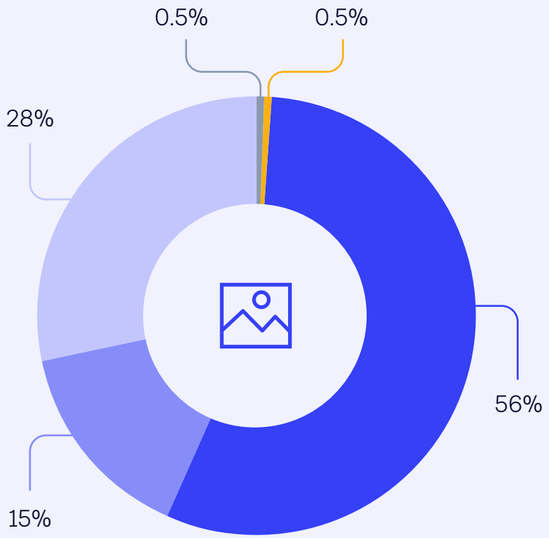
Les photos d’écrans sont l’attaque biométrique la plus courante.

Les méthodes d’attaque les plus fréquentes que nous voyons à travers la biométrie sont les moins sophistiquées. Une photo d’un écran (où les fraudeurs capturent une photo d’une image sur un écran, au lieu d’utiliser leur propre visage) représentait 56% de toutes les usurpations selfie et 48% de toutes les usurpations vidéo.

Pour mettre cela en perspective, si un fraudeur utilise une pièce d’identité volée, il peut effectuer une recherche en ligne pour trouver un réseau social ou une image de cette personne en ligne et prendre une photo ou une vidéo de celle-ci avant d’essayer de la faire passer pour la version réelle.

Une autre façon dont les fraudeurs tentent couramment de contourner la vérification biométrique consiste à utiliser un document d’identité usurpé. Ils prennent une photo de l’image sur le document d’identité pour correspondre à ce qui a été capturé lors du contrôle des documents.

Les types de fraude biométrique



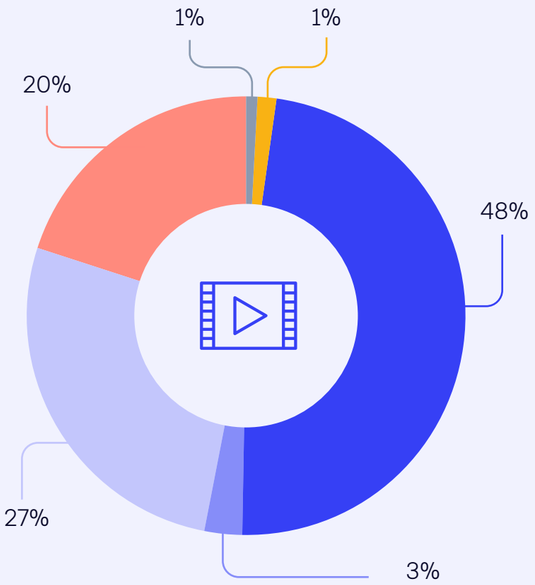


Photo sur écran
Une photo ou une vidéo d’une image sur l’écran.

Photo imprimée sur papier
Une photo ou une vidéo d’une image imprimée sur papier.

Faux document d’identité
Une photo ou une vidéo de l’image figurant sur le document d’identité.

Masque 2D
Photo ou vidéo d’un masque imprimé imprimé.

Masque 3D
Photo ou vidéo d’un masque 3D ou d’autres objets 3D.

Vidéo à l’écran
(Contrôle vidéo uniquement) : Une vidéo d’une vidéo à l’écran.

La plupart des fraudes biométriques sont peu sophistiquées pour l'instant

Le fait que les fraudeurs optent toujours pour des méthodes d'attaque relativement peu sophistiquées à travers la biométrie suggère deux choses. Les méthodes d'attaque sophistiquées sont toujours hors de portée pour la plupart des fraudeurs. Ou bien, les fraudeurs ne veulent tout simplement pas faire l'effort de contourner la vérification biométrique.

Comment Onfido arrête les photos sur les écrans et les falsifications

Nos algorithmes analysent les selfies et les vidéos à la recherche d'une texture anormale. Cela permet de capturer des photos de photos ou des photos d'écrans, qu'un fraudeur peut essayer de faire passer pour de vraies choses.

Démasquer les fraudeurs

Par rapport à des méthodes d'attaques biométriques relativement peu sophistiquées comme une photo à l'écran, nous voyons beaucoup moins de masques 2D et 3D. Cela souligne la tendance plus large selon laquelle la biométrie agit comme un bon moyen de dissuasion. Les masques 3D sont chers et les fraudeurs solitaires ou amateurs ne voudront pas investir de l'argent ou des efforts pour tenter de duper le système de cette façon.

Mais il est important qu'en tant qu'entreprise, vous soyez protégée contre ces types d'attaques. Les réseaux de fraude et le crime organisé sont plus susceptibles d'employer des méthodes sophistiquées comme celle-ci, et nous nous attendons à voir davantage d'attaques de ce type à l'avenir.

Comment Onfido arrête les masques 2D et 3D

Onfido Selfie analyse la texture de l'image pour détecter les signes de fraude. Et Onfido Video combine des techniques avancées de défense contre la fraude, notamment le suivi de mouvement, la synchronisation des lèvres et l'analyse de texture pour vérifier que l'utilisateur est physiquement présent. Nous proposons également plus de 4 000 combinaisons d'actions aléatoires, afin que les fraudeurs ne puissent pas tromper le système avec des vidéos préenregistrées.

Documents et visages frauduleux sur un pied d'égalité

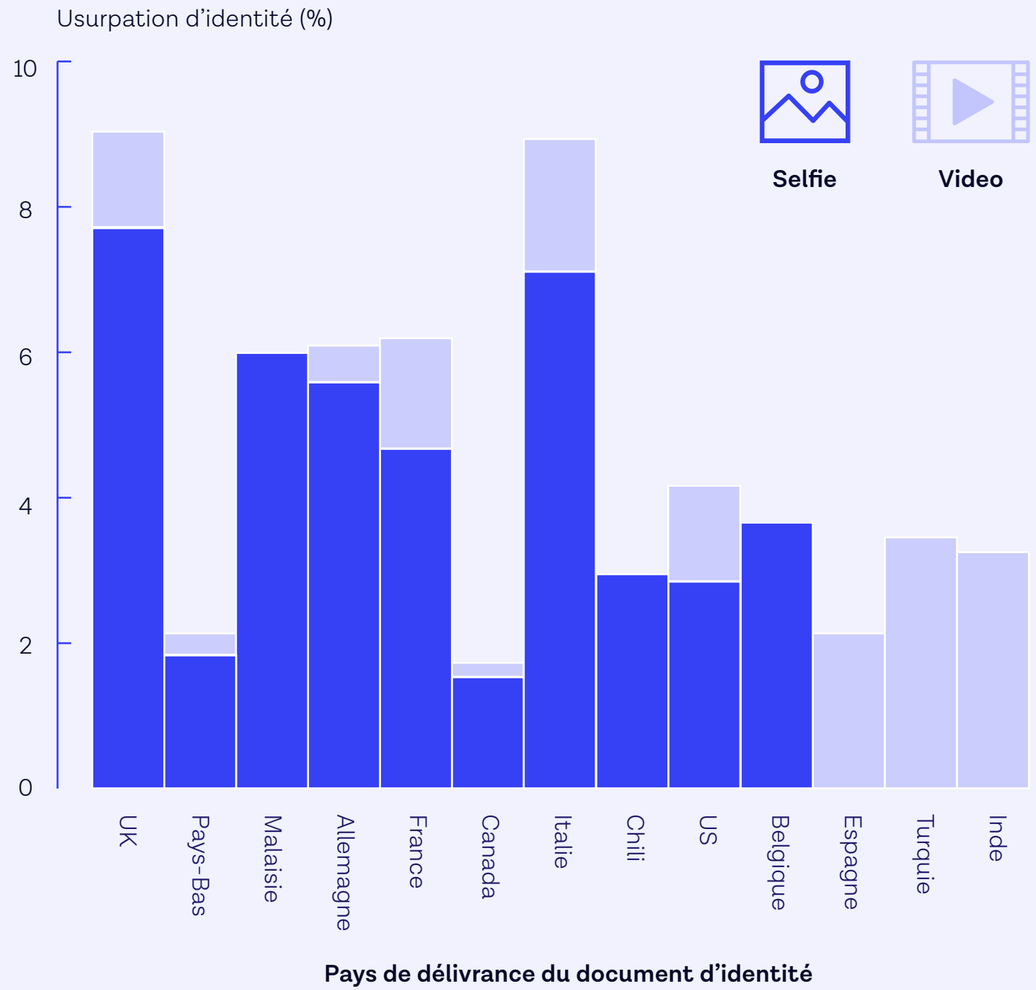
Étant donné que la plupart de nos clients combinent la vérification des documents et la vérification biométrique, prenons le temps d'analyser la fraude constatée entre les documents et la biométrie, pour voir s'il existe des tendances.

Ces graphiques montrent le niveau de fraude biométrique que nous constatons en fonction du pays émetteur du document. Par rapport à notre liste des documents les plus fréquemment attaqués, nous observons une corrélation intéressante.

Pour les documents les plus fraudés de notre liste, il apparaît plus probable qu'ils soient associés à des taux de fraude biométrique plus élevés que ceux du pays émetteur du document concerné. Cela suggère que lorsque les fraudeurs falsifient un document spécifique, ils poursuivent et tentent également de frauder le contrôle biométrique.

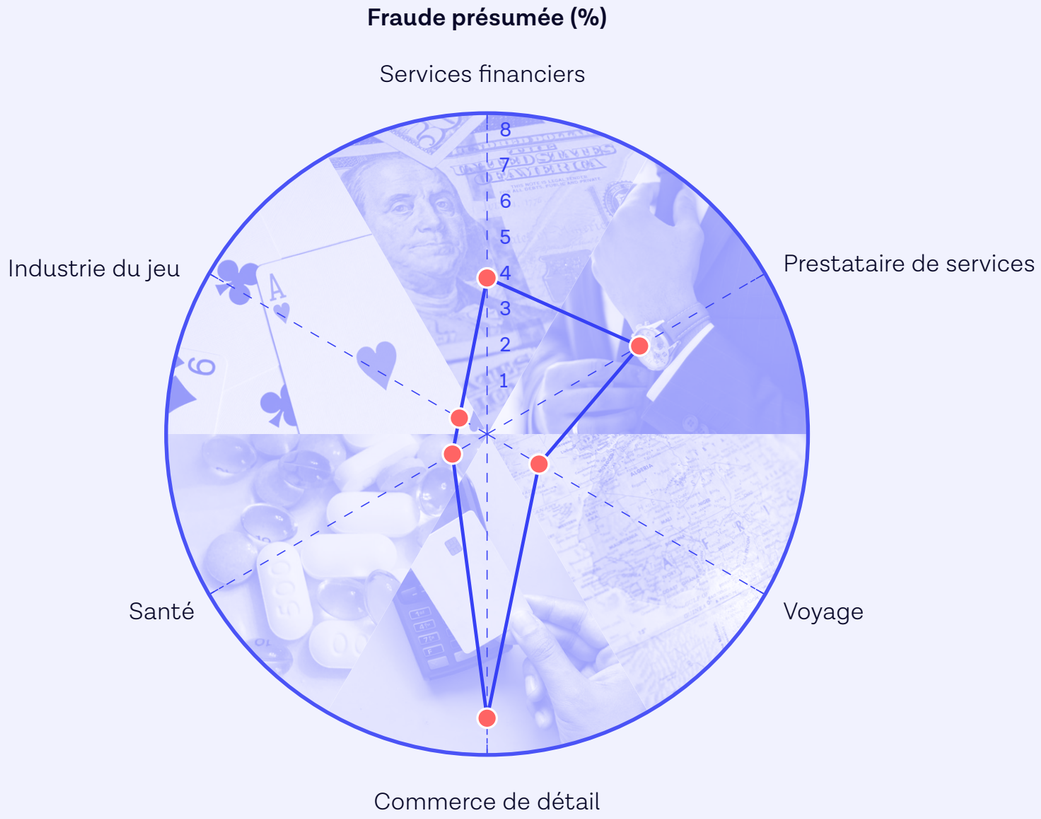
Le pourcentage élevé de fraude biométrique au Royaume-Uni pourrait également refléter le nombre de services numériques disponibles dans cette zone géographique. Puisque cela offre un terrain de jeu plus vaste aux fraudeurs.

Fraude biométrique par rapport au pays émetteur du document



Tendances de la fraude par secteur d’activité

Taux de fraude par secteur d’activité



Les fraudeurs se sont tournés vers le secteur du commerce de détail

Cette année, les services financiers et les prestataires de services sont les deux secteurs les plus touchés, comme l’année dernière. Les fraudeurs ont tendance “à suivre l’argent”, il n’est donc pas surprenant qu’ils ciblent ces deux secteurs.

Mais cette année, nous avons également assisté à une forte augmentation de la fraude dans le secteur de la vente en ligne. En raison des perturbations causées par la pandémie, les fraudeurs ont tourné leur attention vers les opportunités offertes par de nouveaux secteurs.

Les services financiers et professionnels connaissent bien la fraude et ont eu amplement le temps de s’adapter et de mettre en place des protections. En comparaison, les services de vente au détail sont généralement moins exposés aux attaques de fraude en ligne. En conséquence, ils ont peut-être eu du mal à ajuster leurs procédures. Par exemple, les employés travaillant à distance, et les centres d’appels se déplaçant du bureau au salon, les procédures devaient s’adapter et changer rapidement. Tout cela a créé des faiblesses exploitées par les fraudeurs.

Étude approfondie sur la crypto

En tant que secteur, la crypto est très volatile et a suscité un grand intérêt du public. Cela en soi la rend attrayante pour les fraudeurs. Les escroqueries liées à la cryptographie ont augmenté. 7 000 personnes ont signalé des pertes de plus de 80 millions de dollars entre octobre 2020 et mars 2021 [référence]*.

Le paysage réglementaire

Les exigences réglementaires (ou, historiquement, leur absence) ont également contribué à l'intérêt des fraudeurs pour le secteur. Selon une étude de 2020, près de 56% de toutes les plateformes d'échange de crypto-monnaies ne suivaient aucune réglementation KYC, ce qui en fait une cible de choix pour la fraude [référence].

Mais cela est en train de changer. Aux États-Unis, les plateformes d'échange de crypto-monnaie régulées par la FinCEN doivent appliquer la procédure KYC et adopter des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT). En Europe, les choses sont un peu plus compliquées. Si une plateforme d'échange de crypto ne traite que des échanges crypto-crypto, alors la législation ne couvre pas entièrement les transactions. Cependant, les contrôles KYC et AML sont désormais requis si un échange propose des transactions fiat-crypto ou crypto-fiat.

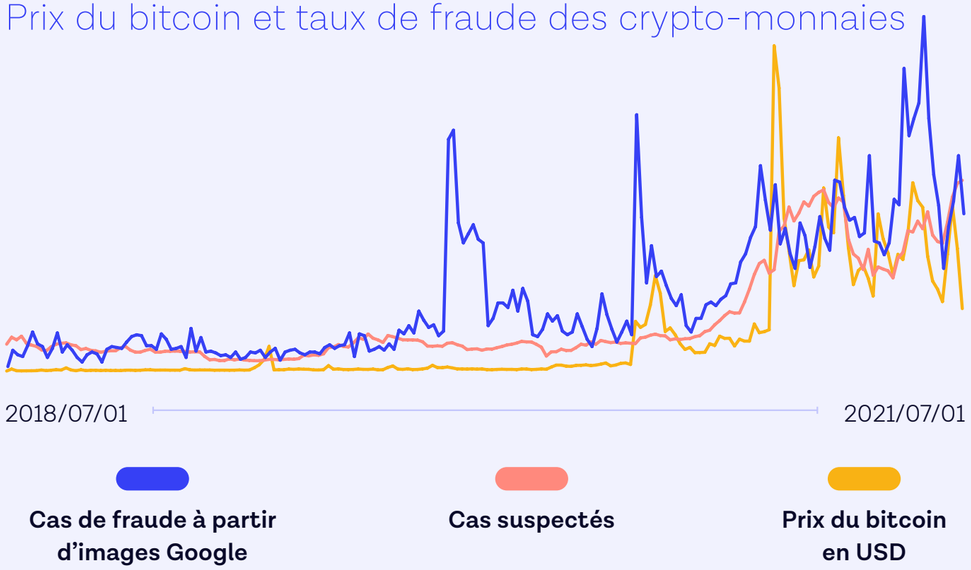
Reference*

Reference**

Le prix des crypto-monnaies augmente, la fraude fait de même

Chez Onfido, nous avons constaté qu'à mesure que le prix des crypto-monnaies augmente, le nombre de cas suspects de fraude augmente également chez nos clients crypto. Des pics supplémentaires de fraude peuvent également être liés aux activités spécifiques de nos clients. Par exemple, s'ils mènent des campagnes offrant une sorte de bonus.

Prix du bitcoin et taux de fraude des crypto-monnaies



«Just Google it»

Cas de fraude à partir d'images Google

Onfido a également remarqué qu'à mesure que le prix du Bitcoin augmente, les tentatives d'inscription frauduleuses utilisant des documents provenant d'une recherche d'images augmentent également. Vous pouvez voir cette tendance via la ligne orange sur le graphique. Les fraudeurs se contentent de rechercher sur Google « passeport » ou « permis de conduire » (les résultats fournissent un grand nombre de photos de documents d'identité, dont certains sont faux et certains sont réels).

Pour détecter ce genre de tentatives, les fournisseurs de crypto-monnaies peuvent mettre en place diverses mesures de contrôle. Par exemple, travailler avec une solution comme celle d'Onfido, qui effectue une analyse de texture sur des photos de documents d'identité, pour confirmer qu'il s'agit bien d'une photo d'un document réel et authentique.

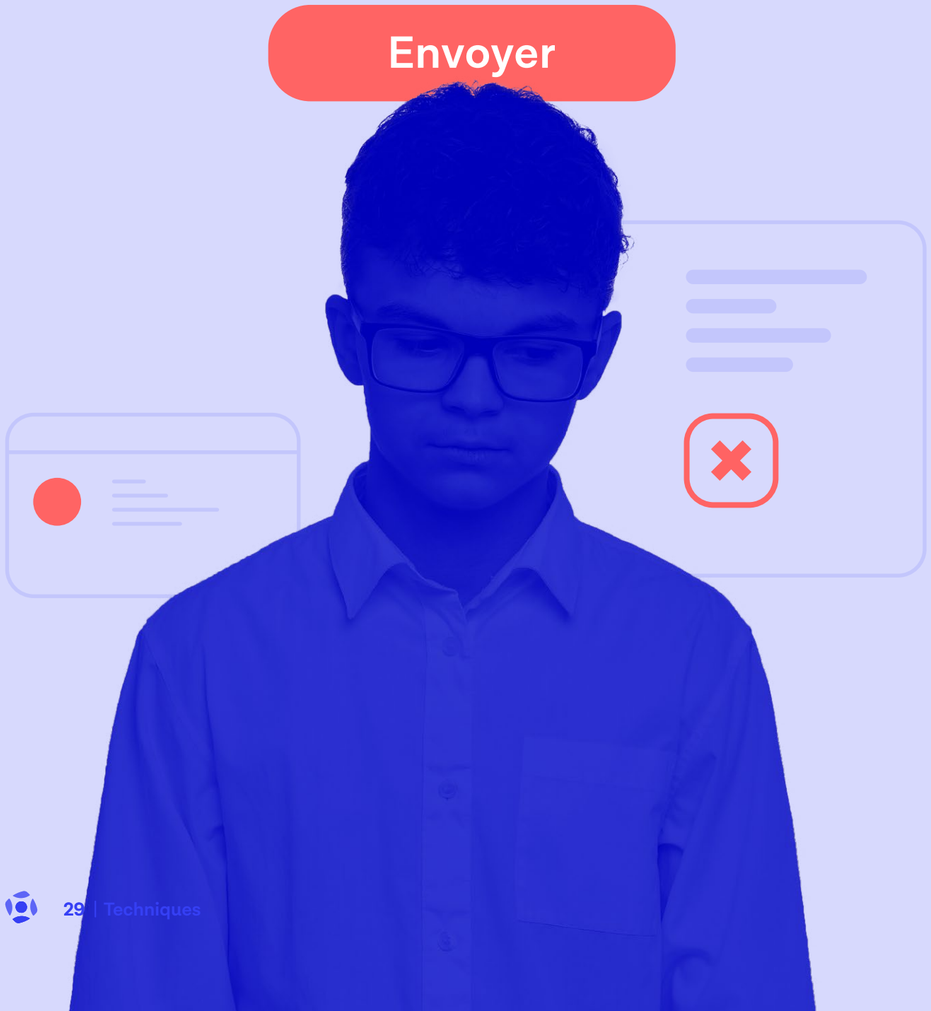
Onfido fournit également des alertes indiquant que les images peuvent être compromises s'ils voient un document d'identité fourni à un client présent sur Internet. Et enfin, bien que cela ne soit pas rendu obligatoire par la réglementation, les fournisseurs de cryptographie peuvent tirer parti de la vérification biométrique parallèlement à une vérification des documents pour contribuer à dissuader les fraudeurs.

Techniques

Profils des fraudeurs

Toutes les fraudes ne sont pas égales. S’ils réussissent, certains fraudeurs auront un impact plus important sur votre entreprise que d’autres. Cela dépend en grande partie de l’auteur de l’attaque, de ses motivations et des ressources dont il dispose.

Onfido a établi un profil des types d’attaques et des fraudeurs que nos clients rencontrent le plus, pour vous aider à savoir ce qu’il faut rechercher.



Le novice

Profil : Un individu ou un petit groupe d'individus qui tentent des attaques ponctuelles. Ils auront une expérience minimale dans les tentatives de fraude et peu de ressources à portée de main. Il peut s'agir simplement de quelqu'un qui tente sa chance (par exemple, une personne mineure qui essaie d'acheter des produits soumis à une limite d'âge) ou qui peut être confrontée à des pressions externes telles que des difficultés financières.

Volume et fréquence : Bien que des individus ou des groupes peuvent n'effectuer qu'une attaque à la fois, les entreprises seront confrontées à un grand nombre de ces types d'attaques.

Sophistication : Facile
Impact, en cas de succès : Faible

Ce qu'il faut rechercher : Signes évidents de fraude, par exemple, des informations sur une pièce d'identité qui ne correspondent pas aux informations d'inscription. Ou des documents d'identité qui échouent à la validation des données.

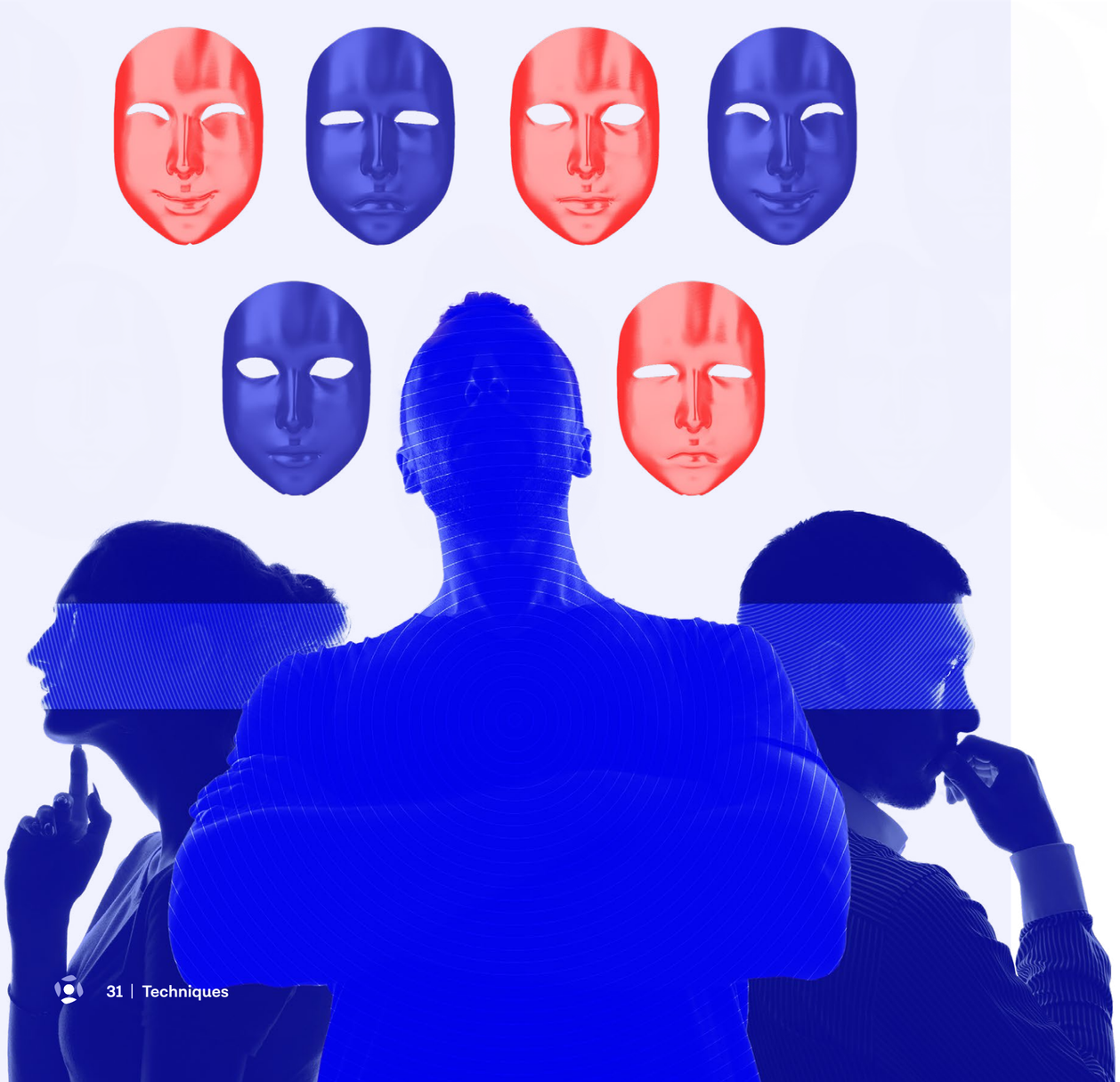
L’opportuniste

Profil : Un individu ou un groupe qui profite spontanément d’une opportunité. Par exemple, abuser des bonus ou profiter des fluctuations cryptographiques.

Volume et fréquence : Volume élevé lié à un événement spécifique, comme lorsqu’une entreprise propose des bonus d’inscription ou des campagnes de nouveaux membres.

Sophistication : Facile à moyen
Impact, en cas de succès : Moyen à élevé

Ce qu’il faut rechercher : Un afflux d’ouvertures de comptes lors de campagnes spécifiques, ou lorsqu’il y a un pic sur un certain marché, par exemple, les fluctuations des prix de la crypto. Un indicateur de fraude peut être un grand nombre de documents du même type, le même pays d’émission ou des informations répétées (telles que l’adresse e-mail ou le nom) lors de différentes inscriptions.



Le réseau de fraude organisé

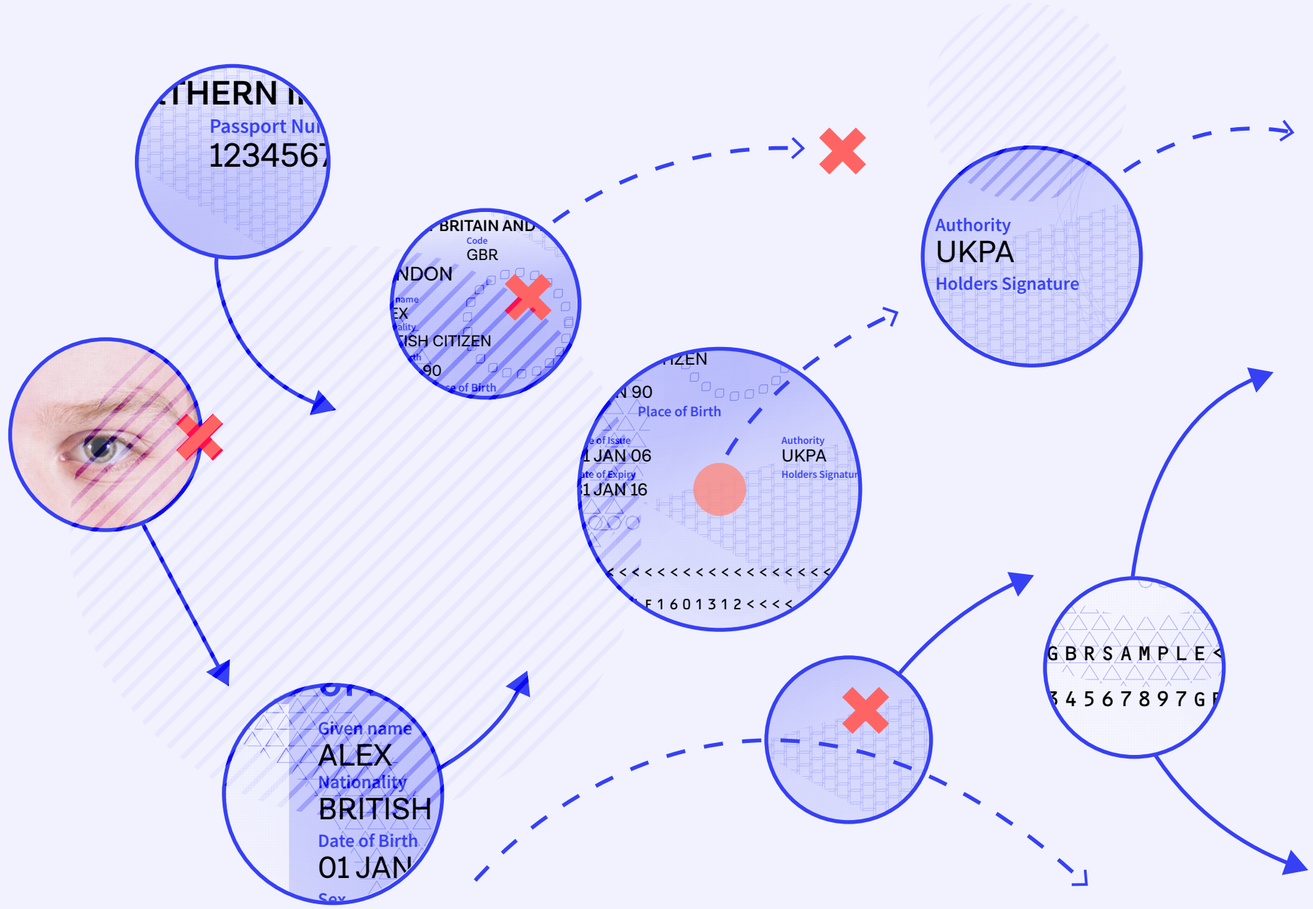
Profil : Opérations sophistiquées de grande envergure, souvent menées par un groupe criminel. Ils auront les moyens de mener des fraudes sophistiquées telles que des deep fakes, des masques 2D et 3D. Ils peuvent également recourir à des techniques comme la coercition.

Volume et fréquence : les entreprises verront moins d'attaques de ce type, mais ce sont celles qui peuvent causer le plus de dégâts dans le plus court laps de temps.

Sophistication: Moyen à dur
Impact, if successful: Élevé

Ce qu'il faut rechercher : La réutilisation d'informations et/ou de types de document, ainsi que les incohérences dans les données du document. D'autres signaux peuvent également être significatifs. Par exemple, si le même arrière-plan est présent sur chaque photo soumise de la pièce d'identité ou du selfie, cela pourrait être un signe que les fraudeurs tentent d'attaquer une entreprise en masse. Enfin, les données de l'appareil et du réseau peuvent sembler suspectes lorsqu'elles sont comparées aux modèles habituels.

Tactiques des fraudeurs

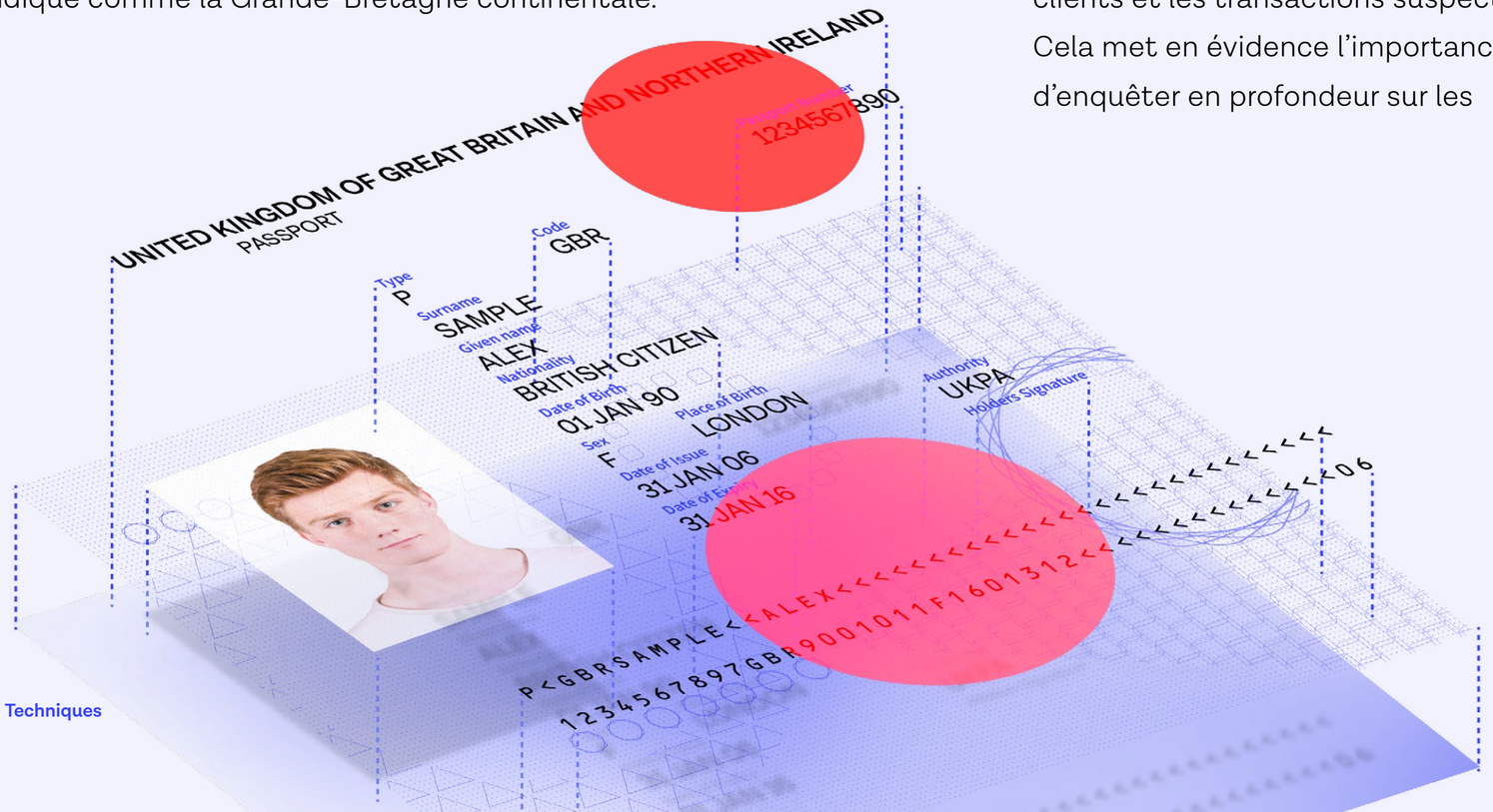


Fraude via la typologie des documents : repérer les fraudes sophistiquées

Lorsqu'il s'agit de prévenir les fraudes sophistiquées, la connaissance de la typologie des documents est souvent ce qui fait la différence. Le croisement d'aspects tels que le pays d'origine ou le numéro de passeport avec d'autres données dans le document mettra souvent en évidence des détails que les fraudeurs ont manqués.

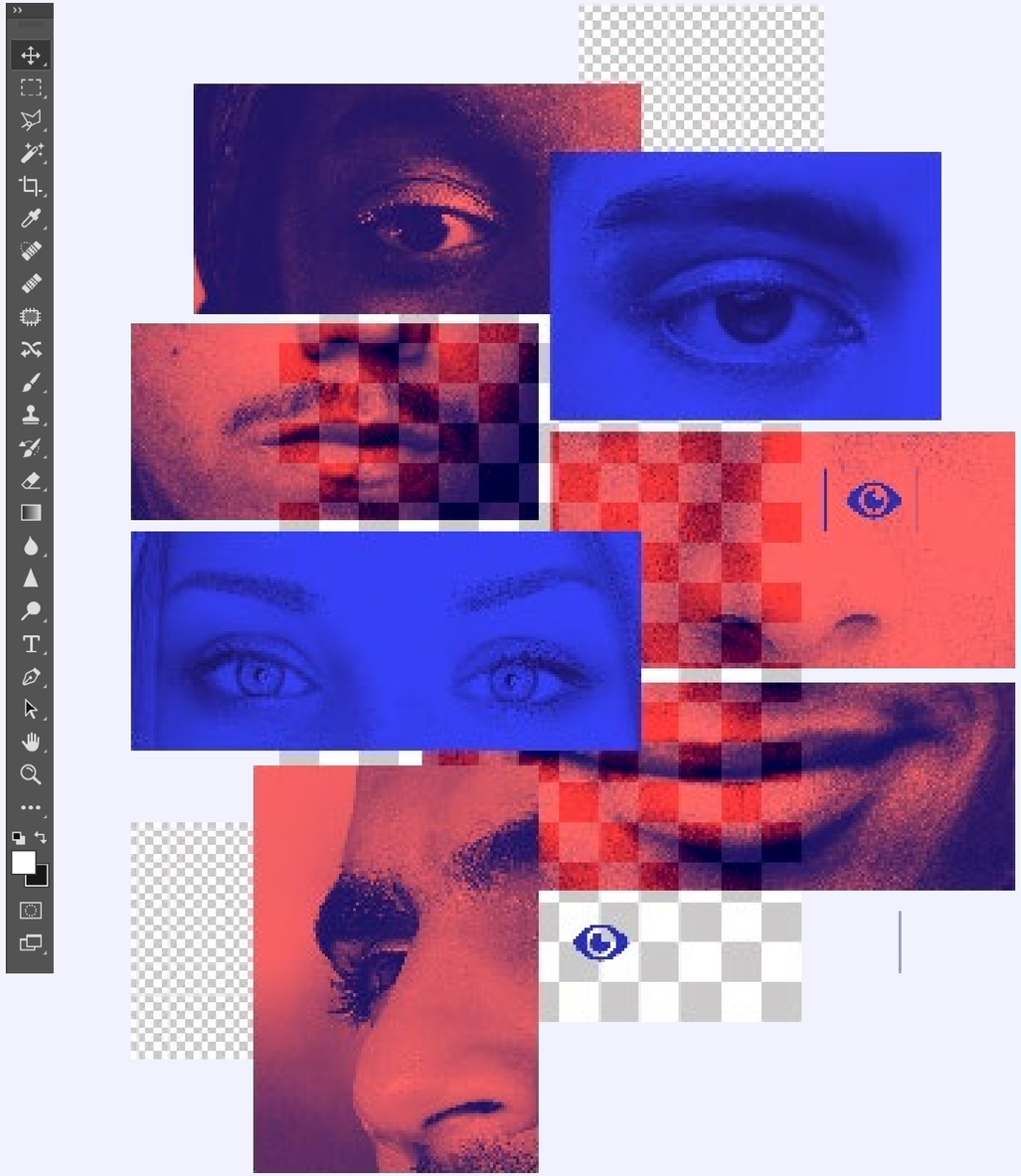
La discordance des données est la clé pour détecter les fraudes sophistiquées.

Dans un cas, nous avons trouvé une différence entre les données sur les passeports britanniques contrefaits que les criminels utilisaient pour ouvrir des comptes bancaires. Les numéros de passeport provenaient d'une série émise dans les îles anglo-normandes, mais le pays d'émission du document était indiqué comme la Grande-Bretagne continentale.



La banque qui a découvert ces criminels les a initialement identifiés à l'aide de contrôles internes faisant le lien entre la base de données clients et les transactions suspectes. Cela met en évidence l'importance d'enquêter en profondeur sur les comptes pour découvrir quelles méthodes ont été utilisées à chaque étape du cycle de vie du criminel. Cela montre également le lien entre les différents types de crimes.

Onfido applique désormais des règles à tous ses clients en fonction de l'autorité émettrice et du format du numéro de document pour bloquer ce type de fraude. Et en tant qu'entreprise, cela peut vous aider à rester au courant des typologies actuelles et à maintenir à jour votre évaluation des risques clients.



Les fraudeurs avertis utilisent Photoshop

Dans cet exemple, nous avons découvert que des criminels fabriquaient des cartes d'identité allemandes contrefaites sophistiquées via Photoshop. Les fraudeurs utilisaient des images virtuelles et des arrière-plans virtuels, ainsi que les bonnes polices sur mesure qu'ils avaient réussi à reproduire.

Une fois que les criminels ont créé un modèle de document, ils l'ont utilisé pour produire plusieurs versions des fausses cartes d'identité avec les mêmes visages, mais des informations personnelles différentes.

Pour éviter ce type de fraude, une entreprise aurait dû examiner manuellement les cartes d'identité allemandes ou conserver une liste de blocage des visages connectés à des documents frauduleux. Une autre solution consiste à utiliser le produit Known Faces d'Onfido, qui permettra de réduire la charge manuelle de l'équipe opérationnelle de l'entreprise.

Tactiques de duplication

Cette année, nous avons constaté une augmentation du nombre d’attaques frauduleuses organisées où les criminels réutilisent les mêmes informations.

Dans trois scénarios différents, nous avons constaté que des criminels s’inscrivaient à des plateformes d’échange de crypto-monnaies ou à des comptes bancaires avec des documents d’identité qui avaient exactement les mêmes visages, mais des informations personnelles modifiées.

Les fraudeurs réutilisent les informations

1.

Les criminels s'inscrivaient à une plateforme d'échange crypto pour réclamer un bonus en espèces en utilisant les mêmes cinq visages sur plus de 1 000 documents d'identité indonésiens. Les seules différences étaient les données personnelles (nom, date de naissance, numéro de document) qui étaient légèrement différentes sur chaque document.

2.

Le deuxième cas impliquait également des bonus en espèces. Les criminels ont utilisé des permis de conduire russes avec le même visage plus de 300 fois par jour pendant deux semaines. Il s'agissait d'une attaque sophistiquée au cours de laquelle ils ont utilisé une manipulation d'image complexe d'un document modèle. La seule différence entre les licences était la légère altération des informations personnelles, que les fraudeurs modifiaient d'un ou deux caractères à chaque fois.

3.

Le scénario final a vu les criminels tenter d'ouvrir des comptes avec une plateforme d'échange de crypto-monnaies pour réclamer, vous l'avez deviné, des bonus en espèces. Cette fois, ils utilisaient des permis de conduire belges avec la même photo. Ils ont fait des centaines de tentatives chaque jour, et la seule différence entre les documents était les deux derniers caractères dans les noms.

Lors d'une mise à jour minime de la typologie ci-dessus, nous avons découvert que les criminels s'inscrivaient sur des comptes bancaires en utilisant les mêmes informations personnelles (par exemple, nom, date de naissance) sur plusieurs documents d'identité, mais avec des photos différentes.

Quand voit-on ces attaques ?

Les groupes criminels et les réseaux de fraude optent le plus souvent pour ces types d'attaques. Un volume de tentatives plus élevé signifie une plus grande chance de succès, et ils ont les ressources nécessaires pour lancer des attaques à grande échelle comme celle-ci.

Nous constatons également une augmentation de ce type de fraudes lorsque les entreprises offrent des bonus en espèces ou des récompenses d'inscription. Si vous envisagez de lancer une campagne comme celle-ci, il vaut la peine de vous assurer que vous avez mis en place des contrôles automatisés pour éviter la charge opérationnelle accrue liée à l'examen des inscriptions ou à la fermeture des comptes par la suite.

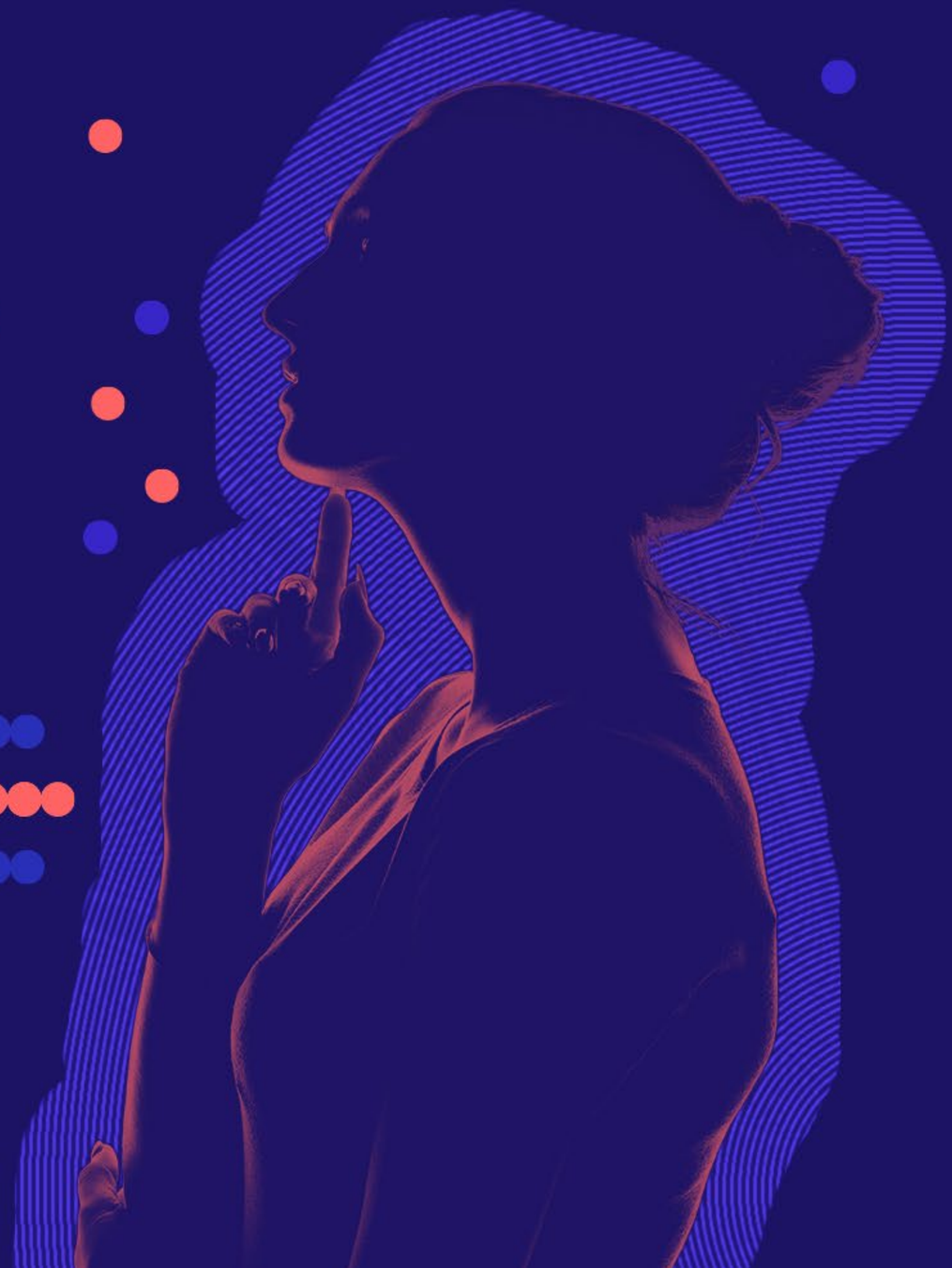
Comment arrêter ce type de fraude ?

Vous pouvez arrêter ce type de fraude, où le même visage est utilisé avec des informations personnelles légèrement modifiées, ou inversement, en utilisant un fournisseur de vérification d'identité comme Onfido.

Notre produit Known Faces vérifie les visages en double utilisés lors de l'inscription.

Un autre contrôle à mettre en œuvre ici consiste à conserver une liste des visages connectés aux tentatives d'inscription frauduleuses connues et à rechercher manuellement vous-même les visages en double. Vous pouvez faire de même pour les informations personnelles en double. Lorsqu'un client s'inscrit avec le même nom et la même date de naissance, ou le même nom et la même adresse, un rapide examen des photos sur les deux documents peut aider à éviter d'inscrire plusieurs fois la même personne.

La Prévention



Onfido Fraud Labs

Comment Onfido améliore son produit pour se protéger contre les dernières tendances et techniques de fraude ?

La plupart des fournisseurs de services de vérification d'identité ne forment leurs modèles que sur des données authentiques. Autrement dit, ils entraînent leurs algorithmes à reconnaître les exemples authentiques et à signaler ce qui ne semble pas authentique.

C'est également ce que nous faisons. Mais nous voulions aussi entraîner nos algorithmes à reconnaître la fraude et à signaler ce qui est considéré comme frauduleux et pourquoi. Cette double approche permet à notre algorithme d'être plus à même à repérer la fraude.

Le challenge

Le machine learning a besoin d'une grande quantité de données nettoyées pour entraîner efficacement les algorithmes. Par rapport à la programmation traditionnelle (voir image), un défi courant avec le machine learning consiste à générer suffisamment de données pour entraîner efficacement les modèles.

Cela est particulièrement vrai dans notre industrie lorsqu'il s'agit de créer des échantillons de données frauduleuses à grande échelle et correctement nettoyées. Il est très difficile d'obtenir suffisamment d'échantillons frauduleux capables d'englober une gamme de vecteurs d'attaque variés. Pour un type de fraude spécifique, nous pourrions n'en voir qu'une sur 100 000.

En comparaison, nous avons accès à un vaste ensemble de données d'exemples authentiques, simplement parce qu'il est beaucoup plus facile d'accéder à des documents authentiques et à des caractéristiques biométriques.

Comment récupérer assez de données frauduleuses pour entraîner nos modèles ?

La solution

Nous avons donc créé le Onfido Fraud Labs. Il s'agit d'un projet dédié à la création de fraudes en interne, avec une équipe d'experts Onfido travaillant ensemble pour répliquer et créer des vecteurs d'attaques frauduleux en masse. Nous utilisons ensuite ces ensembles de données frauduleuses pour entraîner nos algorithmes.

Nous générons ces ensembles de données de deux manières.

1.

En créant des usurpations physiques
(par exemple l'impression de documents, de masques 2D ou 3D)

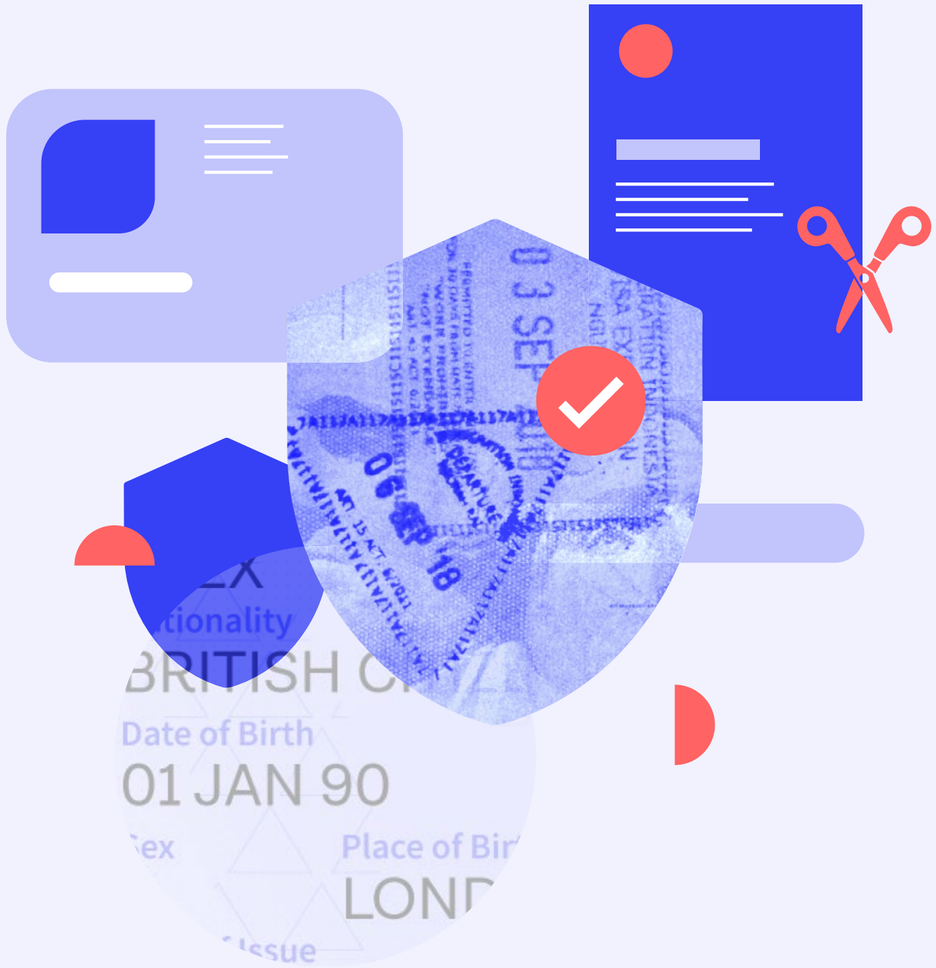
2.

En créant des falsifications numériques
(par exemple en créant des modèles de documents Photoshop ou des masques numériques)

Le résultat

En formant nos modèles avec des ensembles de données frauduleux, ainsi qu'authentiques, nous aidons nos systèmes à mieux détecter la fraude dans le monde réel.

Et non seulement le Onfido Fraud Labs nous aide à détecter les types de fraudes que nous voyons aujourd'hui, mais également les fraudes que nous anticipons. Lorsque nos systèmes peuvent détecter davantage de fraudes, sur un plus large éventail de vecteurs d'attaque, cela nous aide à mieux protéger nos clients et leurs clients.



Préparer l’année à venir

Tendances à surveiller pour 2022 et au-delà

Violations de données

L'année a été chargée pour les hackers. Le nombre de violations de données en 2021 est déjà supérieur de 17 % à celui de toute l'année 2020 [référence]. Cette tendance ne devrait pas changer pour 2022.

Les violations de données peuvent tout compromettre, de l'adresse d'un client à sa date de naissance, son numéro de passeport ou de permis de conduire, ou même les images de la pièce d'identité d'un client. Et les informations recueillies à partir des violations de données permettent aux fraudeurs de continuer et de commettre d'autres types de fraudes.

Reference*

Cela peut inclure :

Attaques de phishing (hameçonnage) ou de spear-phishing (harponnage)

Les fraudeurs encouragent les utilisateurs à effectuer une action spécifique, comme donner d'autres informations d'identification.

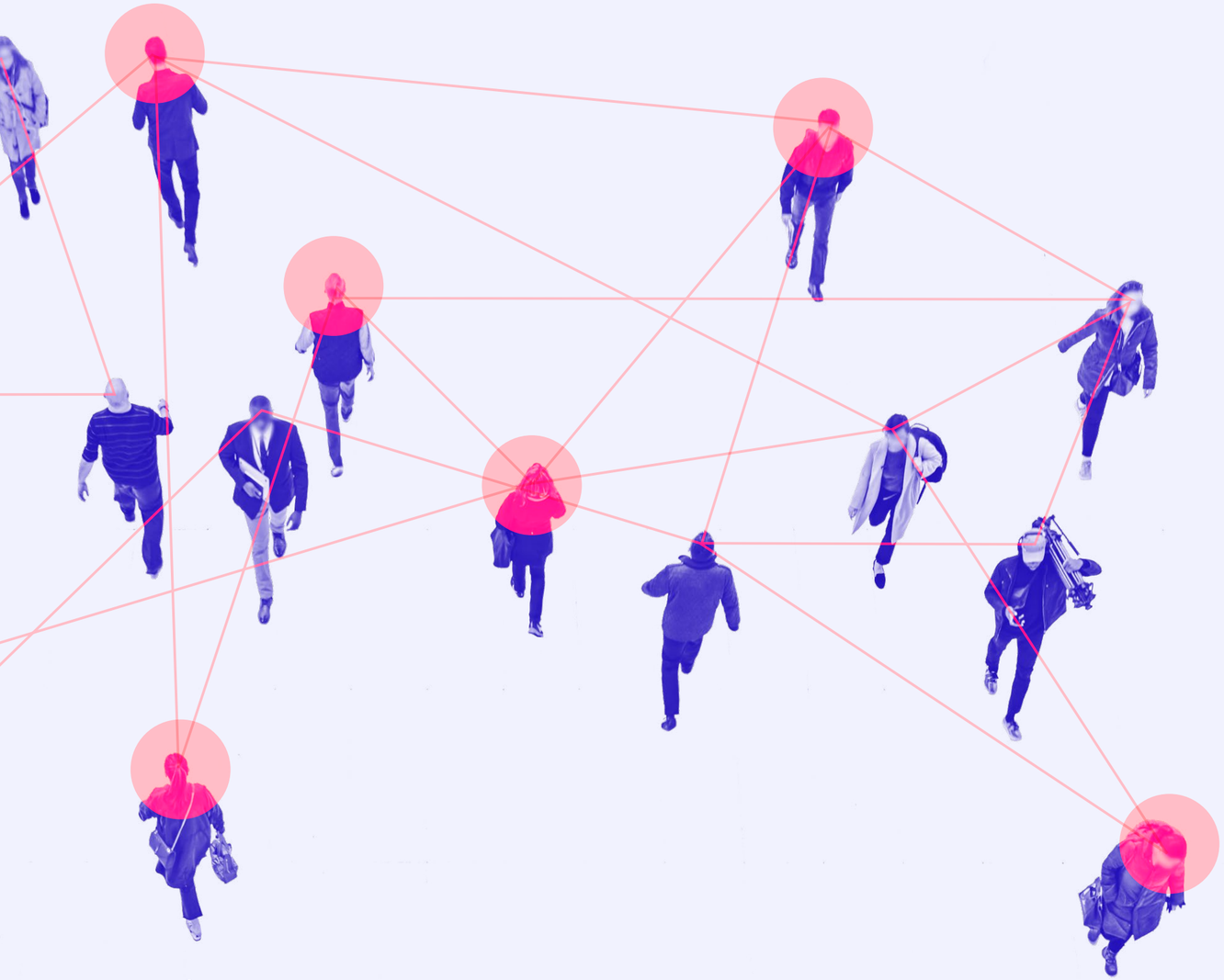
Compromission des e-mails professionnels

Les fraudeurs accèdent aux comptes de messagerie professionnels et imitent l'identité du propriétaire. Leur objectif est de frauder l'entreprise, ses employés, ses clients ou ses partenaires.

Fraude à la prise de contrôle de compte

S'ils ont accès à suffisamment d'informations personnelles, les fraudeurs peuvent usurper l'identité de véritables clients pour accéder à un compte avant d'effectuer des transactions non autorisées.

Avec de grandes quantités de données personnelles disponibles en ligne, les entreprises doivent redoubler d'efforts pour assurer la sécurité de leurs clients.



Attaques réseau

Attaques de Malware (logiciels malveillants)

Si votre réseau n'est pas sécurisé, les fraudeurs peuvent recourir à toute une gamme d'attaques pour contourner ses défenses. La récupération des données sur les logiciels mobiles malveillants (scraping) est un problème qui affecte de nombreux types d'organisations dans divers secteurs. Les pirates informatiques malveillants utilisent le scraping pour collecter des informations sur les entreprises. Ils utiliseront ensuite ces informations pour les cibler avec des attaques plus importantes. Les entreprises doivent auditer leurs sites Web pour s'assurer qu'ils n'exposent pas d'informations sensibles.

Les ransomwares (rançongiciels)

Les ransomwares (rançongiciels) sont une autre forme de cyber-extorsion que les fraudeurs continueront d'exploiter. Ils obligent les utilisateurs à payer une rançon pour accéder à nouveau à leurs données. Les entreprises et les clients doivent maintenir les systèmes d'exploitation mis à jour et corrigés et ne jamais installer de logiciel sans savoir exactement de quoi il s'agit.

Attaques de données synthétiques

Les attaques de données synthétiques, qui impliquent la fusion d'informations réelles et fausses, sont de plus en plus courantes. Nous nous attendons à ce que les fraudeurs continuent de commettre des fraudes d'identité synthétiques, mais à ce qu'ils se tournent probablement également vers d'autres types d'attaques synthétiques.

Deep fakes

Pour la première fois, nous commençons à voir des deep fakes, où les fraudeurs utilisent une forme d'intelligence artificielle appelée deep learning pour générer de fausses vidéos. Ils utilisent cette technologie pour remplacer le visage (ou la voix) de la personne d'origine par celui de quelqu'un d'autre.

Fraude vocale synthétique

De même, la fraude vocale synthétique est un type d'escroquerie audio deep fake où les fraudeurs utilisent un logiciel d'IA capable de cloner des voix. Cette forme de fraude pourrait être utilisée pour essayer de contourner des choses comme le logiciel de reconnaissance vocale d'une banque.

Fraude liée à l’investissement

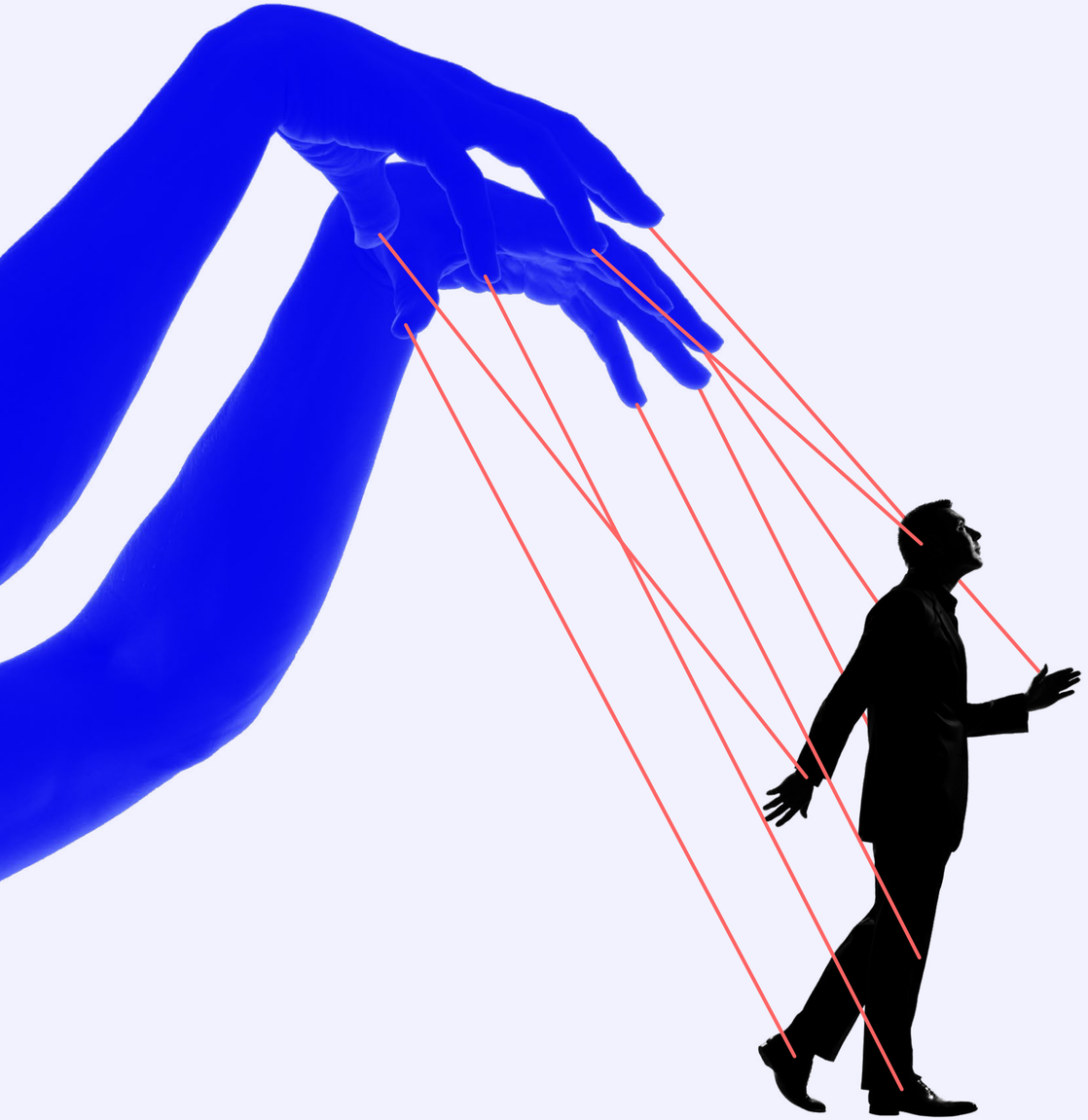
La crypto est un domaine attrayant pour les fraudeurs. Ils continueront de cibler les plateformes d’échange de crypto-monnaies, les plateformes d’investissement et de courtage à l’approche de 2022.

Crypto jacking

L’une de ces méthodes d’attaque est le crypto jacking. Les fraudeurs utilisent l’ordinateur de quelqu’un d’autre pour extraire la crypto-monnaie en incitant les victimes à cliquer sur un lien malveillant. Cela charge ensuite le code de cryptominage sur l’ordinateur. Ils peuvent ensuite voler la crypto-monnaie d’autres portefeuilles numériques ou utiliser les ordinateurs piratés pour extraire des crypto-monnaies de valeur.

Escroqueries à l’investissement

Les fraudeurs cibleront également directement les victimes avec des escroqueries à l’investissement. Ce type d’attaque vise à amener des personnes sans méfiance à remettre de l’argent. Il peut être difficile à repérer, car l’opportunité d’investissement semblera souvent légitime.



Escroqueries par ingénierie sociale et coercition

Les escroqueries par ingénierie sociale ou coercition resteront une méthode de prédilection pour les fraudeurs. Ces attaques nécessitent peu de sophistication technologique, mais les fraudeurs doivent prouver aux victimes qu'elles sont « authentiques ». C'est là qu'ils peuvent utiliser les informations recueillies via des violations de données ou d'autres méthodes. 75% des victimes affirment que les fraudeurs disposaient déjà de leurs informations personnelles lorsqu'ils les ont forcés [référence].

Ces escroqueries sont difficiles à détecter car les fraudeurs n'interagissent pas directement avec l'entreprise. Au lieu de cela, les escrocs convainquent les victimes de se frauder elles-mêmes. Les outils de détection de fraude standard considéreront ces paiements comme « légitimes », car ils proviendront de l'appareil de confiance de l'utilisateur, la connexion réseau correspondra au profil de l'utilisateur et les victimes passeront également toutes les étapes d'authentification.

Eduquer les victimes contre ces formes d'attaques est le meilleur moyen de les prévenir. Cependant, il peut également y avoir des changements subtils dans le comportement numérique qui pourraient suggérer une escroquerie d'ingénierie ou de coercition.

reference*

Bonnes pratiques pour prévenir la fraude

Superposer la vérification d'identité et l'analyse des signaux

Traditionnellement, les entreprises doivent s'appuyer sur des indicateurs pour faire confiance à un nouvel utilisateur. Il s'agit notamment de l'IP de l'appareil, du numéro de téléphone ou des bases de données de crédit. Mais les fraudeurs peuvent également falsifier ces informations . De plus, les violations massives de données ont laissé d'énormes quantités de données à caractère personnel disponibles à la vente sur le dark web. Atlas VPN a trouvé des ensembles de données, notamment des numéros de sécurité sociale, des noms complets, des numéros de permis de conduire, des numéros de passeport et des adresses e-mail disponibles pour aussi peu que 4 $ [référence] .

La superposition des processus d'identité, par exemple en combinant l'identité d'une personne avec sa biométrie physique, aide les entreprises à renforcer l'assurance de l'identité réelle de leurs utilisateurs. La vérification des documents est la première ligne de défense contre la fraude. Et l'ajout de la vérification biométrique aide à protéger contre le vol d'identités et peut dissuader les fraudeurs qui ne veulent pas mettre leur visage sur un nom. Pour les fraudes les plus sophistiquées, envisagez d'utiliser des fonctionnalités de déduplication comme Known Faces d'Onfido.

L'étude Forrester Total Economic Impact TM d'Onfido a révélé que les entreprises qui utilisent la solution de vérification d'identité d'Onfido constatent en moyenne une augmentation de 27% du nombre de comptes frauduleux détectés [référence] .

reference*

reference**

Tirer parti de la technologie de déduplication

Nous avons constaté que les criminels optent de plus en plus pour des attaques de fraude organisée où ils réutilisent les mêmes informations. Par exemple, ils soumettent des centaines de documents avec le même visage ou des numéros de document similaires. Avec ce type d'attaque, les fraudeurs essaient essentiellement d'attaquer votre système en frontal en soumettant encore et encore les mêmes informations d'identification illégitimes.

Known Faces d'Onfido peut aider à protéger votre entreprise contre ces attaques en reconnaissant l'identité des fraudeurs récurrents. Known Faces permet à vos équipes de voir quand un visage en double est entré dans leur système et de suivre son parcours en temps réel.

Utiliser des méthodes d’authentification robustes

Il ne sert à rien de simplement protéger vos clients lors de l’inscription. Les fraudeurs utilisent diverses tactiques tout au long du cycle de vie du client pour tenter d’accéder aux comptes via de fausses demandes de récupération de compte.

Il est tentant de faire franchir la porte aux clients en utilisant une vérification d’identité faible. Pour la corriger plus tard avec des processus d’authentification plus vulnérables tels que les noms d’utilisateur, les mots de passe et l’authentification basée sur les connaissances (KBA). Mais cela expose votre entreprise à la fraude, pénalise la conversion et entraîne de la frustration pour vous et vos clients.

Les entreprises doivent mettre en place des méthodes d’authentification robustes pour s’assurer qu’il s’agit bien que la personne qui tente de récupérer l’accès ou d’effectuer une transaction de grande valeur est bien le propriétaire légitime du compte. Face Authenticate d’Onfido, alimenté par FaceTec, vous permet de vérifier vos clients via un document d’identité émis par le gouvernement et la biométrie faciale lors de l’inscription, vous utilisez alors ces mêmes signaux biométriques pour autoriser les mêmes futurs accès de manière transparente et sécurisée.

Chez Onfido, nous fournissons gratuitement à nos clients un ensemble de kits de développement logiciel (SDK) pour intégrer un flux de capture de documents et de visages optimisé et accessible dans leurs propres applications.
En guise d’alternative, l’API Onfido permet aux clients de soumettre des contrôles de vérification par programmation et est basée sur les principes REST. Il utilise des codes et des verbes HTTP standards, ainsi qu’une authentification basée sur des tokens.

Les SDK offrent plusieurs avantages, notamment la facilité et la flexibilité d’intégration, la validation de la qualité de l’image, une UX excellente et accessible et la dissuasion de la fraude. Et dans l’ensemble, nous voyons moins de cas suspects de fraude via nos SDK. En effet, la capture en direct réduit considérablement le risque de soumission d’images falsifiées numériquement et nos contrôles d’intégrité de l’appareil garantissent l’authenticité des captures.

Contributeurs

Michael Van Gestel
General Manager & Global Fraud Expert

Simon Horswell
Document Specialist Lead

Dimitrie Dorgan
Senior Fraud Risk Manager

Sarah Munro
Director of Product (Biometrics)

Giulia Di Nola
Biometrics Product Manager

Albert Roux
Director of Fraud

Vincent Guillevic
Staff Product Designer

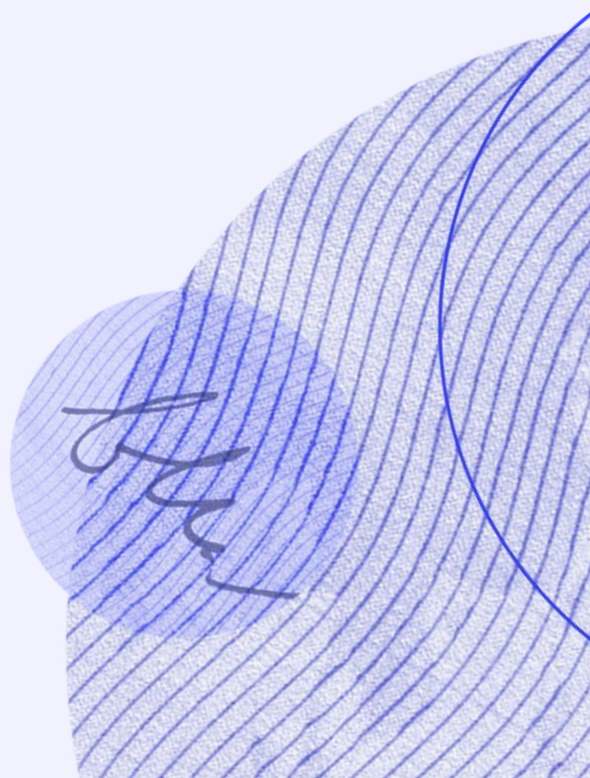
Virginia Chiarentin
Product Operations Manager

With thanks to Cable Tech

cable

Vous souhaitez en savoir plus sur les tendances en matière de fraude et sur la manière de protéger votre entreprise contre celles-ci ?

Contactez-nous



onfido | Real Identity