Comment protéger vos détenteurs de compte contre les escrocs.

celebrus

Les pertes dues aux escroqueries augmentent

Les tactiques d'escroquerie sont de plus en plus utilisées pour duper les clients des banques afin qu'ils transfèrent des fonds vers des comptes contrôlés par des fraudeurs. Les banques, qui ont traditionnellement offert des programmes de sensibilisation et d'éducation à leurs clients pour lutter contre ces menaces, recherchent des méthodes plus solides pour différencier leurs offres de services et mieux protéger leurs clients.

Mais attraper les escrocs est très difficile. Les fraudeurs choisissent des stratégies d'escroquerie difficiles à détecter – les escroqueries impliquent des tromperies sophistiquées qui amènent les clients à transférer volontairement de l'argent aux comptes mules contrôlés par des fraudeurs. L'argent perdu est effectivement irrécupérable dans ces situations. Alors, comment une banque peut-elle identifier et prévenir une escroquerie lorsque la victime a échoué à le faire ?

+ 62%
Escroqueries amoureuses

+123%
Escroqueries par usurpation d'identité

+95%
Escroqueries en matière d'investissement

Les banques et les organisations financières peuvent protéger leurs clients contre les escroqueries, la fraude en ligne et la criminalité financière en utilisant les comportements uniques des fraudeurs pour les identifier.

Malgré l'évolution de leurs techniques, les fraudeurs ne peuvent pas reproduire la façon dont les utilisateurs authentiques se comportent lorsqu'ils accèdent aux plateformes en ligne et effectuent des paiements.

Lorsqu'un client est entraîné dans une arnaque, il se comporte différemment, et ces données en temps réel offrent à la banque une occasion unique de détecter et d'arrêter l'escroquerie. En tirant parti des informations comportementales automatisées qui fonctionnent de manière transparente avec vos outils de gestion de la fraude existants, vous pouvez arrêter les escroqueries instantanément.

Les organisations qui travaillent de manière proactive pour protéger les titulaires de comptes contre les escrocs se différencient sur le marché et fidélisent à long terme.

Bien que le débat fasse rage sur la question de savoir si les banques et les institutions financières devraient être responsables des pertes de clients dues à leur propre négligence, la réalité est qu'en aidant à protéger vos titulaires de compte contre les escrocs, vous construisez la confiance, l'autorité et une forte fidélité avec vos clients. Et n'oubliez pas l'avantage financier direct – éliminer des heures et des heures d'appels d'assistance inutiles lorsqu'un client se rend compte qu'il a été victime d'une arnaque et contacte votre organisation pour obtenir de l'aide.

En utilisant une solution en temps réel qui offre une authentification fluide, invisible et continue, vous pouvez transformer l'expérience client et fournir une protection transparente contre les escroqueries. La détection en temps réel est un élément essentiel des solutions de lutte contre la fraude, car la clé est de signaler instantanément les comportements anormaux des clients qui indiquent qu'ils sont victimes d'une arnaque, ce qui vous permet de prendre des mesures immédiates.

Principaux points à retenir

- Les pertes dues eux escroquerie augmentent et les entreprises qui protègent leurs clients se différencient,
- L'exploitation des données pour identifier les fraudeurs en fonction de leurs comportements uniques aide à prévenir les escroqueries,
- Aider à prévenir les escroqueries fidélise les clients et réduit les coûts de gestion de la fraude,
- L'authentification sans friction améliore l'expérience client tout en offrant une protection contre la fraude.

Protégez vos titulaires de compte contre les escroqueries courantes

Jetons un coup d'œil aux quatre types d'escroqueries les plus courants et à la façon dont la détection moderne de la fraude peut les prévenir en temps réel.

Escroqueries par usurpation d'identité

Les escroqueries par usurpation d'identité sont l'une des attaques les plus créatives, car les fraudeurs prétendent être une personne ou une entreprise apparemment légitime et créent souvent des e-mails, des comptes et d'autres actifs avec des informations copiées.

Au début, cela peut être exécuté simplement pour collecter des informations pour une utilisation ultérieure dans la réalisation de l'escroquerie.

Une fois le faux profil établi, il est utilisé pour collecter des fonds provenant de l'escroquerie. Rien qu'au Royaume-Uni, les escroqueries par usurpation d'identité ont plus que doublé au cours du premier semestre de 2021, les fraudeurs ayant continué d'étendre leurs tactiques d'escroquerie.

Ces escroqueries peuvent cibler à la fois les consommateurs et les entreprises, car les fraudeurs peuvent également prendre le contrôle ou usurper le courrier électronique des employés, des clients d'une entreprise, ou des vendeurs. Ceci est particulièrement puissant lorsque la « demande » provient d'un gestionnaire ou d'un cadre supérieur. Pour l'usurpation d'identité de fournisseur, cela peut être aussi simple que de modifier les détails du compte sur une facture à l'aide d'un e-mail usurpé. Dans tous les cas, le fraudeur disparaît après l'escroquerie – n'ayant jamais interagi directement avec un système bancaire. Voyons à quoi cela pourrait ressembler :

Escroqueries par usurpation d'identité.

1 – Le fraudeur obtient une partie des informations de la banque, du contact et d'autres détails clés de la victime.

2 – Le fraudeur contacte ensuite la victime, prétendant provenir d'une source fiable comme la police ou sa banque.

3 – La victime est convaincue de sa légitimité parce que le fraudeur dispose d'informations privilégiées clés.

4 – Le fraudeur dit à la victime que ses économies sont attaquées ou qu'une amende est due et qu'elle doit effectuer un paiement

5 – La victime clique sur un lien, ou appelle une hotline exploitée par le fraudeur, pour effectuer le paiement « urgent ».

6 – La victime effectue un paiement au fraudeur et n'est pas au courant de la fraude pendant de nombreuses heures, voire plusieurs jours.

Escroqueries en matière d'investissement.

Elles impliquent généralement des promesses de gros paiements, d'argent rapide ou de rendements garantis en échange d'un investissement d'argent, souvent pour peu ou pas de risque. Bien que cela puisse sembler être la situation classique « si c'est trop beau pour être vrai, c'est probablement le cas », les escroqueries en matière d'investissement peuvent être très sophistiquées et convaincantes. L'essor de la crypto-monnaie a également entraîné une augmentation des escroqueries en matière d'investissement, car il est plus facile pour les fraudeurs de profiter d'un environnement moins réglementé.

Les comptes mules sont généralement utilisés pour déplacer et extraire de l'argent avec des escroqueries d'investissement. Bien qu'il soit difficile pour les institutions financières de suivre les comptes muletiers de manière indépendante, les solutions avancées en matière de fraude exploitent la puissance des réseaux de renseignement sur la fraude pour identifier les comptes et identités compromis. Cela signifie que lorsqu'un consommateur tente d'effectuer un paiement sur un compte muletier, il est instantanément averti et peut être empêché.

1 – Le fraudeur ouvre une série de comptes « muletiers » dans le but d'extraire des fonds des victimes sans être détecté.

2 – La victime est contactée par le fraudeur ou répond à une annonce pour une opportunité d'investissement.

3 – Le fraudeur incite la victime à transférer de l'argent à un fond fictif ou à payer pour un faux investissement, créant une urgence avec une limite de temps ou une prime pour investir avant une date fixée.

4 – Les nombreuses victimes ne découvrent pas l'escroquerie avant es semaines, voire des mois.

Escroqueries amoureuses

Les escroqueries amoureuses sont l'une des fraudes les plus courantes sur le marché – rien qu'aux États-Unis, des pertes énormes de 1 milliard de dollars ont été signalées en 2021 selon le FBI.

Ces escrocs profitent des émotions de la victime et ont diverses approches pour escroquer leurs cibles. Voici un cycle de vie typique de l'escroquerie amoureuse :

1 – Le fraudeur établit un certain nombre de faux comptes de rencontres en ligne ou de médias sociaux.

2 – Les victimes potentielle sont contactées par le fraudeur dans l'intention d'établir une fausse relation.

3 – Lorsqu'une victime réagit, le fraudeur utilise une gamme de tactiques malveillantes pour établir un lien solide sur une longue période.

4 – Une fois qu'une relation a été établie, le fraudeur demande un peit paiement, tissant une histoire de difficultés financières.

5 – La victime désigne le fraudeur comme nouveau bénéficiaire et effectue plusieurs petits paiements au fil du temps.

6 – Le fraudeur convainc la victime de faire un paiement beaucoup plus important, invoquant souvent une urgence médicale ou familiale, ou voulant rencontrer la victime en personne.

Escroqueries par imposteur

Dans une escroquerie par imposteur, une personne malhonnête ment et incite la victime à lui envoyer de l'argent. Ils peuvent appeler au téléphone ou envoyer un courriel ou un message texte. Les imposteurs peuvent essayer d'obtenir un paiement en demandant à la victime d'acheter une carte-cadeau ou un virement bancaire. Il existe de nombreuses variantes, mais elles fonctionnent de la même manière – un escroc prétend être quelqu'un en qui vous avez confiance pour vous convaincre de lui envoyer de l'argent.

Cela peut prendre la forme d'un compte de médias sociaux cloné d'un ami proche ou d'un parent, donnant l'impression qu'il s'agit d'une personne connue, ou d'une organisation familière telle qu'une organisation gouvernementale ou un organisme de bienfaisance. Plus de 2,3 milliards de dollars de pertes déclarées par les consommateurs américains en 2021 étaient dues à des escroqueries par imposteur, soit près du double de ce qu'elles étaient en 2020.

1 – Le fraudeur obtient une liste de contacts de médias sociaux.

2 – Le fraudeur crée un compte de médias sociaux copie d'un ou plusieurs contacts de la victime.

3 – Le fraudeur contacte la victime avec le faux compte, lui demandant d'envoyer de l'argent.

4 – La victime envoie la carte-cadeau ou transfère l'argent, croyant qu'elle une personne qu'elle connaît.

5 – La victime n'est peut-être pas au courant de l'escroquerie avant des heures, des jours ou même des semaines.

Comment protéger vos détenteurs de compte

Le signalement de nouvelles destinations, de nouveaux destinataires et de nouveaux comptes est un comportement opérationnel standard pour la détection des fraudes, mais sans contexte, il est difficile de déchiffrer lesquels sont légitimes ou ceux qui sont provoqués par un escroc. Les règles habituelles de prévention de la fraude ne s'appliquent pas tout à fait, car dans la plupart des cas d'escroquerie, un client réel et authentifié est connecté à son compte afin d'effectuer le paiement. L'objectif est d'identifier rapidement les activités à haut risque, de sorte que la contextualisation est essentielle pour détecter les victimes potentielles d'une escroquerie. Déterminer si l'activité est conforme aux interactions typiques du client, identifier et tracer les comptes muletiers signalés et superposer la biométrie comportementale à tout cela crée une recette pour réussir à identifier et à prévenir les attaques sur vos titulaires de compte.

Grâce à une plate-forme avancée de données sur la fraude, les entreprises peuvent protéger leurs titulaires de comptes valides en excluant les imposteurs. Il existe **7 domaines clés** dans lesquels une plate-forme de données complète permet une prévention proactive de la fraude :

1. Comparer les interactions des utilisateurs avec le profil historique.
2. Comparer les interactions des utilisateurs avec des profils connus bons ou mauvais.
3. Collectez des signaux et des scores en temps réel pour détecter la fraude.
4. Obtenir des informations supplémentaires à partir du modèle de données pour les enquêtes, l'IA, les règles et les rapports.
5. Incorporer des signaux cognitifs tels que des raccourcis, des modèles de frappe, le temps de réponse, la mémoire/rappel et le collage de données dans le profil d'identité.
6. Capturez les informations personnelles des bénéficiaires en temps réel pour permettre un suivi et une enquête plus approfondie.
7. Utilisez la biométrie comportementale et les signaux cognitifs pour identifier instantanément les fraudeurs.

La biométrie comportementale est l'ingrédient secret dans la détection et la prévention des escroqueries. Avec une plateforme de données intégrant la biométrie comportementale, l'entreprise peut constamment créer des profils de comportement légitime des utilisateurs. Par exemple, un client bancaire typique ne demande probablement pas de virements bancaires régulièrement, voire pas du tout. Lorsque ce client tente de proposer un virement bancaire, à la demande d'un escroc créatif, il hésitera souvent et prendra plus de temps pour trouver ce qu'ils recherchent, remplir les informations nécessaires, etc. Il s'agit d'un point de données pour la plateforme de données sur la fraude à incorporer avec tous les autres points de données. Les signaux de comportement biométrique d'une victime sont également très différents lorsqu'elle se connecte à son compte si elle panique ou est pressée. Les utilisateurs qui craignent de perdre leurs économies de toute une vie ou qui se précipitent pour profiter d'une opportunité limitée dans le temps ne peuvent s'empêcher de traduire ces émotions en vitesse de frappe, en gestes, etc. De même, une victime d'escroquerie amoureuse ou d'usurpation peut hésiter, se demandant si cette nouvelle personne (ou personne connue) les remboursera. Ces anomalies de comportement sont collectées, détectées et envoyées sous forme de signaux aux systèmes et aux équipes de gestion de la fraude en quelques millisecondes.

Une solution de fraude moderne peut également détecter automatiquement les comportements couramment exposés par les personnes escroquées, sur la base de centaines de milliers d'interactions suivies au fil du temps. La notation avancée et l'intelligence artificielle (IA) peuvent contextualiser davantage les comportements connus de l'escroquerie contre les victimes, par exemple dans le cas des escroqueries amoureuses où les fraudeurs intensifient souvent leurs demandes d'argent ou de cadeaux.

Celebrus for Fraud vous aide à protéger vos clients contre les escrocs

Celebrus for Fraud, la principale solution de défense contre la fraude en temps réel, vous permet d'attraper le fraudeur avant la fraude en tirant parti des riches données comportementales capturées par notre plate-forme.

Celebrus capture toutes les interactions des clients sur votre site Web, votre application mobile et vos appareils IOT. Notre technologie préconfigurée et conviviale pour les analystes détecte automatiquement les comportements couramment exposés par les personnes arnaquées.

Des tableaux de bord sophistiqués et une IA intégrée fournissent des informations instantanées pour mettre fin aux escroqueries avant que vos clients ne soient escroqués de leur argent.

Celebrus définit les événements et les signaux pour la détection des fraudes, signale et capture de nouvelles informations sur les bénéficiaires, y compris les PII, en quelques millisecondes.

Les données et signaux détaillés sont ensuite envoyés aux systèmes et aux équipes de gestion de la fraude pour une enquête plus approfondie et/ou un blocage des paiements en temps réel.

Par exemple, des signaux définis peuvent déclencher un message sur l'écran de la victime disant « Arrêtez-vous et réfléchissez – connaissez-vous cette personne ? Vous ne récupérerez peut-être jamais cet argent ! S'il vous plaît appelez-nous immédiatement », puis le paiement est bloqué ou arrêté pour une enquête plus approfondie en temps réel.

L'analyse comportementale en temps réel de Celebrus fournit à votre organisation les outils dont vous avez besoin pour garder une longueur d'avance sur les escrocs. Et il n'est pas nécessaire de remplacer votre système de gestion de la fraude, de vérification d'identité ou d'authentification existant.

Celebrus améliore parfaitement ces applications pour offrir une prévention de la fraude de niveau supérieur. Nous fournissons également un support complet et des services gérés si vous recherchez une solution complète.

Découvrez comment Celebrus peut vous aider à suivre, contextualiser et identifier les ccomportements frauduleux pour protéger vos clients contre les escroqueries.