Comment vaincre les fraudeurs créatifs :

Passer de la détection des fraudes à la prévention

celebrus

Comment vaincre les fraudeurs créatifs : passer de la détection des fraudes à la prévention

Les consommateurs s'empressent d'adopter des alternatives digitales aux interactions en face à face, d'autant plus que la COVID-19 a bouleversé le statu quo. Malheureusement, les fraudeurs redoublent également d'efforts. La volatilité des marchés économiques et politiques, l'inflation et l'augmentation des voyages offrent aux cybercriminels encore plus d'opportunités à exploiter, et c'est ce qu'ils font.

Les fraudeurs digitaux sont un groupe innovant – ils adaptent et font évoluer leurs techniques en permanence pour déjouer les technologies antifraudes actuelles et maximiser leur succès. Il est temps pour les entreprises de s'adapter et de passer à l'offensive.

Les tendances sont à la hausse, dans tous les secteurs. Selon le rapport 2022 sur l'état de la fraude et de la sécurité des comptes, la majorité des secteurs ont connu une augmentation de 400 % des attaques, et ceux du secteur du voyage ont connu une réapparition majeure – 45 % du trafic sur les sites de voyage proviendrait d'attaques de scraping.

Des informations récentes montrent qu'une connexion sur cinq est une tentative de piratage de compte, avec une augmentation globale de 85 % des attaques sur les connexions et les inscriptions.

De plus,

- + de 70 % d'augmentation des pertes signalées liées à la fraude en 2021 (FTC)
- Augmentation de 98 % des attaques par bourrage d'identifiants (utilisation de l'automatisation pour essayer différents noms d'utilisateur et mots de passe à grande échelle) – leur nombre devait doubler en 2022 (Arkose Labs)
- Augmentation de 85 % des attaques de connexion et d'enregistrement en 2021 (Arkose Labs)
- 2/3 des entreprises des secteurs de la technologie, des médias et des télécommunications ont été victimes d'une forme de fraude en 2021 (PwC)
- Les fintechs ont un taux de fraude moyen d'environ 0,30 %, soit le double de celui des cartes de crédit qui se situent en moyenne entre 0,15 et 0,20 %. (Experian)

Le vol d'identité synthétique, l'un des types de fraude les plus créatifs, est en plein essor lorsque les fraudeurs créent de fausses identités pour escroquer les entreprises, en particulier dans les services financiers et les assurances. De nouvelles catégories de technologies financières, comme le paiement différé (BNPL), se développent et offrent de plus en plus d'opportunités de fraude dans le commerce de détail. Et la liste est longue. Dès que les experts en fraude peuvent détecter et empêcher un type de fraude, un autre émerge.

Dans le même temps, l'augmentation des réglementations en matière de confidentialité et de conformité rend plus difficile pour les professionnels de la fraude et de la sécurité de faire la différence entre les « bons » et les « mauvais » acteurs.

Ce guide explore l'essor de la fraude numérique et comment battre les fraudeurs à leur propre jeu.

Contenu

Aperçu du paysage de la fraude digitale

La fraude digitale est en hausse. Les fraudeurs ont rapidement mis au point de nouvelles stratégies pour exploiter les canaux digitaux, ce qui a entraîné une montée en flèche des pertes financières. Avec l'émergence des paiements en temps réel, les pertes se produisent rapidement et la capacité de récupération est faible.

Avec la pression croissante exercée par les régulateurs sur les banques pour qu'elles agissent, la détection et la prévention sont devenues une priorité absolue pour les services financiers.

La plupart des solutions actuelles de lutte contre la fraude sont inadéquates et n'ont pas la sophistication nécessaire pour activer toutes les données, qu'elles soient transactionnelles ou digitales. Les solutions nouvelles et traditionnelles sont réactives et non préventives. Elles sont conçues pour identifier la fraude une fois qu'elle s'est déjà produite, lorsqu'il est trop tard pour faire quoi que ce soit à ce sujet.

Les solutions traditionnelles de lutte contre la fraude sont transactionnelles et rétrospectives. Ils ne s'intéressent qu'aux transactions unitaires effectuées et aux modèles de transactions historiques. Ces solutions ignorent les comportements détectés autour de chaque transaction et s'appuient plutôt sur des règles de décision rigides et difficiles à adapter.

Les nouvelles solutions de lutte contre la fraude se concentrent uniquement sur la détection comportementale et constituent souvent une boîte noire. Elles offrent une analyse biométrique comportementale, mais n'intègrent pas de connaissances transactionnelles. Ces solutions sont peu précises et manquent généralement d'explicabilité.

La majorité des solutions de lutte contre la fraude, qu'elles soient nouvelles ou traditionnelles, permettent de détecter et d'enquêter sur la fraude après qu'elle se soit produite, mais ne sont pas en mesure de prévenir la fraude en temps réel. Dans un monde de paiements digitaux en temps réel, ces solutions sont à la traîne.

Vous n'avez pas besoin de plus de données, vous avez besoin de perspective.

Les données à elles seules ne peuvent pas fournir la perspective nécessaire pour activer la prévention de la fraude en temps réel. Lorsqu'il s'agit de données en contexte, la perspective est essentielle.
Le contexte est essentiel pour détecter et prévenir la fraude, tout comme la rapidité.

Les solutions de lutte contre la fraude nouvelles et traditionnelles ne peuvent pas suivre l'évolution rapide des stratégies utilisées par les fraudeurs pour échapper à la détection. Une solution de lutte contre la fraude contextuelle, évolutive nécessite 5 fonctionnalités clés :

1. Combiner les transactions et les interactions :

La combinaison d'informations transactionnelles conventionnelles avec des données comportementales pour décrire les interactions digitales peut fournir des informations contextuelles précieuses qui permettent d'obtenir des connaissances plus riches, y compris la détection des comportements frauduleux.

2. Faire correspondre les identités pour détecter les clients :

Au fur et à mesure que les clients passent d'un canal à l'autre, plusieurs systèmes capturent les données client dans différents formats. La solution de lutte contre la fraude doit être capable de faire correspondre et de relier les profils des clients à travers diverses sources de données.

3. Bénéficier d'une précision accrue avec des millions de modèles :

La formation et le déploiement d'un modèle personnalisé d'IA ou d'apprentissage automatique pour chaque client permettent de détecter plus précisément si les interactions proviennent de clients légitimes ou d'imposteurs.

4. Agir en temps réel pour piloter l'intervention :

Grâce à des temps de réponse de l'ordre de la milliseconde, les entreprises peuvent non seulement détecter les fraudes, mais conduire également une intervention qui permet d'éviter les pertes.

5. Apprendre et évoluer en continu :

L'utilisation de l'intelligence artificielle (IA) et des méthodes d'apprentissage automatique pour former en permanence sur le comportement des utilisateurs permet de détecter de nouvelles tactiques de fraude au fur et à mesure qu'elles apparaissent, offrant ainsi une solution évolutive.

Passer de la détection à la prévention

Pour mettre fin à la fraude, vous avez besoin d'une solution qui vous permette de comprendre les acteurs malveillants et d'intervenir dans leurs parcours avec des actions préventives en temps réel.

L'intervention elle-même peut être définie par la gravité et la probabilité de fraude et peut aller d'un message d'avertissement à un paiement bloqué.

Pour prévenir activement la fraude, votre solution doit :

Écouter

Créer une vue contextuelle de chaque transaction, en combinant des informations détaillées sur la transaction et les comportements digitaux qui illustrent la façon dont les utilisateurs naviguent, se déplacent et interagissent avec les canaux digitaux.

Comprendre

Profiler et comparer un client individuel avec le comportement attendu en appliquant des modèles d'IA et d'apprentissage automatique hyper-personnalisés en temps réel pour quantifier le risque de fraude.

Décider

Utiliser votre processus décisionnel pour déterminer si une intervention est nécessaire et, le cas échéant, la gravité. Visez un équilibre entre la minimisation des pertes, l'optimisation de l'expérience et la réduction des coûts de gestion de la fraude.

Agir

Si la menace est évaluée comme une fraude, effectuer l'intervention appropriée en temps réel pour la prévenir. Si elle est jugée authentique, autoriser la transaction à se poursuivre.

La prise de décision contextuelle permet une prévention de la fraude en temps réel à grande échelle

La génération de données plus précises, opportunes et contextualisées fournit des informations qui simplifient les enquêtes et améliorent l'efficacité. En réduisant les enquêtes sur les fraudes et la gestion des dossiers, votre organisation peut éliminer des frais généraux et améliorer l'efficacité globale.

La capture de plusieurs points de données sur plusieurs canaux, pour des millions d'utilisateurs, et la contextualisation des données transactionnelles avec des données comportementales nécessitent une quantité massive de travail et d'informations. L'automatisation de ce processus et l'utilisation d'une technologie intelligente rationalisent considérablement le processus pour l'exécuter à grande échelle. Bien que les fraudeurs soient de plus en plus sophistiqués, les mêmes règles s'appliquent à l'inverse : les entreprises financières et autres doivent devenir plus sophistiquées dans leurs solutions de prévention de la fraude.

En intervenant en temps réel dans les transactions frauduleuses, vous pouvez non seulement réduire les pertes dues à la fraude, mais aussi réduire les faux positifs.
Cela améliore l'expérience client car vous n'arrêtez que les transactions frauduleuses, pas les transactions authentiques, ce qui réduit considérablement les frictions avec les clients. Intervenir de manière proactive pour protéger les clients à risque permet également d'améliorer l'expérience client.
Avec une solution anti-fraude tournée vers l'avenir, vous pouvez faire face à l'évolution des menaces et garder une longueur d'avance sur les nouveaux types et stratégies de fraude.

Par exemple, l'un de nos clients, l'une des 5 plus grandes banques mondiales, était aux prises avec une fraude par prise de contrôle d'accès à distance (RAT), qui a augmenté de 15 % pendant la COVID. La banque subissait plus de 2 000 cas de fraude par mois et perdait 2 700 $ par cas de fraude. Face à l'escalade des pertes et de la pression exercée par les régulateurs, la banque devait agir rapidement. Ils avaient besoin d'une solution en temps réel pour détecter les fraudes et prévenir les pertes avant qu'elles ne se produisent.

La banque a déployé Celebrus pour la capture de données complète en temps réel et l'identification des utilisateurs sur tous les canaux, ainsi que Teradata Vantage pour la configuration des données et l'analyse à l'échelle de l'entreprise. Ils ont mis en place une solution de lutte contre la fraude comportementale hyper-personnalisée pour prévenir la fraude, améliorer l'expérience client, réduire les pertes et améliorer l'efficacité de l'entreprise.

Avec 250 000 parcours clients uniques par heure aux heures de pointe, il y avait beaucoup de données à traiter. La solution combinée a commencé par la capture des interactions digitales en temps réel, puis l'analyse des données pour détecter les modèles transactionnels et comportementaux. Ils ont été en mesure d'exécuter des millions de micro-modèles pour évaluer les comportements et déployer des informations dans des temps de réponse inférieurs à la seconde.

Les résultats ont été impressionnants :

- 70 % des cas de fraude de la banque sont désormais détectables et évitables
- 100 millions de dollars de fraude détectée et évitée

Pour prévenir la fraude, il est essentiel de permettre à l'utilisateur de prendre des décisions et d'agir contextuellement pendant qu'il est en direct sur un canal digital.

La biométrie comportementale et la course à l'armement technologique de l'escroquerie

Au fil des ans, les institutions financières ont développé des moyens d'éradiquer la fraude et les escroqueries.

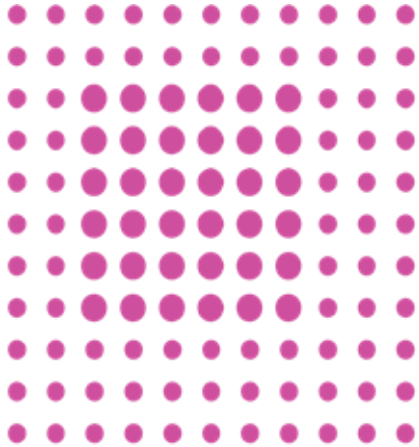
Les banques et les émetteurs de cartes ont dépensé des millions de dollars pour mettre en œuvre des algorithmes afin d'analyser l'activité des transactions à la recherche d'anomalies permettant de découvrir des comptes ou des informations d'identification compromis pour que les équipes d'analyse de la fraude puissent enquêter. Leurs modèles de données examinent des modèles globaux, tels que le temps passé sur des pages Web spécifiques ou l'emplacement de l'appareil pour vérifier la crédibilité des transactions ou des montants des transactions. Cependant, ces systèmes basés sur des règles sont facilement infiltrés par des fraudeurs entreprenants, généralement détectés trop tard pour prendre les fraudeurs en flagrant délit.

Les technologies de biométrie comportementale offrent une alternative supérieure pour aider à identifier les anomalies comportementales et à mieux se protéger contre la fraude. La biométrie comportementale utilise plusieurs points de données, tels que la façon dont une personne tient, touche ou tape sur son appareil, pour se prémunir contre les types d'attaques connus et inconnus.

Les données collectées peuvent être utilisées pour suivre l'activité des victimes d'escroquerie sur tous les appareils et systèmes afin de trouver les identités associées violées par les escrocs et de définir des alertes en fonction de ces activités. Lorsqu'elle est combinée aux systèmes traditionnels de prévention de la fraude, la biométrie comportementale permet à des organisations telles que les institutions financières de détecter et de prévenir une série d'escroqueries en temps réel, à grande échelle, de manière automatisée et avec un degré très élevé d'exactitude. Ils offrent aux équipes de lutte contre la fraude une couche supplémentaire de données pour révolutionner la prévention de la fraude en connectant les activités frauduleuses pour découvrir les réseaux d'escroquerie.

Bien qu'en théorie, il soit possible pour les escrocs de tromper la technologie d'identification et d'imiter une personne réelle, la réalité est que cela ne serait efficace qu'avec une approche ponctuelle. Il faut beaucoup de temps, de ressources et de programmation pour contourner efficacement la biométrie comportementale à grande échelle. La plupart des attaquants ne disposent tout simplement pas de ces ressources, c'est pourquoi il s'agit d'un bouclier si efficace contre la fraude.

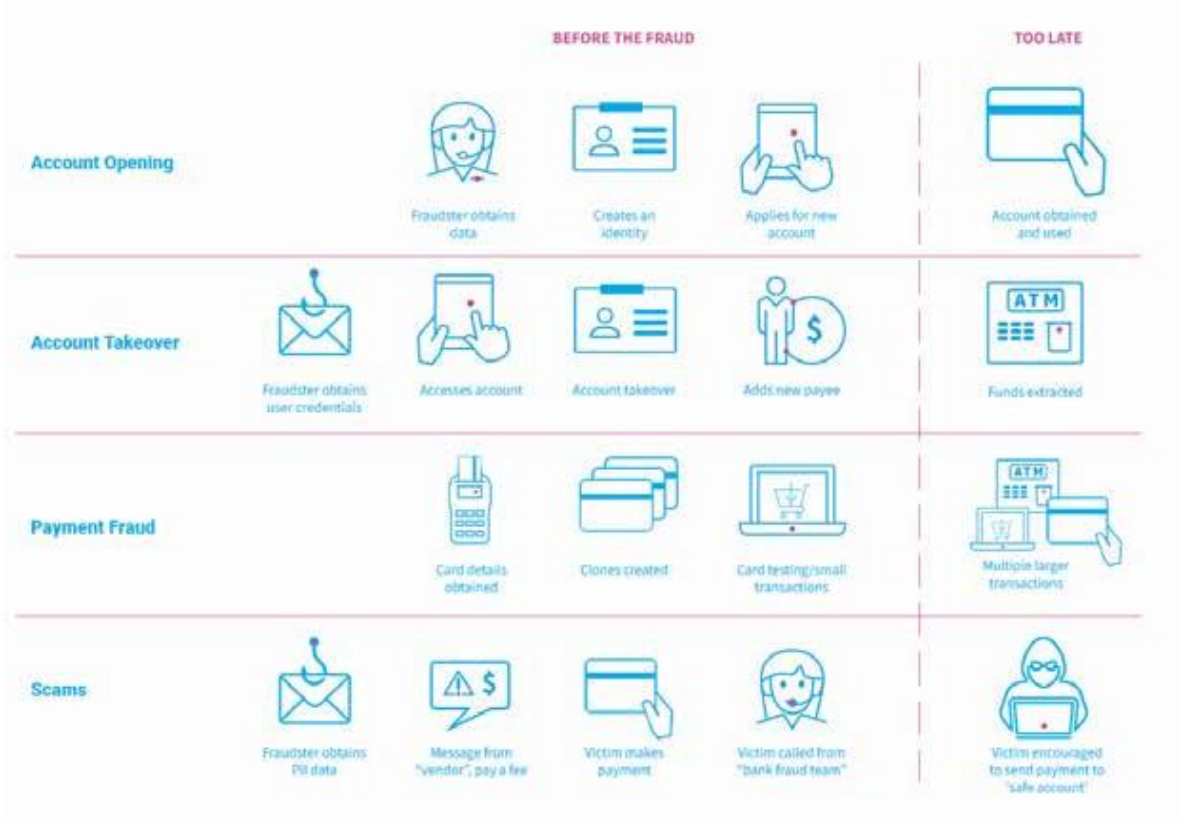
Bien que les escroqueries soient devenues une nuisance acceptée par la société, la technologie digitale a permis aux escrocs de commencer et de se développer rapidement, pour ensuite disparaître derrière des tampons technologiques. Les organisations peuvent modifier la dynamique du pouvoir en retournant les « empreintes digitales » numériques des criminels contre elles, en utilisant la biométrie comportementale pour prendre l'avantage.



Le pouvoir de la prévention

La ligne de démarcation est mince entre les endroits où la fraude peut être évitée et ceux où il est trop tard. Si l'on considère qu'environ 25 % seulement des pertes liées à la fraude sont récupérées, cette mince ligne équivaut à des millions, voire des milliards de dollars par organisation. Si vous pouvez faire bouger cette ligne d'une seule étape dans le processus, les résultats sont extraordinaires. Considérez quatre types de fraude courants : les nouveaux comptes, le piratage de compte, le paiement et les escroqueries. Chacune comporte plusieurs étapes avant qu'il ne soit trop tard, afin d'identifier et de prévenir la fraude.

Une plateforme de prévention de la fraude identifie et arrête les activités frauduleuses avant qu'il ne soit trop tard. Dans le cas de la fraude à l'ouverture de compte, l'identité et le comportement de l'utilisateur lorsqu'il remplit sa demande fourniront des points de données précieux pour évaluer la validité. Avec la prise de contrôle de compte, il peut y avoir des indicateurs pendant le point d'accès au compte en plus des signaux lorsqu'un nouveau bénéficiaire est ajouté ou que des informations sont modifiées. Une augmentation de l'activité, telle qu'une série de petites transactions, peut signaler une fraude potentielle au paiement, tandis qu'un comportement de paiement contextualisé avec les comportements des clients peut indiquer une escroquerie potentielle.



Le temps réel est essentiel

Le terme « temps réel » est utilisé de manière exhaustive de nos jours, en particulier dans le domaine de la technologie, et chacun a sa propre définition. Selon le dictionnaire Oxford, le temps réel signifie « relatif à un système dans lequel les données d'entrée sont traitées en quelques millisecondes, de sorte qu'elles sont disponibles pratiquement immédiatement sous forme de retour d'information ». Pour être clair, une milliseconde correspond à 1/1000 de seconde. Ainsi, les plateformes de données clients, les CDP qui prétendent à la capture de données « en temps réel » mais n'offrent qu'un chronométrage de 30 ou 60 secondes, ne fournissent pas de solution en temps réel. Pour rivaliser dans le jeu de la prévention de la fraude en temps réel, nous parlons de millisecondes.

Mettons cela en perspective :

- L'œil humain met 300 millisecondes à cligner des yeux
- Le temps de réaction humain moyen (le temps qu'il faut pour réagir à l'entrée) est de 250 millisecondes
- L'intervalle entre le glissement d'une carte et l'approbation de la transaction est mesuré en quelques secondes
- Il faut 7 millisecondes pour claquer des doigts

Lorsqu'il s'agit de prévention de la fraude, la rapidité est essentielle. Plus le parcours d'un acheteur est long, moins il a de chances de passer à la caisse. Lorsque vous recherchez des solutions de prévention de la fraude, n'oubliez pas de tenir compte à la fois de la capture et du traitement des données (le temps nécessaire pour les livrer à votre plateforme de prise de décision). Les données capturées en quelques millisecondes ne servent pas à grand-chose s'il faut 30 minutes pour fournir des informations exploitables à vos applications en aval.

L'expérience utilisateur en termes de faux positifs est tout aussi sensible au facteur temps. Plus vite vous pouvez différencier les utilisateurs légitimes des mauvais acteurs, plus vite vous pouvez permettre à la transaction de se poursuivre sans interrompre le parcours de l'acheteur. Et, bien sûr, l'objectif ultime est de battre le fraudeur AVANT qu'il ne soit en mesure de commettre la fraude, protégeant ainsi votre organisation et vos clients.

Celebrus FDP est la solution la plus avancée et la plus complète au monde qui capture en temps réel des données biométriques comportementales et des informations personnelles de première main tout au long du parcours client, et pas seulement sur la page de paiement.

La disponibilité instantanée de données contextualisées transforme la prévention des escroqueries et des fraudes financières telles que la création de nouveaux comptes, le piratage de comptes et la fraude aux paiements. La possibilité d'intervenir pour attraper le fraudeur avant qu'elle ne se produise offre une expérience client plus fluide, rationalise la gestion des ressources et réduit les dépenses liées à la fraude pour l'organisation.

Découvrez comment Celebrus FDP vous permet de battre les fraudeurs créatifs en passant de la détection des fraudes à la prévention.

CONNECTEZ-VOUS MAINTENANT