GUIDE

4 éléments essentiels

à la prévention moderne de la fraude

celebrus

Le temps presse pour prévenir la fraude en temps réel. Êtes-vous prêt ?

Ce qu'il faut retenir

- La fraude augmente considérablement et les entreprises doivent agir rapidement pour prévenir la fraude et fidéliser leurs clients
- Les données et la technologie sont essentielles pour identifier et prévenir la fraude en temps réel
- Les quatre éléments clés de la prévention moderne de la fraude

Le temps presse pour prévenir la fraude en temps réel. Êtes-vous prêt ?

À mesure que nous avançons dans le 21e siècle, le nombre d'ouvertures de comptes numériques augmente considérablement. En effet, selon Gartner, d'ici 2025, 75 % des ouvertures de nouveaux comptes se feront sur les canaux numériques.

Bien qu'il s'agisse d'une statistique impressionnante, elle signifie également une augmentation des possibilités pour les fraudeurs. La vitesse à laquelle la fraude se produit augmente à un rythme alarmant, et le nombre de fraudes augmente de façon encore plus spectaculaire. Les entreprises doivent se préparer au risque accru que la fraude fait peser sur leurs résultats – les organisations doivent agir rapidement pour prévenir tout dommage. Il ne suffit plus de simplement gérer la fraude, les organisations qui réussissent savent qu'il faut le faire préventivement en attrapant le fraudeur avant qu'il ne commette la fraude. Et cela nécessite des données et une activation en temps réel.

Pour agir en temps réel, vous allez devoir vous assurer que vous avez le plus d'informations possible avant que les activités frauduleuses n'aient lieu. Accumulez des preuves au fil du temps, évaluez les preuves sur le moment, prenez une décision et agissez... en quelques millisecondes.

En détectant les anomalies en temps réel et en analysant les données à grande échelle, les organisations peuvent reconnaître les écarts qui permettent de découvrir où et comment la fraude se produit.

C'est plus facile à dire qu'à faire, bien sûr. Il s'agit d'un équilibre délicat : vous ne voulez pas contrarier vos clients actuels en intervenant et en créant plus d'étapes dans le processus d'ouverture de compte. Mais des décisions mieux informées offrent une expérience client plus positive. C'est là que les données entrent en jeu. En analysant de grandes quantités de données en temps réel et en utilisant des technologies telles que l'IA et l'apprentissage automatique pour maximiser l'efficacité, les entreprises obtiennent une compréhension beaucoup plus riche de ce qui se passe sur leurs plates-formes et peuvent prendre des décisions plus intelligentes. C'est essentiel pour la prévention de la fraude, car les méthodes traditionnelles telles que les solutions de boîte noire et la collecte de données « ponctuelles » ne suffiront pas et ne vous donneront pas assez pour prendre une décision plus rapidement. Pour réussir à détecter et à prévenir la fraude, il faut activer des données d'identité et biométriques contextualisées en un instant.

La composition d'une solution moderne de prévention de la fraude

Il y a quatre éléments clés d'une solution moderne de prévention de la fraude qui doivent être intégrés à votre plateforme de données sur la fraude.

1. Graphe d'identité

Bien que la valeur de la prévention de la fraude soit indéniable, elle doit être mise en œuvre en mettant l'accent sur l'expérience client pour les utilisateurs légitimes. Il y a deux objectifs essentiels qui devraient guider tous les aspects de votre stratégie de lutte contre la fraude : connaître votre client et réduire les faux positifs. L'identité est la clé des deux.

Une cartographie complète de l'identité, alimentée par une capture approfondie des données et une biométrie comportementale, garantit un séquençage et une authentification précis des clients tout au long du parcours client. Dans le cadre de votre plateforme anti-fraude, un graphe d'identité vous permet de créer des structures d'identité complexes pour identifier et authentifier les utilisateurs, tout en mesurant les interactions entre les sessions et les plateformes. De nombreuses solutions n'ont pas la capacité d'identifier ou de rappeler le contexte de multiples interactions utilisateur sur les canaux et domaines numériques en raison des défis liés aux cookies et les restrictions du navigateur. Pour réussir à réduire les faux positifs et à fournir des opportunités de détection et d'intervention en temps réel de la fraude, il est essentiel de créer des profils robustes qui, en fin de compte, sont liés entre eux.
Cela vous permet de connecter des parcours anonymes à des parcours authentifiés au fil du temps, en fonction des clés d'identification Avec le modèle de données approprié lié à ces profils, vous aurez le plus d'éléments à portée de main pour prendre la meilleure décision sur le moment.

Il est important de noter que le terme « utilisateurs » ne fait pas seulement référence à ceux qui se connectent, mais à tous les parcours et interactions, qu'ils soient anonymes, connus ou authentifiés. Il y a de la valeur à chaque étape du parcours de l'utilisateur : la plupart des gens passent beaucoup de temps sur des appareils numériques, mais tout ne se passe pas dans un état authentifié. Pensez aux opérations bancaires – Vous pouvez naviguer sur le site Web de votre banque pour consulter les différentes options de prêt hypothécaire ou de prêt consommateur et les offres actuelles avant de vous connecter à votre compte. En termes de prévention de la fraude, la capture de ces informations contextuelles permet de développer des signaux basés sur ce qu'un consommateur fait bien avant qu'il ne soit authentifié. Si un visiteur recherche des options de prêt de manière anonyme, puis est ensuite connu ou authentifié, cela fournit des signaux à la plate-forme de données sur la fraude démontrant une utilisation légitime, ce qui accélère le processus d'authentification.
La clé est d'assembler ces signaux sur le canal et l'appareil dans le cadre du graphe d'identité.

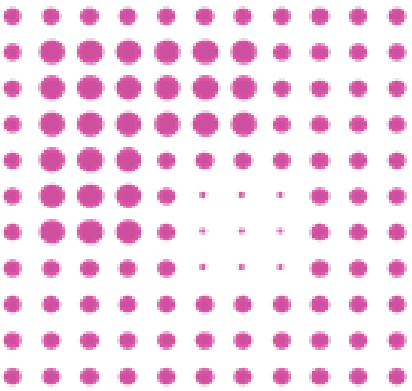
La capacité de conserver les identifiants au fil du temps sur chaque appareil numérique est essentielle pour augmenter les chances de se souvenir de l'identité de cette personne au moment où elle arrive sur un canal particulier. Cela nécessite une solution first party capable d'identifier et de conserver les profils d'une manière qui n'est pas affectée par la prévention intelligente du pistage (ITP) d'Apple, les récents changements des navigateurs et, en fin de compte, les différents degrés de législation sur la protection de la vie privée dans le monde.

La confiance et la propriété des données sont également essentielles, et les organisations doivent tenir compte de la capacité à capturer les informations personnelles de manière sécurisée, conforme et de première partie comme suit : les individus fournissent ces informations tout au long de leur parcours numérique. Les solutions de gestion de la fraude d'aujourd'hui sont principalement de nature tierce ou ne reçoivent que des identifiants hachés pour créer des profils et détecter les anomalies.
Ce n'est pas efficace, car les données d'identification personnelle jouent un rôle essentiel dans la détection des fraudes. L'ajout de données personnelles qui s'étendent au-delà d'un identifiant haché permet d'améliorer de 30 % l'identification des activités frauduleuses. Alors que les organisations continuent de lutter entre limiter les pertes dues à la fraude et réduire le nombre de faux positifs, une stratégie de gestion de la fraude sans informations personnelles laisse la porte ouverte à des failles dans votre stratégie.

Les entreprises ont besoin d'une meilleure solution pour vérifier l'identité en temps réel, tout en restant conformes.

Un graphe d'identité en temps réel permet d'identifier les visiteurs du canal en quelques millisecondes, ce qui garantit que les systèmes de prise de décision disposent des données nécessaires pour valider les transactions, quelle que soit l'authentification de l'utilisateur. Il ne suffit pas de se fier uniquement à ce qui se passe à un instant donné : les organisations doivent être capables d'agir sur la base d'un historique et d'un contexte complets, en conservant l'identité sur l'ensemble des canaux, domaines et appareils. Rien n'est plus dommageable pour l'expérience client que d'interrompre le parcours en signalant de faux positifs. Créer des récits d'identité complexes signifie utiliser des ensembles de données et d'identité complets pour évaluer les profils de risque des clients et vérifier l'identité.
Plus vous pouvez identifier avec précision les imposteurs, plus vite vous pouvez vérifier les visiteurs légitimes et les laisser poursuivre leur parcours sans interruption inutile.

Une compréhension précise de l'identité permet aux organisations de prendre des décisions commerciales cruciales en matière de prévention de la fraude. Par conséquent, un graphe d'identité intégré en temps réel est un élément essentiel de toute solution de prévention de la fraude.



2. Biométrie comportementale

Les entreprises peuvent identifier correctement les activités et les utilisateurs frauduleux sur la base de comportements, d'actions et d'informations personnelles connus en combinant la puissance d'une technologie et d'informations d'identité complètes de première partie avec l'ajout d'attributs et de signaux comportementaux.

Au-delà des méthodes d'identification des fraudes des solutions conventionnelles (c'est-à-dire l'appareil, l'emplacement, les échecs de connexion), la biométrie comportementale donne aux entreprises la possibilité de capturer et d'authentifier les utilisateurs en fonction de leur comportement numérique. Les modèles comportementaux, tels que la main prédominante, les pressions biométriques et les tendances de navigation, aident à légitimer les utilisateurs et à signaler les activités anormales afin que vous puissiez détecter la fraude tout au long du parcours client.

Par exemple, dans le cas d'une fraude par prise de contrôle à distance de compte, un fraudeur peut inciter un client à faire quelque chose sur son site de services bancaires en ligne, ce qui pourrait augmenter le temps passé sur des pages Web spécifiques. À l'aide d'une solution de lutte contre la fraude standard, cela pourrait signaler un événement inhabituel en fonction du temps moyen passé sur ces pages par tous les utilisateurs. Cependant, dans de nombreux cas, cette tendance est tout à fait normale, ce qui crée de nombreux de faux positifs, ce qui entraîne de graves frictions pour les clients et de la frustration pour les équipes chargées de l'expérience client.

La biométrie comportementale résout ce problème en créant un profil biométrique individuel pour chaque client. Pensez-y comme à la réponse aux questions «QQOQC» : Qui êtes vous ? Que faites-vous généralement en ligne ? Où êtes-vous situé ? Quelles sont vos habitudes ? Comment naviguez-vous sur le site ? Et ainsi de suite.

Le profil biométrique permet d'enregistrer de manière éthique ce qu'une personne fait normalement en ligne. Lorsqu'un fraudeur prend le contrôle du compte, ses comportements s'écartent du profil biométrique établi, ce qui envoie des signaux en temps réel à la banque indiquant que le compte est compromis. La banque peut alors intervenir et attraper le fraudeur avant que la fraude ne soit réalisée.

En reliant les structures de données et les plates-formes actuellement utilisées dans la pile technologique existante de votre organisation, vous pouvez exploiter les données pour créer des profils détaillés individuels de comportements légitimes et frauduleux connus, et les évaluer en temps réel.
La biométrie comportementale, comme la direction du balayage, la vitesse de frappe ou la pression d'appui, permet de créer des modèles de notation utilisant des données en temps réel pour détecter et prévenir les fraudes telles que l'ouverture de compte et prendre le relais pour attraper le fraudeur avant la fraude.

3. Détection d'anomalies

Les solutions traditionnelles de détection des fraudes se concentrent sur l'identification des comportements frauduleux, tandis que les technologies plus avancées se concentrent sur l'identification du client réel par rapport au fraudeur. Par exemple, un fraudeur peut facilement prendre connaissance de l'identifiant, du mot de passe, du numéro de compte, etc., d'un utilisateur, en se faisant passer pour un client légitime. Ceci est basé sur ce que le fraudeur sait.

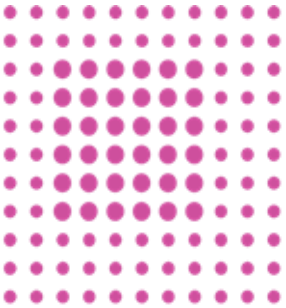
Cependant, les comportements de chaque utilisateur seront différents, et leur capture change la donne. Ces subtilités, propres à l'individu et à son interaction spécifique, peuvent être capturées, enregistrées et comparées pour identifier spécifiquement qui est le client, ou qui il n'est pas.

Par exemple, un utilisateur peut généralement effectuer des achats de commerce électronique le soir ou le week-end, tandis qu'un autre paie toutes ses factures le deuxième vendredi du mois. Un client peut faire preuve d'une familiarité numérique et utiliser systématiquement une application mobile avec une orientation horizontale de l'appareil et une dominance de la main droite, tandis qu'un autre utilise toujours un ordinateur de bureau et a des mouvements de souris irréguliers.

La détection avancée des anomalies et du timing des exécutions automatisent l'enregistrement et la mesure de ces points de données agrégés sur le comportement des clients sur tous les canaux numériques. Les anomalies de données susceptibles de signaler une fraude peuvent alors alerter l'entreprise et votre équipe de gestion de la fraude en temps réel sur la base des plages de variations et des résultats acceptables.

Une compréhension plus approfondie des clients basée sur les traits comportementaux et les analyses vous permet de reconnaître la fraude avant qu'elle ne se produise en mettant au jour des schémas de données cachés tels que les échecs de connexion, les attaques DDoS, la collecte de noms d'utilisateur ou de mots de passe, les échecs d'application et les attaques de bots.

Lorsqu'une organisation est en mesure d'identifier rapidement ses clients, elle réduit la probabilité de faux positifs. En surveillant les transactions en temps réel, à l'aide d'informations contextuelles issues de la biométrie comportementale, les entreprises peuvent immédiatement reconnaître les activités anormales et agir en conséquence.



4. Traçage des comptes et des identités compromis

Les données contextualisées en temps réel peuvent transformer la prévention des escroqueries et des fraudes financières telles que la création de nouveaux comptes, le piratage de comptes et la fraude aux paiements, en reconnaissant et en traçant les activités frauduleuses. Les comptes mules et les identités compromises sont une marque de fabrique de l'industrie de la fraude. Après tout, une fois qu'un fraudeur a votre argent, il doit le déplacer pour que vous ne puissiez pas le récupérer. Dans la plupart des cas, plusieurs comptes mules sont utilisés pour le rendre essentiellement irrécupérable.

Bien que la persistance de l'identité propriétaire soit essentielle pour identifier à la fois les clients légitimes et les fraudeurs, il s'agit également d'un outil précieux pour identifier et retracer les comptes mules. En tirant parti de profils d'identité complets, les entreprises peuvent suivre les identités compromises sur leurs comptes mules et suivre ces comptes muletiers pour découvrir d'autres identités compromises et de faux comptes. Une solution moderne de prévention de la fraude signalera également les comptes mules connus pour déclencher une alarme lors de leur prochaine utilisation.

Étant donné que la plupart des fraudeurs sont des récidivistes et qu'ils font souvent partie de grands réseaux, cela peut s'avérer inestimable pour prévenir la fraude de manière proactive. Lorsqu'une identité compromise et le compte mule qui lui est associé sont reconnus, il peut être avantageux de laisser le compte tranquille afin qu'il puisse être retracé jusqu'à d'autres fraudes afin d'éviter d'autres pertes liées à la fraude.

L'absorption d'une seule perte peut en valoir le coût si elle conduit à l'identification de plusieurs comptes mules ou d'un réseau entier qui peut être démantelé avant que d'autres dommages ne se produisent. Le suivi des activités frauduleuses des comptes mules au niveau individuel rationalise également la gestion des ressources et réduit les dépenses liées à la fraude pour l'organisation.

Rien qu'aux États-Unis, la fraude à l'identité a entraîné des pertes de 52 milliards de dollars en 2021, les consommateurs signalant des pertes de plus de 5,8 milliards de dollars, soit une augmentation de 70 % par rapport à l'année précédente. Une fois que ces pertes sont réalisées, moins de 25 % sont récupérés – c'est pourquoi la prévention est beaucoup plus efficace que la poursuite après coup.

L'identification et le traçage actifs des fraudeurs permettent aux organisations de réagir de manière stratégique aux activités à haut risque au moment de la tentative de fraude, voire avant, et non des heures ou des jours plus tard. Les entreprises à la pointe s'en rendent compte et peuvent protéger efficacement à la fois les clients et l'argent de l'entreprise tout en offrant une expérience client sans friction.

Les solutions de détection des fraudes ont parcouru un long chemin, mais elles s'appuient toujours sur des humains pour porter des jugements sur la base d'informations incomplètes et tardives. Avec la bonne plateforme de données et les bonnes informations, vous pouvez donner à votre équipe les moyens de prendre de meilleures décisions en matière de fraude, en temps réel.

Pour prévenir la fraude en temps réel, vous avez besoin d'une solution de lutte contre la fraude à multiples facettes qui permette de recueillir autant d'informations que possible avant que la fraude ne se produise. Plus vos décisions sont éclairées, moins il y a de frictions pour vos clients. C'est là qu'intervient une solution moderne de prévention de la fraude : elle doit inclure un graphe d'identité, la biométrie comportementale, la détection des anomalies, et le traçage des comptes pour créer des graphes d'identité complets et détecter les irrégularités en temps réel. L'utilisation d'une plateforme de données sur la fraude dotée de ces fonctionnalités vous permet de prendre des décisions qui offrent une expérience client positive sans mettre en péril la sécurité. Alors, qu'attendez-vous ? Arrêtez d'utiliser des solutions universelles et donnez à vos clients le meilleur des deux mondes : sécurité et commodité.

Le temps presse, il est temps de passer de la gestion de la fraude à la prévention de la fraude.

À propos de Celebrus FDP

Les méthodes traditionnelles de détection et de prévention de la fraude ne suffisent pas à protéger contre les tentatives de fraude en constante évolution, qui deviennent de plus en plus sophistiquées chaque jour. Mais les entreprises sont également soumises à une pression croissante pour répondre aux demandes des consommateurs en matière d'expérience client transparente.

Celebrus FDP permet aux grandes entreprises d'améliorer l'expérience client grâce à une authentification sans friction, invisible et continue tout en prévenant la fraude en temps réel, en identifiant les fraudeurs par leurs comportements uniques.

S'appuyant sur des données comportementales riches en temps réel pour vraiment prévenir la fraude, Celebrus FDP offre une prévention de la fraude et des escroqueries sur tous les points de contact numériques avec des informations comportementales entièrement automatisées et une intégration fluide avec les outils de gestion de la fraude existants. Une détection plus précise des fraudes réduit considérablement les faux positifs et traite rapidement les nouvelles menaces, de la fraude aux paiements au piratage de compte, en passant par l'ouverture de nouveaux comptes et les escroqueries.

Le graphe d'identité Celebrus permet d'identifier les visiteurs du canal en temps réel, en quelques millisecondes, afin d'obtenir une vue complète de chaque visiteur afin que les systèmes de prise de décision disposent des informations nécessaires pour valider les transactions et les utilisateurs, quelle que soit l'authentification. La biométrie comportementale détecte les comportements atypiques, ce qui vous permet de prévenir l'escroquerie avant qu'elle ne se produise, et l'IA réduit les pertes et les faux positifs.

« Tout collecter » signifie que les bonnes données et informations sont toujours disponibles pour prendre de meilleures décisions en matière de fraude. L'activation de données d'identité et biométriques contextualisées fournit des analyses instantanées pour détecter la fraude et alimenter les systèmes de décision et de gestion de la fraude.

Arrêtez de mettre en péril l'expérience client avec une solution unique et limitée et commencez à prévenir la fraude avant qu'elle ne se produise.

CONNECTEZ-VOUS MAINTENANT

Biométrie

IA et analytique

Prévention de la fraude en temps réel