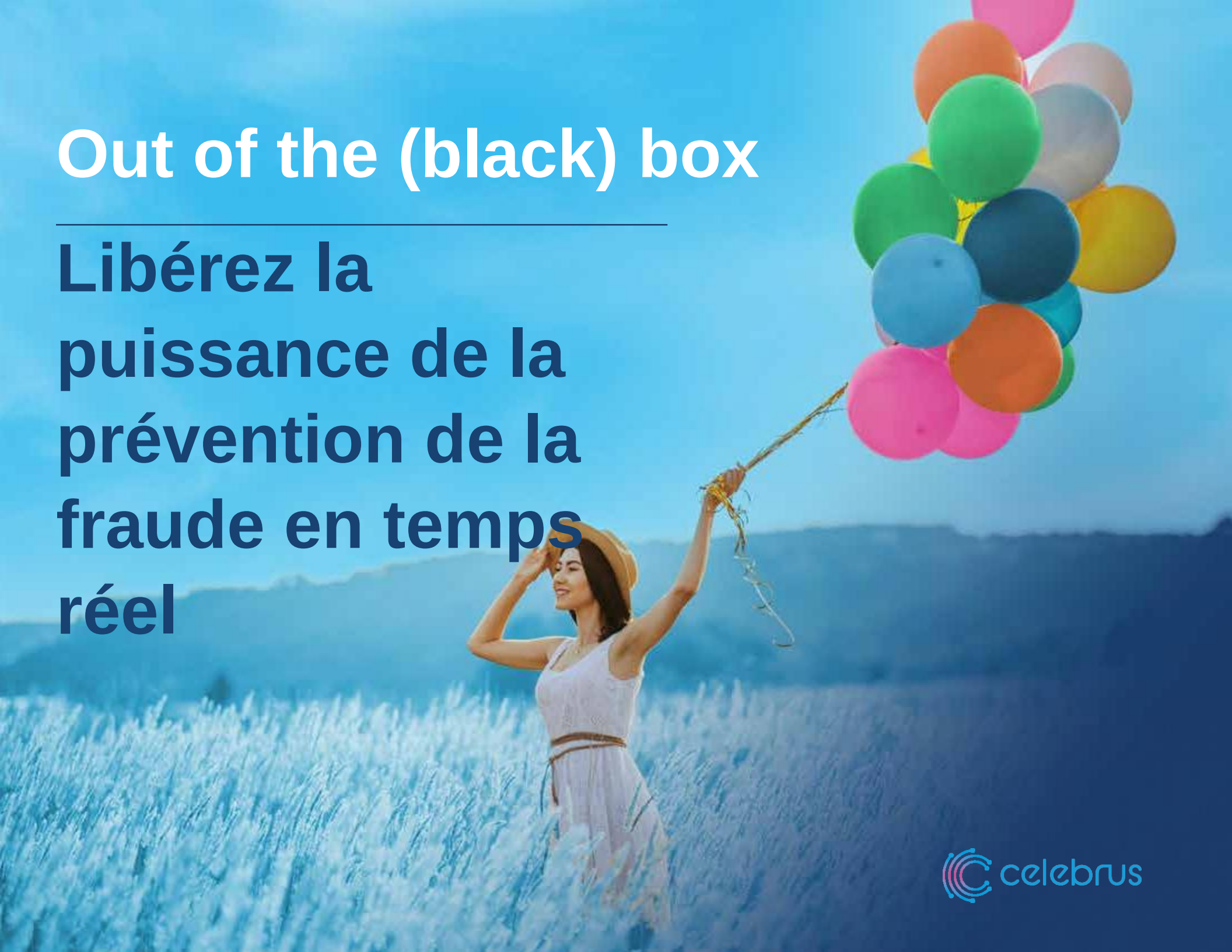
Out of the (black) box

Libérez la puissance de la prévention de la fraude en temps réel



celebrus

Libérez la puissance de la prévention des fraudes en temps réel avec une solution de fraude intégrée

La plupart des solutions de lutte contre la fraude ne s'adressent qu'à un seul type de fraude, voire deux. La raison en est simple : c'est plus facile. Mais facile ne veut pas dire meilleur. Bien qu'il existe différentes approches pour les différents types de fraude, il y a aussi beaucoup de points communs.

De plus, ces solutions de lutte contre la fraude à usage unique vivent dans une « boîte noire », ce qui signifie qu'elles sont complètement séparées et distinctes de l'organisation, les unes des autres, et qu'elles ne transmettent pas (en fait, NE PEUVENT PAS) les données dans les deux sens. Nous y reviendrons plus tard, mais examinons d'abord les types de fraude les plus courantes qui causent de gros soucis aux professionnels de la fraude aujourd'hui.

Contenu :

Les quatre principaux types de fraude auxquels les banques doivent s'attaquer

Bien qu'il existe autant de variantes de fraude qu'il y a de fraudeurs, les attaques peuvent être regroupés en quatre grands types. Comprendre les mécanismes qui les sous-tendent est la première étape d'une stratégie proactive de prévention de la fraude.

Escroqueries – lorsqu'un fraudeur utilise un stratagème ciblant directement des personnes ou des groupes et les convainc (c'est-à-dire les trompe) d'effectuer un paiement ou de transférer de l'argent.

Alors que d'autres types de fraude peuvent être moins interventionnistes et s'appuyer sur la technologie, les escroqueries impliquent généralement une forte implication personnelle des deux côtés. Et les escroqueries font partie de tous les autres types de fraude – une escroquerie permet souvent de collecter ou d'enrichier les informations nécessaires pour créer une fausse identité, prendre le contrôle d'un compte ou blanchir les fonds volés après l'exécution de la fraude. Les exemples courants incluent les escroqueries par usurpation d'identité, les escroqueries sentimentales, les escroqueries à l'investissement et les escroqueries aux mules.

Les escroqueries sont le type de fraude le plus difficile à combattre en raison du facteur humain - le propriétaire du compte envoie légitimement son argent à quelqu'un qui l'a trompé pour qu'il le fasse. Lorsqu'une victime fournit involontairement ses renseignements à un fraudeur, effectue un paiement sur un faux compte ou transfère des fonds à partir d'un compte légitime, ce n'est pas aussi évident qu'une fausse demande ou une transaction suspecte. Par conséquent, les solutions de lutte contre la fraude visant à identifier les escroqueries utilisent généralement l'analyse comportementale, y compris la biométrie, pour détecter les comportements susceptibles de signaler une situation d'escroquerie potentielle ou un client agissant hors de l'ordinaire.

Fraude Piratage de compte – lorsqu'une une personne non autorisée prend le contrôle d'un compte existant.

En règle générale, les fraudeurs volent les identités et les informations d'identification des comptes des consommateurs, telles que le nom d'utilisateur et les mots de passe, qu'ils utilisent pour accéder au compte et voler des fonds. Les informations peuvent être collectées en achetant sur le dark web, en exploitant les médias sociaux et par le biais d'escroqueries en contactant directement le propriétaire du compte. Le fraudeur tentera souvent de modifier les informations du compte, le mot de passe et les notifications afin que le propriétaire réel ne soit pas au courant des activités malveillantes de son compte.

Une solution de lutte contre la fraude visant à identifier le piratage de compte recherchera des activités telles que plusieurs demandes de réinitialisation de mot de passe ou les tentatives de connexion infructueuses, les modifications d'informations clés telles que l'adresse e-mail ou le numéro de téléphone, et les comportements liés à la fraude tels que les mouvements erratiques de la souris.

Fraude au paiement – lorsqu'un fraudeur vole les informations de paiement d'une personne ou ouvre un faux compte pour effectuer un achat sans avoir l'intention de le payer.

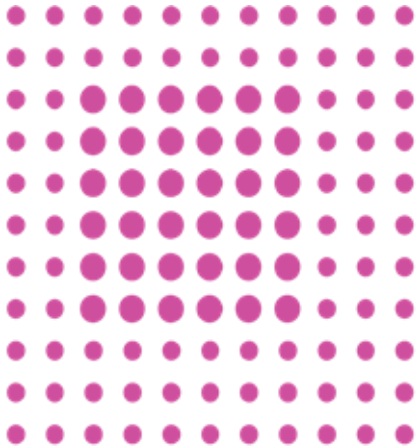
En général, il s'agit de toute transaction fausse ou illégale effectuée par un criminel. Il s'agit notamment de la fraude BNPL (Buy Now Pay Later) dont la réputation ne cesse de croître et qui est de plus en plus difficile à détecter. La fraude au paiement peut également se produire lorsqu'un client légitime demande un faux remboursement en contestant un prix ou en prétendant que le produit n'a pas été reçu, alors qu'en fait, il l'a été.

Une solution de fraude aux paiements recherchera des signes d'usurpation d'identité, de multiples transactions suspectes, de changement d'adresse de livraison, d'anomalies d'utilisation, etc., mais elle se concentre généralement sur la surveillance des transactions. La notation basée sur le risque et l'authentification/vérification font également souvent partie des solutions de fraude aux paiements.

Fraude liée à une demande – Lorsqu'un fraudeur utilise une pièce d'identité volée ou fausse pour demander un prêt ou une ligne de crédit sans avoir l'intention de rembourser le prêteur.

Ce type de fraude comprend également les clients légitimes qui falsifient les informations de leur demande. Il peut également s'agir d'une fraude à la demande d'assurance, lorsqu'une personne falsifie ses informations ou crée une fausse identité pour obtenir une assurance ou ajouter un bénéficiaire de perte pour une future escroquerie à l'assurance.

Une solution de lutte contre la fraude visant à identifier les fraudes aux demandes consiste littéralement à analyser les informations contenues dans une demande et à rechercher les signaux d'alerte. L'analyse comportementale peut compléter en identifiant les comportements frauduleux tels que le copier-coller, tandis que la résolution d'identité peut découvrir plusieurs demandes utilisant le même nom, la même adresse e-mail ou une adresse similaire.



Pourquoi les systèmes de lutte contre la fraude en boîte noire ne suffisent pas

Comme nous l'avons mentionné, la fraude, sous toutes ses formes, ne vit pas dans un silo ou une boîte noire. Différents types de fraude déploient plusieurs méthodes qui fonctionnent ensemble pour exécuter la fraude la plus importante. Les escroqueries sont un parfait exemple du croisement entre les types de fraude, car elles sont régulièrement utilisées pour recueillir des informations qui permettent le piratage de comptes, le vol d'identité, la création de fausses identités et la fraude au paiement push autorisé (APP), y compris les fraude liées à une mule.

Par exemple, dans le cadre d'une fraude à la prise de contrôle d'un compte, les fraudeurs exécutent souvent une escroquerie pour collecter un numéro de compte, remplir des informations manquantes telles que des questions de sécurité ou contourner les contrôles de sécurité en demandant à la victime de fournir son mot de passe ou son code de vérification pour terminer la prise de contrôle du compte. Ils peuvent ensuite transférer des fonds du compte piraté vers un compte frauduleux créé par le biais d'une demande frauduleuse. Ensuite, ils utilisent une mule pour effectuer ce transfert.

De même, la fraude à la demande peut utiliser des escroqueries pour collecter des informations afin de créer une fausse identité qui est utilisée pour créer de nouveaux comptes, crédit ou des polices d'assurance. En parlant d'assurance, les escroqueries sont souvent la dernière étape de la fraude à l'assurance – la mise en place d'un faux scénario (ou d'un faux bénéficiaire) pour obtenir un paiement.

En fait, il est très peu probable, voire impossible, qu'un type de fraude soit complètement autonome. Le succès de la fraude dépend de la combinaison d'un grand nombre de ces approches. C'est exactement la raison pour laquelle votre solution de lutte contre la fraude doit faire de même.

L'autre problème flagrant de la plupart des solutions de lutte contre la fraude est qu'elles sont des boîtes noires parce qu'elles sont externes. Lorsqu'il s'agit de banques et d'institutions financières, il y a tellement d'exposition au risque qu'elles doivent crypter massivement les informations de la banque et ne peuvent pas transférer d'informations personnelles identifiables. La quantité de cryptage et d'étapes supplémentaires qui seraient nécessaires pour renvoyer ensuite toutes ces informations à la banque est irréaliste.
Au lieu de cela, ils opèrent dans un environnement de boîte noire, ce qui signifie que la banque n'obtient jamais les données réelles - tout ce qu'elle obtient, c'est un score sans contexte, sans explicabilité et sans informations partageables. Et comme la sécurité l'emporte sur la rapidité, il est impossible pour les systèmes tiers de lutte contre la fraude d'obtenir des données en temps réel pour prévenir activement la fraude. Enfin, cette méthode de notation simpliste crée beaucoup de faux positifs en raison du manque de contexte, sans que l'on sache pourquoi. Ce n'est pas une bonne expérience pour les clients légitimes.

Le résultat de cette approche à service unique est que chaque banque dispose de plusieurs systèmes de lutte contre la fraude, fonctionnant dans plusieurs départements, traitant plusieurs types de fraude – complètement INDÉPENDANTS les uns des autres. Non seulement c'est coûteux et inefficace, mais cela empêche l'organisation de créer des profils d'identité complets qui rassemblent les données d'activité, les données comportementales et les données contextuelles pour obtenir une vue à 360 degrés du client afin de prévenir la fraude en temps réel. Ils ne peuvent pas voir que l'utilisateur123 a parcouru quatre de leurs sous-domaines et a soumis une demande de carte de crédit sur chacun d'eux, avec des informations légèrement différentes, mais la même adresse IP et la même biométrie comportementale.
Ils ne peuvent pas dire qu'un client légitime est connecté à leur application bancaire sur son ordinateur de bureau en même temps qu'il est dans l'application mobile et l'un d'entre eux peut être sous l'influence d'un fraudeur. Ils peuvent seulement voir qu'un client légitime effectue un paiement sur un nouveau compte qu'il vient d'ajouter. Et comme le système de fraude au paiement est déconnecté du système de fraude à l'ouverture, ils n'ont aucune idée que le compte qui a été vient d'être ajouté est le même que celui qui vient d'être signalé par l'application de fraude des demandes.

Comment lutter contre tous les types de fraude grâce à une solution de lutte contre la fraude sur une plateforme « first party ».

Pour lutter efficacement contre la fraude, et plus particulièrement pour la prévenir, les institutions financières ont besoin d'une solution complète qui détecte tous les types de fraude en temps réel et construit des graphes d'identité complets qui augmentent leur capacité à prévenir tous les types de fraude.
La capture et la consolidation des données sur l'ensemble des sessions, des appareils, des domaines et au fil du temps multiplient la puissance d'une solution de lutte contre la fraude intégrée et réduisent les faux positifs.

À l'aide d'une solution « first party » de lutte contre la fraude, toutes les données sont capturées et stockées en interne, protégées par les protocoles de sécurité robustes de l'organisation, afin que les banques puissent activer toutes leurs données pour les utiliser dans l'ensemble de l'organisation, pour chaque cas de fraude. Elles peuvent également créer leurs propres modèles de détection de fraude et garantir la confidentialité et la conformité réglementaire. Il peut même être utilisé pour améliorer les systèmes existants de gestion de la fraude et fournir des décisions en temps réel pour prévenir efficacement la fraude.

Chaque banque dispose d'une équipe de lutte contre la fraude, dont les data scientists élaborent des modèles de détection de fraude. Chacune de ces équipes utilise une pléthore de technologies différentes telles que FICO, SAS, Quantexa, BAE et d'autres - et chacune a ses propres modèles (fraude prise de contrôle, demande frauduleuse, escroqueries, fraude au paiement). Chacun de ces modèles peut bénéficier de meilleures données.

De meilleures données signifient de meilleurs résultats. En connectant une vue complète du client à tous les points de données dans un environnement protégé, ces solutions peuvent maximiser l'efficacité de technologies telles que la biométrie comportementale, l'apprentissage automatique (Machine Learning) et l'analyse des liens pour non seulement détecter et prévenir la fraude en temps réel, mais aussi pour identifier les comptes mules connus et les retracer vers d'autres comptes et profils connectés.

Une véritable solution intégrée est la référence en matière de lutte contre tous les types de fraude et de résolution des défis posés par les systèmes traditionnels de lutte contre la fraude en boîte noire afin de prévenir activement la fraude en temps réel, dans l'ensemble de l'organisation.

Connectez-vous maintenant et réservez une démo

Atteindre l'excellence

Celebrus FDP est une solution de lutte contre la fraude sur plateforme interne à l'organisation qui résout tous les types de fraude en temps réel. Grâce à la capture connectée et conforme de données, les entreprises peuvent regrouper les utilisateurs sur tous les canaux, toutes les sessions, tous les appareils et toutes les périodes pour obtenir une vue complète des identités qui peut être utilisée dans toute l'organisation, et dire adieu aux silos pour toujours. Faire tout cela en quelques millisecondes permet de prendre des décisions instantanées pour intervenir. L'impact de cette situation sur la valeur est énorme : au lieu de regarder en arrière pour voir ce qui s'est passé (comme la plupart des solutions de lutte contre la fraude), l'organisation peut voir ce qui se passe MAINTENANT, dans l'instant. Lorsque vous prévenez les pertes en premier lieu, vous n'avez pas besoin de passer du temps à les récupérer. Vos clients et votre organisation sont protégés.

Le niveau de données produites par Celebrus est inégalé dans l'industrie. Parce que Celebrus FDP est propriétaire, réside au sein de votre organisation, vous avez accès aux données réelles et pouvez les charger dans n'importe quel système de votre choix, en parallèle. Il complète vos autres solutions de lutte contre la fraude, afin qu'elles puissent fonctionner de manière optimale. Les données sont capturées de manière transparente et peuvent non seulement être introduites dans vos systèmes de gestion de la fraude et vos modèles de données existants, mais elles peuvent également recevoir des données d'autres systèmes pour les contextualiser et les renvoyer, formant ainsi une synchronisation bidirectionnelle précieuse des informations.

Étant donné que Celebrus FDP est intégré directement dans les sites Web et les applications mobiles de votre organisation, il offre également la possibilité d'intervenir en temps réel, c'est-à-dire en affichant un avertissement contextuel pour un compte mule suspect ou en prenant le contrôle de toute la session pour empêcher activement l'exécution de la fraude.

Exemple : un client est sur son téléphone exactement au moment où il est connecté à son compte bancaire. Il s'agit d'un comportement atypique, mais la plupart des solutions de lutte contre la fraude ne sont pas en mesure d'identifier ces signaux, car elles ne peuvent pas conserver l'identité sur tous les canaux. Et bien qu'il puisse s'agir d'un événement parfaitement légitime, cela peut également indiquer une escroquerie où le fraudeur est au téléphone pour convaincre le client de fournir ses informations de connexion, d'effectuer une vérification ou de transférer des fonds sur un compte sous le contrôle du fraudeur.

Celebrus CDP peut capturer ces données complètes simultanément et les faire correspondre au profil d'identité, tout en les comparant à des comptes mules connus ou à des comportements frauduleux, et en déclenchant instantanément des signaux de risque élevé. Il peut également pousser une intervention, telle que la mise en attente du transfert et l'envoi d'un message dans l'application conseillant au client de contacter directement sa banque.

> **Pour vaincre la fraude et la prévenir en temps réel, il faut cesser de regarder en arrière ce qui s'est passé et être en mesure de voir exactement ce qui se passe MAINTENANT, en temps réel.**

Découvrez Celebrus FDP

Celebrus FDP est la solution de lutte contre la fraude sur plateforme « first party » la plus avancée et la plus complète au monde, qui capture en temps réel les données biométriques comportementales et les informations personnelles tout au long du parcours client, et pas seulement sur la page de paiement.

La disponibilité instantanée de données contextualisées transforme radicalement la détection et 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'il ne commette une fraude 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 prévenir tous les types de fraude en temps réel.

CONNECTEZ-VOUS