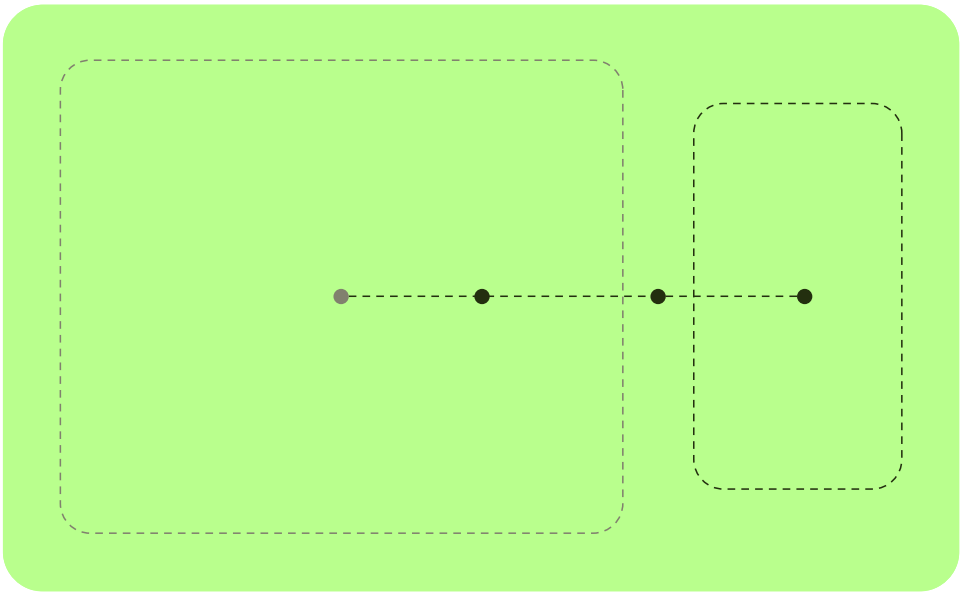
feedzai



Identifier l’ATO avant que l’argent ne soit volé

Plus d’1 milliard de clients dans le monde nous font confiance pour éviter plus d’1 milliard de dollars de pertes chaque année

مصرف الراجحي alrajhi bank · jack henry · stet · zeller

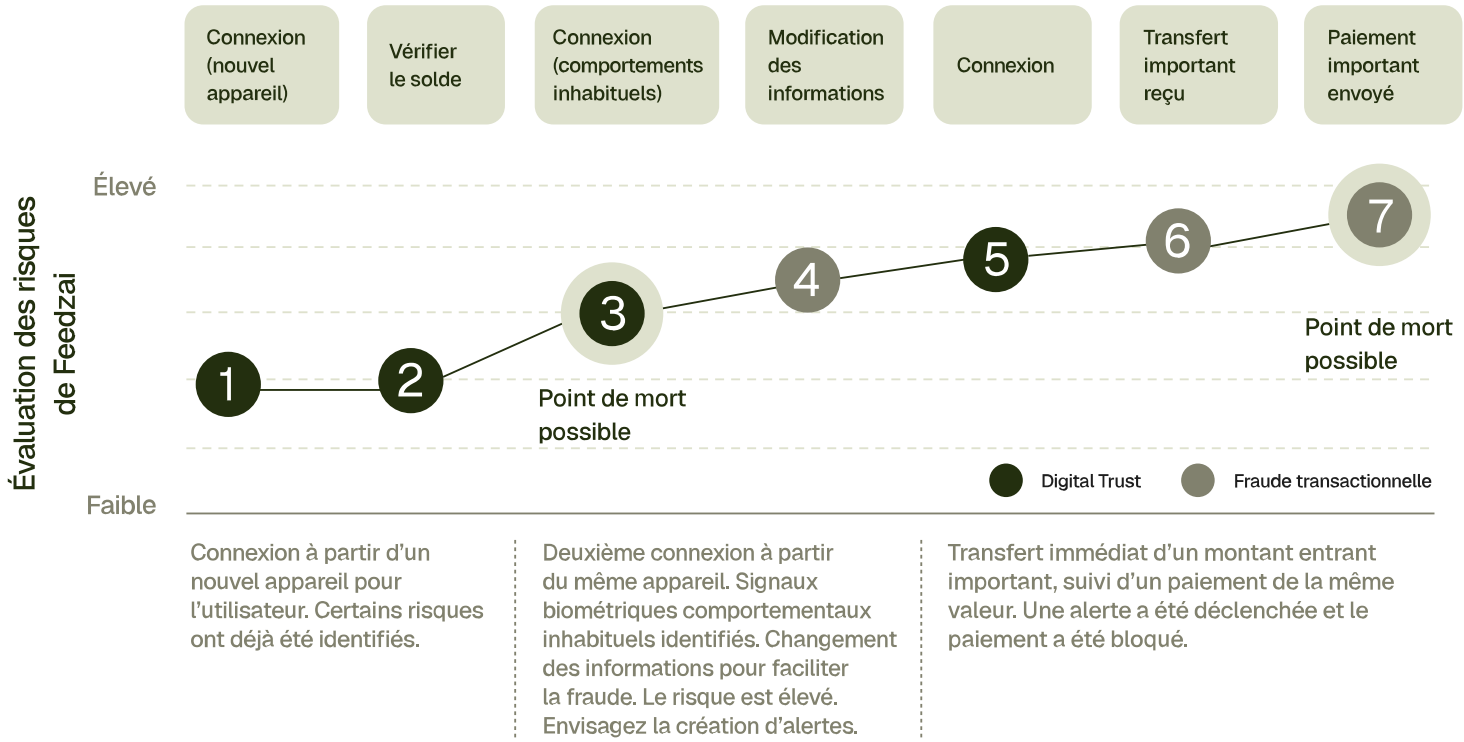
La prise de contrôle de compte (ATO) est rarement un événement unique. Cela commence souvent tranquillement, avec une information d’identification volée, un appareil qui ne convient pas tout à fait, ou une connexion qui semble légitime d’elle-même, mais suspecte dans son contexte. Lorsque la fraude devient visible, le compte est déjà compromis et l’argent est déjà en mouvement.

Le véritable défi est que les signaux sont généralement fragmentés. L’utilisation de l’appareil lors de la connexion, les signaux comportementaux pendant les mises à jour du compte et les informations sur l’activité de paiement sont souvent surveillés séparément, ce qui rend difficile de relier de la manière la plus efficace les signaux d’alerte à la tentative de monétisation éventuelle. Cette séparation crée des angles morts, entraînant des résultats de performance sous-optimaux.

Pour arrêter efficacement la fraude par prise de contrôle de compte, les institutions ont besoin de renseignements connectés en temps réel qui relient l’identité, l’appareil, le comportement et les modèles de paiement sur l’ensemble du parcours client. Ce n’est qu’à ce moment-là que l’accès suspect peut être identifié précocement, que les comptes compromis peuvent être mis à l’épreuve plus tôt et que les transferts illicites peuvent être interrompus avant que l’argent ne quitte le compte.

L’approche connectée de Feedzai identifie l’ATO plus tôt

Les signes de fraude par ATO apparaissent souvent tôt, soit par des sessions de reconnaissance, soit par des événements qui permettent l’accès, comme la réinitialisation des mots de passe. Les meilleures stratégies utilisent ces événements contextuels pour bloquer la fraude plus tôt, en prenant directement des décisions sur ces événements ou en utilisant les renseignements en aval lorsqu’un événement à plus haut risque (par exemple, un paiement) a lieu. L’intelligence connectée est essentielle pour garantir que la valeur de vos données s’accumule avant tout transfert d’argent.



Connexion à partir d'un nouvel appareil pour l'utilisateur. Certains risques ont déjà été identifiés.

Deuxième connexion à partir du même appareil. Signaux biométriques comportementaux inhabituels identifiés. Changement des informations pour faciliter la fraude. Le risque est élevé. Envisagez la création d'alertes.

Transfert immédiat d'un montant entrant important, suivi d'un paiement de la même valeur. Une alerte a été déclenchée et le paiement a été bloqué.

Principaux avantages de l'approche Feedzai

Optimiser l'utilisation des données non monétaires
Tirez parti de l'analyse comportementale, de l'empreinte digitale des terminaux et de la Network intelligence sur des événements non monétaires (p. ex., connexions) afin de créer des opportunités d'intervention précoce ou d'utiliser l'intelligence en aval pour améliorer les décisions de paiement.

Gardez une longueur d'avance sur l'évolution de la fraude
Reconfigurez les contrôles rapidement, lancez de nouvelles règles avec souplesse et reformez continuellement les modèles afin que votre stratégie de fraude reste actuelle, réactive et garde une longueur d'avance sur l'évolution des menaces.

Arrêter le flux de fonds illicites
Surveillez les paiements entrants et sortants à l'aide de l'analyse des transactions, des ratios et des vitesses pour intercepter les flux illicites. Évaluez les fraudes historiques et les normes des clients pour découvrir des comportements anormaux. Intervenez lorsque des fonds suspects arrivent ou bloquez les transferts avant qu'ils ne sortent.

Renforcez vos décisions grâce à la Network Intelligence
L'intelligence réseau de Feedzai exploite les informations provenant de plus **90 milliards d'événements** dans l'ensemble du domaine de données de Feedzai pour renforcer les décisions en matière de risques, sans partager de données PII. Il enrichit chaque interaction avec des modèles issus de la base de clients mondiale de Feedzai, permettant une détection plus précoce des tactiques ATO émergentes et améliorant les performances globales de détection.

Cas client

Problème
Raiffeisen Bank International (RBI), une grande banque européenne comptant 12 banques filiales, souhaitait renforcer la détection d'ATO à mesure que les activités bancaires et de paiement numériques augmentaient. La banque devait aller au-delà des seules données de paiement et ajouter des signaux comportementaux et liés aux appareils pour mieux détecter la fraude tout en maintenant une expérience client fluide et simple.

Solution
RBI a mis en œuvre la solution Digital Trust de Feedzai pour enrichir les données de transaction avec des données biométriques comportementales, des signaux liés aux appareils et des informations réseau pour les canaux Web et mobiles. L'approche combinait les informations de session numérique avec les événements de paiement afin que RBI puisse mieux comprendre l'intégralité du parcours client, en commençant par la connexion plutôt qu'au seul terme du flux de transaction. Le déploiement a permis à la banque de capturer en permanence les données comportementales et relatives aux appareils tout au long de la session, renforçant ainsi la décision finale concernant les risques.

Résultat :

Amélioration de 37 % des taux de détection de la fraude

Enrichissement en temps réel des événements de paiement

Une approche de prévention de la fraude plus holistique

« À ce moment-là, nous avons décidé que nous devions étendre l'intervention à la fin du parcours client au début de ce parcours, dès la connexion. »

Responsable produit de la surveillance des transactions frauduleuses du groupe RBI



Solutions connectées de Feedzai pour empêcher la prise de contrôle de compte

Digital Trust
Validez l'identité et l'intention en temps réel grâce à la Behavioral biometrics, à la Network intelligence et à l'intelligence des menaces. L'IA de Feedzai apprend continuellement du comportement des utilisateurs et des signaux contextuels pour détecter les accès suspects, les modèles inhabituels et les techniques d'attaque émergentes tout au long de l'intégration, de la connexion, des mises à jour de compte et de l'ensemble de la session.

Fraude transactionnelle
Utilisez l'historique utilisateur, les métriques en temps réel et les données de paiement entrant/sortant pour surveiller les tentatives de paiement une fois que le compte est compromis. L'IA de Feedzai crée des **profils Segment-of-One** pour chaque utilisateur, en analysant les modèles de transaction pour détecter les écarts subtils que les règles ou les segments statiques manquent. Cela permet une détection précise des intentions de paiement anormales, en réduisant les faux positifs tout en bloquant les transferts suspects et en stoppant la fraude au point de paiement.

Feedzai IQ Score
Affinez le score final de risque en tirant parti des informations issues de la Network Intelligence de Feedzai, fondées sur des signaux de plus de 140 milliards d'événements traités par an. L'IA de Feedzai transforme cette ampleur en une prise de décision plus solide, aidant les clients à reconnaître plus tôt les nouveaux schémas de fraude et à améliorer la détection dans l'ensemble de l'écosystème.

Profilage des paiements entrants
Détectez les prises de contrôle de compte en surveillant les transactions entrantes afin de repérer des schémas suspects (par ex., des dépôts de grande valeur suivis de sorties rapides), permettant aux banques d'identifier et d'arrêter rapidement les activités frauduleuses.

Reconnu par IDC datos INSIGHTS Celent. Chartis

Stoppez l'usurpation de compte en temps réel.

Demander une démo

sales@feedzai.com
info@feedzai.com
feedzai.com

