feedzai

Analyse des transactions entrantes en temps réel : Amélioration de la détection de la fraude et comptes mules

Royaume-Uni

Table des matières

« Il est prudent de ne jamais accorder une confiance totale à ce qui nous a trompés une fois. »

- René Descartes

La crise liée la fraude : Les banques ont besoin de nouveaux outils pour faire face à un paysage en mutation

Rien qu'en 2023, les banques britanniques ont vu les criminels s'emparer d'un montant estimé à 1,168 milliard de livres sterling via des fraudes autorisées et non autorisées, soit à peine une baisse par rapport à l'année précédente (1,2 milliard de livres sterling). Ces chiffres ahurissants de UK Finance soulignent une dure réalité : malgré les efforts du secteur, la fraude reste une menace florissante, qui mine la confiance et la stabilité financière. La mise en œuvre d'une réglementation exigeant un partage des responsabilités à parts égales dans le remboursement des victimes d'escroquerie d'ici à 2024 est un appel clair aux banques pour qu'elles révisent leurs systèmes actuels de détection des fraudes. Mais par où commencer ?

Pertes liées à la fraude sur les paiements au Royaume-Uni

	2023	2022	2021
Pertes liées à la fraude	1,168 livres	1,2 livres	1,29 livres
Fraudes signalées	2,9 millions	2,9 millions	3 millions

Par la surveillance des paiements entrants.

Cet ebook est votre carte de navigation à travers les complexités de la surveillance des paiements entrants – une stratégie de pointe et proactive prête à transformer la façon dont les banques détectent, préviennent et gèrent la fraude. Au-delà de la simple explication du « quoi » et du « pourquoi », nous fournissons un guide concret du « comment faire » pour intégrer cette approche sophistiquée dans vos systèmes existants. De la compréhension de l'infrastructure technologique nécessaire à la dotation en personnel et à la formation, en passant par la conformité réglementaire, nous vous accompagnons à chaque étape critique vers un avenir résistant à la fraude.

Forte de ces connaissances, votre banque pourra non seulement répondre aux exigences réglementaires à venir, mais aussi ouvrir la voie à une nouvelle norme en matière de confiance des clients et de sécurité des transactions.

Le nouveau paysage réglementaire

La réglementation britannique incite les banques à prendre des mesures proactives pour prévenir les fraudes et les pertes dues aux escroqueries au lieu d'avoir une attitude réactive face à ces dernières. Ces changements réglementaires sont les suivants :

Remboursement obligatoire de la responsabilité à parts égales

À partir d'octobre 2024, la réglementation britannique sur les services de paiement (PSR) exigera des banques britanniques qu'elles remboursent les victimes d'escroqueries par paiements autorisés par escroquerie aux paiements par ingénierie sociale (APP) dans la quasi-totalité des cas. La responsabilité des pertes liées aux escroqueries sera répartie équitablement (à parts égales) entre les banques expéditrices et les banques réceptrices.

Il s'agit d'un changement important par rapport à l'époque où seules les banques expéditrices étaient tenues de couvrir les remboursements. Les banques réceptrices sont désormais également responsables de la détection, de l'arrêt et de la restitution des fonds liés à des pertes dues à des escroqueries. En vertu de cette réglementation, les banques doivent surveiller attentivement les fonds qui entrent dans leurs systèmes, et pas seulement la destination des fonds lorsqu'ils en sortent.

La réglementation britannique incite les banques à prendre des mesures proactives pour prévenir les fraudes et les pertes dues aux escroqueries au lieu d'avoir une attitude réactive face à ces dernières.

Confirmation du bénéficiaire (CoP)

Les banques sont également tenues de vérifier que le nom du bénéficiaire correspond aux informations de son compte bancaire lorsqu'un client transfère des fonds. Cette couche de sécurité supplémentaire vise à réduire les pertes dues aux escroqueries par APP et à réduire les pertes résultant d'erreurs humaines telles que les fautes de frappe ou d'orthographe. D'ici à octobre 2024, l'obligation du CoP s'appliquera à toutes les banques britanniques et à toutes les entreprises de traitement des paiements qui proposent des services de Paiements instantanés, BACS et CHAPS.

Rendre publiques les pertes liées aux escroqueries

Dans le cadre de la réglementation actualisée de la PSR, les banques britanniques doivent également s'attendre à un examen plus approfondi de leurs efforts de prévention des fraudes et des escroqueries. En 2023, la PSR a commencé à publier la manière dont les banques et les autres prestataires de services de paiement traitent les pertes liées aux escroqueries et leurs efforts de remboursement. Les rapports PSR indiquent le montant des remboursements reçus par les victimes d'escroquerie, le montant envoyé par chaque entreprise et le montant accepté en raison des pertes subies par l'APP. Ces informations publiques inciteront les banques britanniques à démontrer leur engagement à rembourser les victimes d'une escroquerie.

Une stratégie uniquement focalisée sur la surveillance des transactions sortantes revient à essayer de résoudre un crime avec un œil fermé.

Les attaques frauduleuses non autorisées – y compris le vol d'informations de cartes de crédit et la fraude par carte absente (CNP) – et les paiements autorisés par escroquerie aux paiements par ingénierie sociale (APP) – notamment les escroqueries sentimentales à l'achat – font partie des tactiques préférées des criminels. Si les pertes dans ces deux catégories ont légèrement diminué en 2023, les chiffres restent considérables et indiquent que les banques britanniques doivent prendre des mesures supplémentaires pour protéger leurs clients.

Sur la base de ces données, les banques pourraient penser que la meilleure solution est de se concentrer sur des politiques et des technologies qui utilisent une approche basée sur les canaux, comme une solution unique pour la fraude par carte, une autre pour les canaux mobiles et une autre pour les services bancaires par téléphone. Mais cela revient à prendre des mesures analogiques alors que les fraudeurs ont évolué numériquement. Cette approche cloisonnée laisse des lacunes et des opportunités que les criminels peuvent exploiter.

Que peuvent donc faire les banques pour lutter efficacement contre la fraude ? Casser les silos. Une stratégie efficace de lutte contre la fraude doit comprendre un contrôle proactif et multi-canaux qui suit les deux côtés de chaque paiement, ce qui permet d'avoir une vue d'ensemble des transactions.

Une stratégie uniquement focalisée sur la surveillance des transactions sortantes revient à essayer de résoudre un crime avec un œil fermé. Cette vision limitée, souvent basée sur les canaux, expose les banques et les clients à des pertes et à des coûts opérationnels inutiles. Il s'agit aussi d'un jeu de la taupe perdu d'avance, car les fraudeurs migrent vers le canal suivant, moins surveillé.

La surveillance des paiements entrants renforce la lutte contre la fraude

La surveillance des paiements entrants consiste à analyser et à examiner minutieusement de manière proactive les paiements reçus par une banque ou une institution financière. Il s'agit essentiellement de surveiller tous les flux d'argent entrant sur les comptes, et pas seulement les flux d'argent sortant.

Ce changement de paradigme permet aux institutions financières d'analyser chaque étape d'une transaction et de relier des activités apparemment sans rapport entre elles. Les banques ne se contenteront pas de connaître leurs clients, elles acquerront une connaissance approfondie de leurs comportements. Cela ouvre des perspectives qui vont bien au-delà de la détection des fraudes. Cela ouvre également la voie à la personnalisation des messages et permet d'offrir à la clientèle une expérience véritablement exceptionnelle.

En plus d'aider les banques à comprendre les comportements de leurs clients, la surveillance des paiements entrants peut les aider à respecter leurs nouvelles obligations réglementaires. Les banques peuvent plus facilement détecter si un escroc tente de transférer de l'argent sur un compte contrôlé par une mule et geler ou approfondir l'enquête sur la transaction. La capacité à prévenir les fonds mal acquis provenant d'escroqueries et de fraudes sera essentielle pour les banques britanniques lorsque la responsabilité à parts égales des institutions émettrices et réceptrices entrera en vigueur.

Les banques ne se contenteront pas de connaître leurs clients, elles acquerront une connaissance approfondie de leurs comportements.

Pour les institutions financières, il est essentiel d'avoir une vision globale de la fraude

Dans le nouveau paysage des paiements, qui comprend l'open banking, l'avènement de nouveaux canaux de paiement et l'évolution rapide des typologies de fraude, traiter les paiements de manière isolée ou à travers un seul canal ne suffit plus.

La révolution numérique, accélérée par la pandémie, a entraîné une modification du comportement des consommateurs et des typologies de fraudes. Les criminels avisés ont rapidement exploité les nouvelles technologies pour contourner les défenses. Ils se sont fondus dans le volume énorme de transactions, se cachant à la vue de tous. L'IA est venue à la rescousse, aidant les institutions financières à examiner des milliards de transactions en un clin d'œil pour identifier les bons et les mauvais comportements. Cependant, les fraudeurs se sont rapidement adaptés à la fraude par piratage de compte (ATO).

La fraude ATO est devenue une boîte de Pandore, donnant accès à des identités entières, et pas seulement à des comptes. Les banques avant-gardistes ont réagi en adoptant des technologies de pointe telles que la biométrie comportementale, mais la chasse au chat et à la souris s'est poursuivie.

Lorsque l'ATO est devenu trop difficile, les fraudeurs ont dévoilé leur arme la plus rusée : les escroqueries par autorisation de paiements. Les escroqueries par autorisation de paiement trompent ou manipulent les victimes pour qu'elles communiquent des données à caractère personnel (DCP), l'accès à leur compte, et bien d'autres choses encore. Aujourd'hui, comme l'IA générative est capable de créer de fausses vidéos, des clones vocaux convaincants et des chats qui trompent presque tout le monde, les banques doivent se préparer à la « Fraude : Édition métavers ».

Mais ce n'est pas tout, car ce n'est pas seulement la fraude qui rend nécessaire la surveillance des paiements entrants. Ce sont les paiements eux-mêmes.

Les escroqueries par autorisation de paiement trompent ou manipulent les victimes pour qu'elles communiquent des données à caractère personnel (DCP), l'accès à leur compte, et bien d'autres choses encore.

La montée des escroqueries

Heureusement, de nombreuses banques ont pris des mesures importantes pour lutter contre les tentatives d'ATO. Mais les fraudeurs ne sont pas découragés par l'échec. En revanche, ils se sont tournés vers le prochain maillon faible de la chaîne de paiement : les clients.

Ils ont lancé une campagne d'escroqueries à l'encontre des clients en utilisant diverses techniques de manipulation. Il s'agit notamment d'escroqueries par usurpation d'identité dans lesquelles ils se font passer pour des représentants de banques, du gouvernement ou des forces de l'ordre, d'escroqueries sentimentales, d'escroqueries à l'achat et d'escroqueries à l'investissement, pour n'en citer que quelques-unes.

Cette avalanche d'escroqueries a valu au Royaume-Uni le triste surnom de « Capitale mondiale de l'escroquerie ». Les changements réglementaires apportés par le PSR (partage des responsabilités à parts égales, CoP et publication des données relatives aux escroqueries) visent à aider le secteur des services financiers du Royaume-Uni à dépasser ce malheureux surnom.

La bonne nouvelle est que, d'après les données de UK Finance, les efforts déployés par les banques pour lutter contre les escroqueries et les fraudes donnent des résultats positifs. Mais comme des millions sont encore perdus, il faut faire plus.

De nouvelles opportunités pour les banques

Le nombre d'escroqueries est devenu si important que les organismes de régulation britanniques envisagent une proposition controversée visant à retarder de quatre jours les Paiements instantanés en cas de suspicion de fraude. Cette mesure, si elle était adoptée, porterait atteinte à la proposition de valeur fondamentale des Paiements instantanés.

On ne sait pas encore si les organismes de régulation adopteront la mesure de ralentissement. En attendant, les banques peuvent protéger leurs clients de manière proactive en surveillant les paiements entrants en temps réel. Cette mesure sera cruciale pour les banques, car elles devront faire face à des pressions pour rembourser les victimes de l'escroquerie APP, démontrer leur engagement à assurer la sécurité des paiements et concrétiser les avantages des Paiements instantanés.

En outre, la surveillance des paiements entrants offre aux banques un outil précieux pour détecter et arrêter les money mules. Bien que les money mules puissent sembler être de petits acteurs de la criminalité financière, ils jouent un rôle essentiel en aidant les criminels à tirer profit de la fraude, de l'escroquerie et d'autres formes de criminalité financière. Il est essentiel de les arrêter pour perturber l'activité criminelle dans son ensemble.

La surveillance des paiements entrants peut également aider les banques à atteindre leurs objectifs en matière de développement durable et de responsabilité sociale. Pay.UK note que plus de 70 % des fraudes sont liées à des activités internationales, souvent menées par des entreprises criminelles, y compris des trafiquants d'êtres humains. Certaines victimes de la traite sont forcées de travailler dans des centres d'appel pour trouver d'autres victimes.

Les fraudes et les escroqueries profitent en fin de compte aux criminels qui blanchissent les profits mal acquis par l'intermédiaire de comptes de mule. Les crimes liés à la traite des êtres humains et aux atteintes à l'environnement sont souvent liés à des activités de blanchiment d'argent. Les banques engagées dans le développement durable devraient examiner comment ces développements affectent leurs priorités environnementales, sociales et de gouvernance (ESG).

Ces changements réglementaires, combinés aux liens entre les money mules et les réseaux criminels, soulignent l'importance pour les banques de les détecter et de les prévenir avant qu'ils ne se produisent. Les récentes réglementations sont plus que de nouvelles obligations pour les banques ; elles sont un appel à l'action pour assurer la sécurité des clients et être des acteurs mondiaux responsables en adoptant une approche proactive de la détection des fraudes.

Les risques et les avantages

Il n'a jamais été aussi urgent pour les banques de mettre en place des systèmes de surveillance sophistiqués capables d'examiner minutieusement les transactions entrantes et sortantes. Les banques doivent être en mesure d'identifier les comportements anormaux des deux côtés de la transaction. L'utilisation des données améliorées disponibles pour le flux de paiement en temps réel, à la fois transactionnelles et comportementales, peut contribuer grandement à l'adaptation de votre stratégie de lutte contre la fraude aux prochaines obligations réglementaires et à la protection de vos clients.

Ne pas surveiller les paiements entrants pour détecter les activités suspectes ou les comportements frauduleux revient à demander à vos équipes chargées de la lutte contre la fraude et la criminalité financière de travailler avec une main liée derrière leur banque parce que cela :

- **Limite votre capacité à détecter la fraude multi-canaux et la criminalité financière.** L'activité des mules, par exemple, implique toujours des paiements entrants pour acheminer des fonds volés et devient beaucoup plus évidente lorsque l'on observe le schéma des paiements entrants et sortants.
- **Augmente les coûts opérationnels et les frictions avec les clients.** Les retenues sur les paiements dues au manque de visibilité créent des demandes de renseignements et des frustrations inutiles.
- **Entrave la prévention proactive de la fraude.** Vous travaillez essentiellement sans un tiers des informations nécessaires pour identifier les menaces émergentes et adapter vos défenses.

Les banques doivent être en mesure d'identifier les comportements anormaux des deux côtés de la transaction.

En revanche, la surveillance des paiements entrants et sortants permet aux banques de :

- **Garantit des transactions sans friction pour les bons clients.** Finis les faux positifs déclenchés par une activité légitime dans un canal.
- **Identifie les activités suspectes.** En examinant l'ensemble du flux de paiement, des schémas inhabituels dans les paiements entrants et sortants deviennent évidents, révélant des ATO potentiels, des activités des mules et d'autres menaces cachées.
- **Identifier les vitesses suspectes.** Les hausses soudaines dans l'une ou l'autre direction ou les écarts entre les flux entrants et sortants mettent en évidence une activité frauduleuse potentielle.
- **Réduire les pertes.** L'identification proactive permet d'intervenir plus rapidement, ce qui réduit les dommages pour les banques et les clients.
- **Protéger le système.** Comprendre la fraude de manière globale permet de lutter contre les menaces émergentes telles que les stratagèmes alimentés par l'IA générative et de renforcer la sécurité du système financier. N'oubliez pas que tout stratagème de fraude implique en fin de compte des mouvements d'argent. Il ne peut y avoir de fraude sans blanchiment d'argent.

Le passage à la surveillance des paiements entrants et sortants ne réduit pas seulement la fraude par canal, comme les cartes ou les données de compte volées. Il ne s'agit pas non plus d'arrêter les malfaiteurs, mais de protéger notre avenir. En adoptant une vision holistique de la fraude, nous pouvons avoir une longueur d'avance et garantir un écosystème financier sûr et prospère, même face à des menaces du métavers telles que l'IA générative.

Objectifs en matière de pertes liées à la fraude et objectifs en matière de croissance commerciale

Les banques luttent en permanence pour trouver un équilibre entre la satisfaction client et la prévention de la fraude. Le défi n'est pas seulement d'arrêter la fraude, mais aussi de s'assurer qu'elle n'entrave pas l'expérience client.

De nombreuses banques ont historiquement surveillé les paiements sortants pour détecter les fraudes, tout en négligeant la surveillance des paiements entrants ou en traitant les deux comme des silos distincts. Cette méthode entraîne toutefois un double problème : des difficultés accrues en matière de service clientèle et/ou des pertes financières accrues.

Le défi n'est pas seulement d'arrêter la fraude, mais aussi de s'assurer qu'elle n'entrave pas l'expérience client.

Imaginons deux banques aux extrêmes de cette approche :

Banque A

Illustre les pièges d'un accès aux fonds trop prudent. L'accès aux fonds est limité pour réduire les risques de fraude. Cependant, cette approche a un impact négatif sur l'expérience client. Attendre le déblocage des fonds devient le principal grief des clients.

Alors qu'elle réalise des économies sur les pertes liées à la fraude, la banque doit soudain faire face aux coûts cachés de la prévention de la fraude en raison de l'augmentation du nombre d'appels au service clientèle de la part de personnes désireuses de confirmer le déblocage de leurs dépôts.

Banque B

Illustre les risques de l'indulgence, en offrant un large accès aux fonds avec un délai minimal. Si cette approche est bénéfique en termes de satisfaction client, elle expose la banque à des pertes importantes liées à la fraude, voire à des problèmes réglementaires ou à une atteinte à sa réputation. La banque perd de l'argent à cause de la fraude, ce qui nuit en fin de compte à ses revenus et à son résultat net.

La mise en œuvre d'une surveillance des paiements entrants permet de tirer le meilleur des deux scénarios et de laisser le reste.

Aperçu de la surveillance des paiements entrants

La surveillance des paiements entrants est un outil essentiel dans l'arsenal d'une banque contre la criminalité financière. En examinant minutieusement les flux de fonds entrants, les institutions financières peuvent identifier et limiter les activités frauduleuses de manière préventive, sauvegardant ainsi leurs actifs, leur réputation et la confiance de leurs clients.

Les anomalies dans le schéma des dépôts peuvent signaler des problèmes bien avant qu'ils ne se transforment en pertes importantes pour l'institution financière ou son client.

Évasion par piratage de compte (ATO)

Les banques peuvent identifier les premières étapes d'un plan d'évasion au moyen de schémas inhabituels de dépôts suivis d'une utilisation maximale des lignes de crédit. Il peut s'agir de hausses soudaines des soldes des comptes qui ne correspondent pas au profil du client ou à son comportement historique, ce qui laisse supposer une activité préparatoire à une opération d'évasion.

Activité des mules

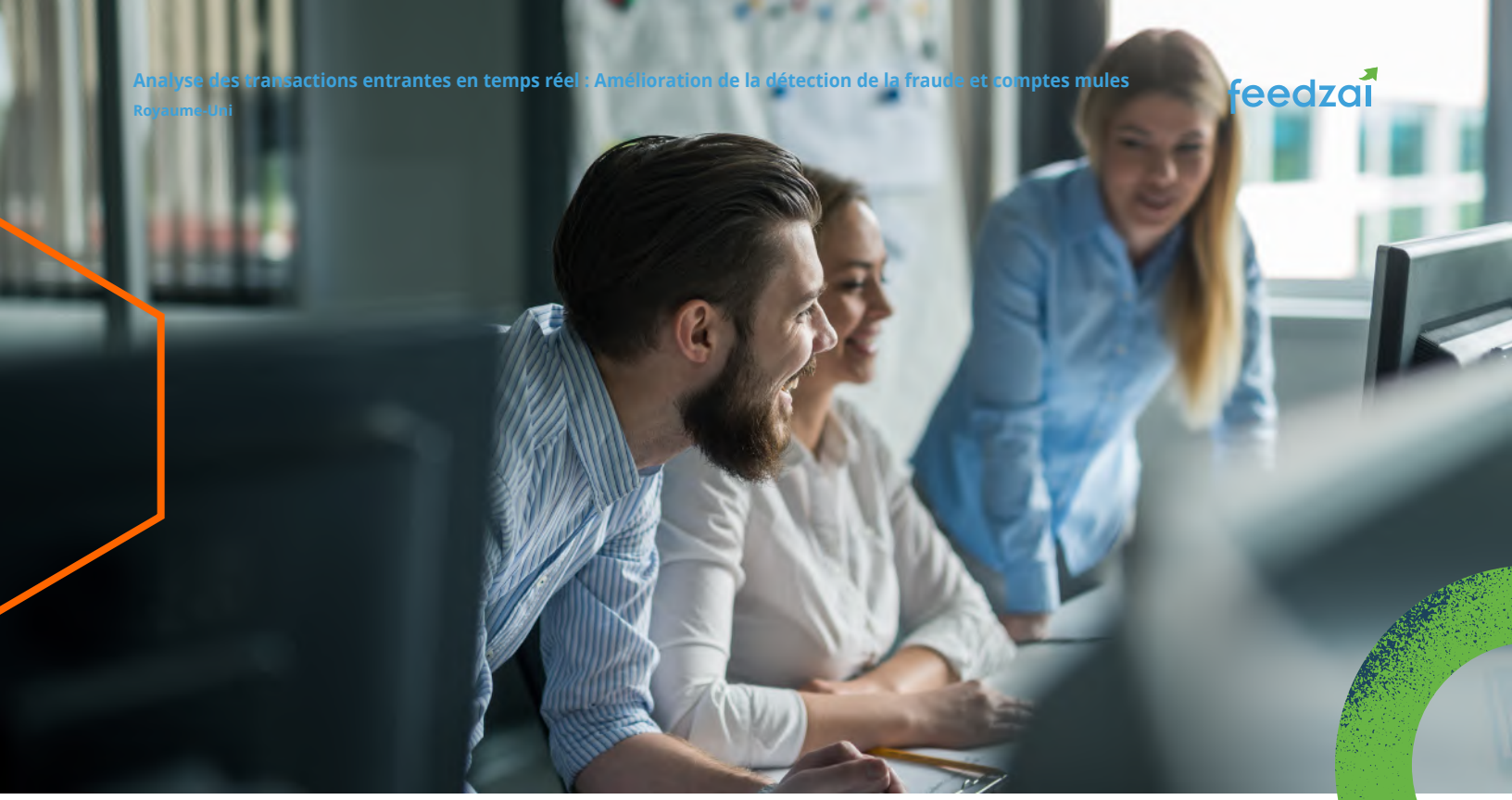
La surveillance des transactions entrantes inhabituelles, en particulier celles qui sont suivies de retraits rapides ou structurés, de transferts vers d'autres comptes ou qui proviennent de sources géographiquement incohérentes avec le lieu où se trouve le client, peut indiquer une activité des money mules. Il peut s'agir de multiples petits dépôts qui restent juste en dessous des seuils de déclaration ou de profils de transactions incohérents qui ne correspondent pas au profil du titulaire du compte.

Escroquerie par paiement autorisé

La surveillance des paiements entrants peut jouer un rôle dans l'identification de ce type de fraude lorsque les fonds sont transférés sur des comptes détenus par l'institution de surveillance. Par exemple, si un compte personnel commence soudainement à recevoir plusieurs paiements d'un montant élevé provenant de différents comptes externes, en particulier si ces paiements sont ensuite rapidement transférés, cela pourrait indiquer que le compte est utilisé dans le cadre d'un stratagème de fraude par APP.

Fraude de première partie

Les banques doivent être en mesure d'identifier les incohérences ou les irrégularités dans les flux de fonds qui indiquent une activité frauduleuse. Il peut s'agir des dépôts de fonds provenant de sources douteuses ou de schémas suggérant le recyclage de fonds pour gonfler la solvabilité apparente.



Comment ça fonctionne

Voici un exemple de la manière dont la surveillance des paiements entrants et sortants renseigne les équipes chargées de la lutte contre la fraude.

Comportement d'évasion : Récapitulatif

La fraude par évasion est un système délibéré par lequel les fraudeurs :

1

Établissent leur solvabilité

Ouvrent des comptes et maintiennent une activité régulière pour se constituer un historique de crédit apparemment bon, souvent en mentant sur leurs revenus réels dans les demandes pour paraître plus solvables.

2

Gonflent les soldes

Reçoivent ou déposent soudainement des sommes importantes sur le compte afin d'augmenter artificiellement le crédit à leur disposition.

3

Maximisent et disparaissent

Épuisent rapidement leurs lignes de crédit (en contractant des prêts, en faisant de gros achats) avant de disparaître sans jamais avoir l'intention de rembourser.

Pourquoi la surveillance des flux entrants et sortants constitue un puissant duo

→ Flux entrants : Système d'alerte précoce

Un compte compromis recevant des dépôts inhabituels et soudains peut déclencher un signal d'alarme important, souvent avant le début d'une activité de dépense malveillante. La surveillance des flux entrants détecte ces mouvements préparatoires en mettant en évidence :

- Des augmentations inexpliquées du solde
- Des fonds provenant de sources inconnues ou à haut risque
- Des écarts par rapport aux modèles de revenus prévus

→ Flux sortants : Attraper les sorties d'argent

Même si la surveillance des flux entrants passe à côté de certains signaux précoces, l'analyse des flux sortants permet de repérer la frénésie des dépenses associée à une tentative d'évasion. L'observation de ces actions permettra de repérer le stratagème :

- Retraits importants d'argent liquide
- Volume élevé et soudain d'achats
- Dépenses atypiques du bénéficiaire (transferts vers de nouveaux comptes, paiements différents de ceux observés précédemment)

L'avantage combiné de la surveillance entrante et sortante

Utilisées conjointement, les banques créent une défense plus complexe contre les stratagèmes d'évasion :

Détection plus rapide

La détection précoce d'une évasion permet de la bloquer avant que d'importantes lignes de crédit ne soient entièrement dépensées.

Une vision plus approfondie

L'analyse des flux entrants et sortants permet de dresser un tableau plus complet du stratagème de fraude et d'améliorer les enquêtes.

Adaptation proactive

Les fraudeurs adaptent leurs tactiques. En combinant la surveillance des flux entrants et sortants, il est plus facile de repérer les écarts dans leurs méthodes, ce qui aide les banques à garder une longueur d'avance sur l'évolution des escroqueries.

Des idées à l'action

Maintenant que nous comprenons le problème posé par un système de surveillance des flux sortants uniquement, voici quelques éléments à prendre en compte dans la suite de votre lecture :

1 Évaluation de la surveillance des paiements entrants

Procédez à une évaluation approfondie de votre surveillance actuelle. Questions clés à poser :

- **Champ d'application des données :** Pouvez-vous analyser une vue complète de l'activité d'un client, de ses comptes et du flux de transactions pour les paiements entrants et sortants ?
- **Silos de canaux :** Votre solution actuelle facilite-t-elle l'analyse des données multi-canaux, ou cette capacité fait-elle défaut ?
- **Focalisation sur la détection :** Dans quelle mesure l'accent est-il mis sur les schémas des flux entrants plutôt que sur les seuls indicateurs sortants ? L'approche reflète-t-elle celle de la banque A ou de la banque B ?

2 Examen des fournisseurs et des solutions

Cet examen doit être guidé par l'évaluation interne. Principales considérations :

- **Adaptabilité :** La solution de votre fournisseur peut-elle évoluer avec les nouveaux canaux de paiement et les menaces telles que l'IA générative ?
- **Capacité de personnalisation :** Votre solution actuelle répond-elle à la taille spécifique d'une banque, à sa clientèle et à son profil de risque ? Il s'agit notamment d'ajuster les paramètres de détection des règles et des comportements.
- **Intégration :** Dans quelle mesure la technologie améliorée s'intègre-t-elle facilement à l'ensemble des outils de lutte contre la fraude de votre banque ?
- **Évolutivité :** La solution de surveillance des flux entrants proposée est-elle adaptée à la croissance à court et à long terme prévue par votre banque ?

3 Conformité et réglementation

La stratégie d'une banque doit être guidée par la volonté de garder une longueur d'avance sur les attentes légales et réglementaires. Actions clés :

- **Mise à jour des politiques :** Réévaluez les procédures internes de lutte contre la fraude à la lumière de l'évolution des normes juridiques relatives à la responsabilité des banques.
- **Formation interne :** Formez les équipes concernées (en particulier le personnel en contact avec la clientèle) aux indicateurs de fraude entrante et aux bonnes pratiques de communication avec les clients concernés.

Protéger votre banque : Techniques de pointe pour une défense proactive contre la fraude

Analyses et techniques de pointe pour la détection des fraudes

Nous savons tous que les criminels conçoivent constamment de nouveaux stratagèmes, même dans les canaux traditionnels. Il est donc essentiel de garder une longueur d'avance en matière de détection des fraudes. Heureusement, les institutions financières disposent d'un arsenal d'outils et de techniques sophistiqués, en particulier d'outils d'analyse et d'enrichissement de pointe qui leur permettent de lutter efficacement contre la fraude, quel que soit le canal (en ligne, mobile, en agence, par carte ou autre) afin de protéger nos clients et leur argent durement gagné.

La protection proactive contre la fraude consiste à éviter ces menaces à l'aide d'un système de défense à plusieurs niveaux axé sur l'analyse de pointe, l'enrichissement ciblé des données et la détection en temps réel.

La protection proactive contre la fraude consiste à éviter ces menaces à l'aide d'un système de défense à plusieurs niveaux axé sur l'analyse de pointe, l'enrichissement ciblé des données et la détection en temps réel.

Une défense à plusieurs niveaux contre des menaces en constante évolution

Une stratégie solide de prévention de la fraude combine des outils sophistiqués, des sources de données internes et externes et des systèmes traditionnels basés sur des règles :

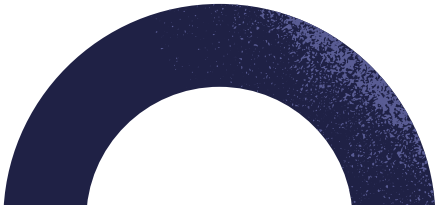
Enrichisseurs internes : Vos données, votre arsenal

Les enrichisseurs internes constituent la base de votre stratégie de détection des fraudes. Ils vous permettent d'exploiter une mine d'informations sur vos comptes et vos transactions afin de dresser un tableau complet de l'activité financière.

Enrichisseurs internes pour la fraude par dépôts

→ Informations sur les comptes, les clients et les transactions

- **Données démographiques de base :** Âge, sexe, adresse, numéro de téléphone, adresse électronique.
- **Historique du compte :** Date d'ouverture du compte, historique du solde, historique des transactions, type de compte et incidents de fraude antérieurs.
- **Relation avec le client :** Durée de la relation avec la banque, produits de prêt ou de dépôt détenus, schémas des activités du compte.
- **Données comportementales :** Activité bancaire en ligne, utilisation des guichets automatiques, transactions bancaires mobiles, habitudes de dépenses.
- **Données contextuelles :** Connexions mobiles, connexions web, changements de compte, messages d'avertissement, mesures à long terme, mises à jour des bénéficiaires.
- **Données de session :** Détection des RAT, risques temporels, hésitation de l'utilisateur, analyse comportementale, modèles de dictée, détection des appels actifs.
- **Données de paiement :** Paiements sortants, paiements entrants, données multi-canaux, prédictions MO, règles d'escroquerie et modèles d'escroquerie.



→ Analyses et techniques de pointe

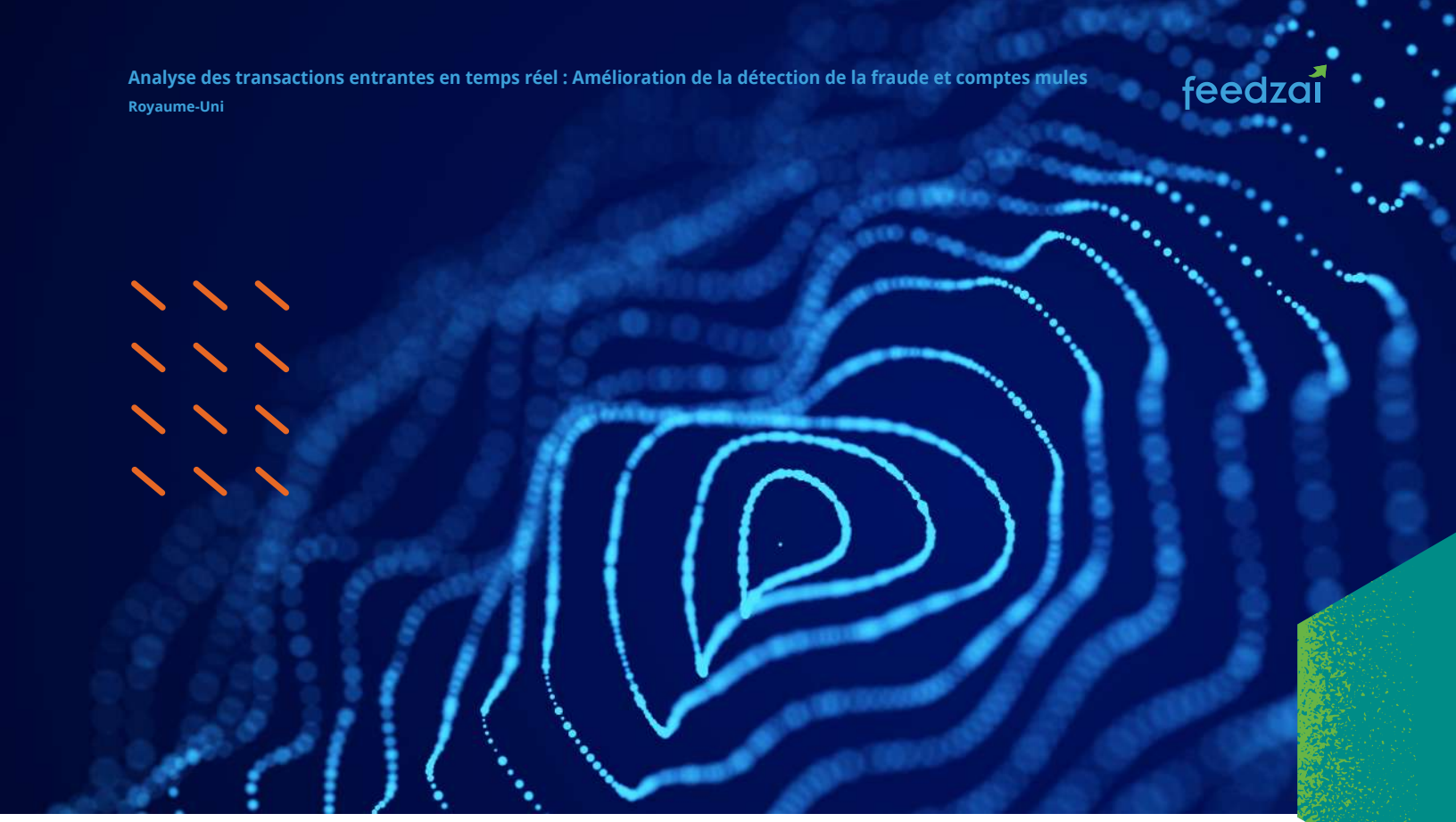
- **Analyse des réseaux :** Identification des liens entre les comptes et les activités potentiellement frauduleuses.
- **Données de géolocalisation :** Analyse de la localisation d'un dépôt pour identifier les divergences avec l'activité habituelle d'un titulaire de compte.
- **Biométrie comportementale :** Analyse des schémas de frappe, des mouvements de la souris et d'autres comportements en ligne pour vérifier l'identité de l'utilisateur.
- **Analyse multi-canaux :** Les fraudeurs utilisent souvent plusieurs canaux. Recherchez des modèles et des incohérences entre les méthodes de paiement pour détecter les stratagèmes sophistiqués.

Ces enrichisseurs internes fournissent des informations précieuses sur les comportements financiers typiques des clients, ce qui permet aux banques d'identifier tout écart susceptible de signaler une fraude potentielle.

Enrichisseurs externes : Élargir le réseau de renseignements

Si les données internes constituent un bon point de départ, il ne faut pas s'arrêter là. Les enrichisseurs externes fournissent des couches supplémentaires de renseignements, en s'appuyant sur :

- **Des systèmes d'alerte précoce :** Bases de données sur les activités frauduleuses connues, partagées par les institutions financières.
- **Des dossiers publics et des données des réseaux sociaux :** Des informations accessibles au public qui peuvent aider à vérifier l'identité et à identifier les signaux d'alarme.



Analyse de pointe : Transformer les données en informations exploitables

L'enrichissement des données n'est qu'une première étape. Le véritable pouvoir réside dans l'analyse de pointe. Les banques devraient exploiter des techniques de pointe telles que :

- **L'analyse des réseaux :** Identification des liens entre les comptes, les appareils et les activités potentiellement frauduleux.
- **Les données de géolocalisation :** Analyse de la localisation des transactions pour identifier les divergences avec l'activité habituelle du titulaire du compte.
- **La biométrie comportementale :** Analyse des schémas de frappe, des mouvements de la souris et d'autres comportements en ligne pour vérifier l'identité de l'utilisateur.

Ces analyses de pointe nous aident à découvrir des modèles et des corrélations cachés que les méthodes traditionnelles pourraient manquer, ce qui permet aux entreprises d'identifier et de prévenir les tentatives de fraude avec plus de précision et d'efficacité.

N'oubliez pas que la prévention de la fraude est un processus continu. Les institutions financières garderont une longueur d'avance en surveillant et en adaptant en permanence leurs stratégies aux menaces émergentes.

Signaux de risque des mules

Lorsque des paiements frauduleux se produisent, qu'ils soient non autorisés ou que quelqu'un se fasse piéger pour envoyer de l'argent, ils vont d'abord sur un compte de mule. La surveillance des paiements entrants permet d'identifier les comptes de money mule en suivant les transactions autorisées, non autorisées et manipulées.

Cette approche proactive améliore la détection des activités frauduleuses, réduisant ainsi les pertes financières. En outre, elle aide à comprendre les profils des comptes de mule, ce qui permet d'affiner les processus d'ouverture des comptes afin d'éviter l'inclusion non désirée de comptes similaires à l'avenir. Cette stratégie réduit également la nécessité et les coûts associés à la suppression des comptes de mule conformément aux exigences en matière de lutte contre le blanchiment d'argent (LCBA).

Les signaux de risque de mules à surveiller dans le cadre de votre programme de contrôle des paiements entrants sont les suivants :

→ Comportement des comptes et des clients

- **Nouveaux comptes avec des transactions très rapides :** Des transactions soudaines et fréquentes, en particulier celles qui portent sur des sommes importantes, sur des comptes nouvellement ouverts doivent déclencher l'alerte.
- **Disparité entre les revenus et le volume des transactions :** Les comptes dont les revenus sont faibles et qui génèrent une activité transactionnelle importante, notamment en ce qui concerne les transferts internationaux, sont le signe d'une activité potentielle de la mule.
- **Des habitudes de dépôt et de retrait inhabituelles :** Des dépôts soudains de sommes importantes suivis de retraits rapides ou des lieux de dépôt incohérents par rapport au lieu de résidence du titulaire du compte sont des signes suspects.
- **Comptes dormants soudainement activés :** Des comptes peu ou pas actifs présentant soudainement un volume élevé de virements vers des destinataires inconnus suggèrent une activité potentielle de mule.
- **Des incohérences comportementales lors de l'ouverture du compte :** Des incohérences entre les professions déclarées et les habitudes de transaction, des adresses incohérentes ou une certaine nervosité lors des procédures d'ouverture de compte peuvent être des signes d'alerte.

→ Analyse des transactions et des réseaux

- **Transactions avec des destinations à haut risque :** Les transferts vers des pays connus pour leurs réseaux de blanchiment d'argent ou de fraude doivent être examinés minutieusement.
- **Interaction fréquente avec des comptes connus pour leur caractère frauduleux :** Les comptes qui envoient ou reçoivent régulièrement des fonds provenant de comptes de mules ou frauduleux identifiés sont probablement impliqués dans des activités criminelles.
- **Augmentation soudaine du volume des transactions :** Une augmentation brutale du nombre de transactions, en particulier avec des destinataires inconnus, justifie une enquête.
- **Des informations sur les comptes et les bénéficiaires qui ne correspondent pas :** Des divergences entre les noms ou les lieux des titulaires des comptes et des bénéficiaires peuvent indiquer des tentatives de dissimulation d'activités suspectes.
- **Regroupement d'activités frauduleuses :** L'identification des groupes de comptes au sein de la banque présentant un comportement similaire à celui d'une mule peut mettre en évidence des réseaux criminels plus étendus.

→ Données relatives aux appareils et à la localisation

- **Incohérences de géolocalisation :** L'activité d'un compte à partir de lieux très différents de l'adresse enregistrée ou des habitudes habituelles peut suggérer l'existence d'une activité de mule.
- **Appareils partagés pour l'accès aux comptes :** L'accès à plusieurs comptes à partir du même appareil, en particulier dans des lieux géographiquement disparates, fait craindre des appareils compromis ou des réseaux de mules.
- **Adresses IP inconnues ou à haut risque :** Les transactions provenant d'adresses IP suspectes, connues pour des maliciels ou des réseaux de zombies, doivent faire l'objet d'une enquête.
- **Changements fréquents d'appareils :** Les comptes auxquels on accède constamment à partir de nouveaux appareils suggèrent des tentatives potentielles d'échapper à la détection par les mules.

→ Signaux supplémentaires

- **Richesse soudaine et inexpliquée du titulaire du compte :** Un écart important entre un niveau de revenu connu et l'accès soudain à des sommes importantes est un indicateur potentiel de l'activité d'une mule.
- **Publications sur les réseaux sociaux concernant des opérations de transfert d'argent ou des avoirs en espèces d'un montant suspect :** Les informations accessibles au public peuvent parfois indiquer une activité potentielle de mule.

Cette approche proactive aide à comprendre les profils des comptes de mules, ce qui permet d'affiner les processus d'ouverture de compte afin d'éviter l'inclusion non désirée de comptes similaires.

Des idées à l'action

1 Vérification de l'analyse et des outils

Passez en revue votre arsenal actuel.

- **Techniques d'analyse :** Quelles sont les techniques d'analyse utilisées ? Couvrent-elles l'éventail proposé (de l'analyse de réseau à la biométrie comportementale) ?
- **Utilisation des données :** Les systèmes et algorithmes actuels exploitent-ils de manière adéquate les ensembles de données multicanaux et les sources externes comme recommandé ?
- **Lacunes dans les solutions :** Existe-t-il des domaines spécifiques où les solutions existantes sont insuffisantes par rapport à la section sur l'analyse de la fraude de cet ebook (par exemple, faiblesse de l'enrichissement des données des réseaux sociaux) ?

2 Évaluation de la collaboration

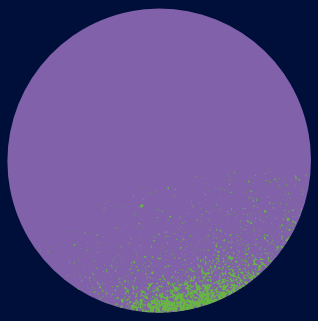
Examinez le niveau actuel de participation de la banque à des efforts intersectoriels et de partenariat :

- **Liaison avec les forces de l'ordre :** Existe-t-il un point de contact établi pour un partage rapide des connaissances sur les nouvelles tactiques de fraude émergentes ?
- **Relations avec les fournisseurs et les consortiums :** Quel rôle jouent les entreprises partenaires dans l'amélioration de l'accès à l'information et des algorithmes de détection ?

3 Feuille de route et investissements

Cette section présente des arguments solides en faveur de la poursuite (ou de l'augmentation) des investissements dans la détection avancée de la fraude. Points à prendre en compte par les banques :

- **Mises à jour technologiques :** La vérification révèle-t-elle un besoin de capacités technologiques nouvelles ou étendues, alignées sur les analyses décrites dans cette section ?
- **Compétences :** Les équipes de données existantes auront-elles besoin de nouvelles embauches ou d'une formation pour utiliser efficacement des outils d'analyse plus sophistiqués ?
- **Investissements internes ou chez des partenaires :** La sempiternelle décision « fabriquer son propre outil ou acheter auprès d'un fournisseur ». Quels sont les outils/enrichisseurs qu'elles peuvent développer en interne, et quels sont ceux qu'il est préférable d'externaliser ou d'obtenir par l'intermédiaire de partenaires ?



Stratégies de surveillance des paiements entrants

La surveillance des paiements entrants à des fins de détection et de prévention de la fraude est une approche relativement nouvelle dans le monde de la prévention de la fraude. En tant qu'entreprise native de l'IA ayant des décennies d'expérience dans la détection des fraudes pour les institutions financières du monde entier et notre propre expérience, voici l'approche de mise en œuvre que nous suggérons.

Approche progressive

Commencez par des programmes pilotes pour un seul canal, et augmentez progressivement la portée en fonction de l'expérience et du succès.

Tests complets

Testez et affinez rigoureusement les modèles de détection des fraudes et les méthodes d'authentification afin de garantir la précision et de minimiser les faux positifs qui perturbent les activités légitimes.

Surveillance et optimisation continues

Examinez et adaptez régulièrement les stratégies de détection des fraudes en fonction de l'évolution des tactiques de fraude et des nouvelles menaces.

Comment fonctionne la surveillance des paiements entrants

La surveillance des paiements sortants se concentre sur la personne qui a initié le paiement. La surveillance des paiements entrants adopte une approche différente en identifiant les schémas et activités frauduleux cachés dans les fonds entrants. Voyons comment cette technologie de pointe permet de découvrir les risques cachés derrière les transactions.

→ Surveillance des paiements sortants

1 Qui a initié le paiement ?

Déterminez si c'est une partie autorisée ou non qui a déclenché le paiement. Cela implique de vérifier l'identité de l'initiateur de la transaction et l'autorité de paiement.

Utilisez la biométrie comportementale pour détecter les anomalies dans la manière dont la partie interagit avec l'appareil pendant la transaction (par exemple, la pression exercée pendant la frappe, les schémas du mouvement de la souris, le temps passé sur des champs spécifiques et les schémas de manipulation de l'appareil, etc.) et qui s'écartent du comportement habituel de l'utilisateur légitime.

2 Comment la fraude a-t-elle été exécutée ?

Déterminez la méthode utilisée par la partie non autorisée ou autorisée pour exécuter la fraude.

Non autorisée
Identifiez les moyens de piratage de compte, généralement grâce aux informations d'identification compromises obtenues par hameçonnage, par des maliciels ou par des violations de données.

Autorisée
Il s'agit généralement de fraude sur les produits et services, sur les relations et la confiance, de fausses demandes de remboursement, d'informations d'identification compromises et d'usurpation d'identité de parties autorisées.

3 Quel est le score de risque de fraude ?

Prenez en compte le niveau de risque lié à la transaction en utilisant une combinaison de modèles d'IA et de décisions basées sur des règles.

Signaux de fraude traités avec des modèles d'IA
Analyse de la géolocalisation et de l'IP, analyse de l'historique des transactions et analyse du profil des clients.

Signaux de fraude traités par des règles
Montants des transactions « si alors cela », nombre de tentatives, etc.

→ Surveillance des paiements entrants :

1 Signaux de fraude traités avec des modèles d'IA

Analyse des comptes et des clients, analyse des transactions et du réseau, données relatives aux appareils et à la localisation.

2 Signaux des mules traités avec des modèles d'IA

Comportement des comptes et des clients, analyse des transactions et des réseaux, données relatives aux appareils et à la localisation.

La surveillance des paiements entrants adopte une approche différente en identifiant les schémas et activités frauduleux cachés dans les fonds entrants.

Tout mettre bout à bout : Hypothèses pour un système financier plus sûr

Jane Smith, âgée de 65 ans, est ravie de son nouvel emploi de comptable dans une entreprise internationale d'antiquités. Son nouvel employeur dépose de l'argent sur son compte, ce qui lui permet de payer ses factures et d'envoyer des cartes-cadeaux à ses clients.

Pendant ce temps, **Anne** travaille pour la banque ABC, qui a récemment mis en place une surveillance des paiements entrants afin d'améliorer sa stratégie de détection des fraudes.

→ Surveillance des flux entrants

- **Anne remarque :** De nombreux dépôts inhabituels sont effectués sur le compte de Mme Smith par des personnes géographiquement dispersées. Ces transactions partagent les mêmes détails de paiement et les mêmes horodatages, ce qui suggère une automatisation ou un effort coordonné.

→ Surveillance des flux sortants

- **Anne enquête :** Mme Smith transfère de l'argent sur des comptes qui ont été ouverts récemment ou qui sont restés inactifs pendant un certain temps. Anne peut constater que Mme Smith n'a jamais utilisé ces comptes auparavant.
- **Biométrie comportementale :** Le comportement de connexion de Mme Smith ne pose pas de problème immédiat, car elle utilise des appareils et des lieux de confiance.

Collaboration et intervention

- **Anne relie les points :** Grâce à la surveillance des flux entrants et sortants, Anne peut suivre l'ensemble du cycle de vie des fonds. Elle observe un schéma dans lequel le compte qui dépose de l'argent sur le compte de Mme Smith en dépose également sur les comptes de trois autres femmes, toutes âgées d'environ 65 ans et vivant dans de petites villes du Royaume-Uni.

  Une enquête plus approfondie révèle que tous ces fonds sont finalement consolidés et transférés vers un ensemble de mauvais comptes connus au niveau international, ce qui témoigne d'une opération sophistiquée de fraude et de blanchiment d'argent. Consciente de la gravité de la situation, Anne prend des mesures immédiates.

  Elle prend contact avec Mme Smith et les trois autres victimes pour les informer qu'elles sont victimes d'une escroquerie. Au cours de ses entretiens, Anne leur indique comment éviter de telles escroqueries à l'avenir et prend des mesures pour bloquer tout nouveau paiement sur les comptes connus pour être frauduleux. Ce faisant, la banque ABC s'assure que toute nouvelle victime potentielle est immédiatement signalée au service des fraudes, ce qui permet d'éviter toute nouvelle exploitation.

- **Les menaces cachées sont dévoilées :** L'analyse combinée des données entrantes et sortantes révèle une opération sophistiquée dissimulée dans des transactions apparemment ordinaires.

- **Mesures prises :** Anne prend contact avec Mme Smith pour en savoir plus, confirmer ses soupçons et protéger Mme Smith. Anne signale également l'activité suspecte aux autorités, ce qui risque de perturber l'ensemble du réseau de blanchiment d'argent.

Prochaines étapes

- **Banque ABC :** Elle enquête sur les titulaires de comptes qui ont déposé de l'argent sur les comptes de Mme Smith et sur les comptes sur lesquels elle a transféré l'argent. Elle partage ces informations avec d'autres institutions financières.

- **Autorités :** La banque ABC signale l'activité frauduleuse et le réseau connecté aux autorités pour enquête et poursuites éventuelles.

Impact sur les clients

Mme Smith est reconnaissante à sa banque pour son intervention et sa protection. Cette expérience, qui aurait pu être source de frictions, a fait d'elle une cliente fidèle, qui le restera toute sa vie.

Au-delà de la détection : Des expériences plus rapides et sans friction

La prévention de la fraude a trop longtemps été synonyme de retards et de désagréments, même pour les clients légitimes. La surveillance avancée des paiements entrants change la donne. Grâce à l'analyse proactive des fonds entrants, les banques peuvent identifier en toute confiance les fraudes potentielles et valider les transactions à faible risque. Cela présente plusieurs avantages d'une grande portée :

Disponibilité plus rapide des fonds

La surveillance des flux entrants permet d'accélérer la confirmation et le déblocage des fonds pour les particuliers ou les entreprises en attente d'un dépôt, ce qui améliore l'expérience globale du client.

Fidélisation et satisfaction

L'élimination des blocages inutiles renforce la confiance et la réputation d'une banque en tant que partenaire centré sur le client, et non en tant qu'obstacle.

Amélioration de l'offre de produits

L'identification avec certitude des « bons » fonds entrants donne aux banques une plus grande flexibilité pour offrir des comptes à primes, des limites de dépenses plus élevées et des produits financiers spécialisés avec des préoccupations minimales en matière de risque. Cela crée de nouvelles opportunités de revenus.

L'amélioration de la visibilité des paiements entrants ne permet pas seulement d'arrêter les malfaiteurs. Elle transforme les bonnes expériences des clients en une institution financière plus forte et plus rentable.

Grâce à l'analyse proactive des fonds entrants, les banques peuvent identifier en toute confiance les fraudes potentielles et valider les transactions à faible risque.

Des idées à l'action

1 Étape exploratoire

Même si elle n'est pas prête à être mise en œuvre immédiatement, cette proposition constitue un bon point de départ pour une discussion interne. Questions à examiner :

- **Lacunes actuelles en matière de détection :** Peut-on dresser une carte des capacités actuelles de classification des fraudes et des escroqueries ? Y a-t-il des points faibles évidents à corriger ?
- **Limites opérationnelles :** Existe-t-il la technologie et les capacités humaines nécessaires pour adapter l'approche progressive mentionnée dans l'ebook ?
- **Implications pour le service client :** Comment la surveillance des flux entrants ET sortants pourrait-elle modifier la manière dont les services traitent certaines enquêtes ? Le personnel aurait-il besoin d'être mis à niveau et formé à cette vision élargie ?

2 Planification du projet pilote

Si l'on souhaite mettre en place un projet pilote de surveillance des flux entrants, cette section sert de liste de contrôle préliminaire. Les actions clés sont les suivantes :

- **Détermination du champ d'application :** Décider quel flux est le plus approprié pour le lancement – comptes à haut risque, cartes, paiements rapides, etc.
- **Métriques de réussite :** Déterminer les indicateurs qui permettront de valider et de démontrer le retour sur investissement avant un déploiement à grande échelle, même à petite échelle.

3 Consultation des fournisseurs

Il est essentiel d'étudier les partenariats susceptibles de renforcer cette stratégie. Concentrez-vous sur les points suivants :

- **L'alignement sur le secteur :** Les modèles analytiques fournis par les fournisseurs sont-ils conformes aux protocoles de classification des fraudes reconnus par le secteur ?
- **Intégration :** Comment les nouvelles solutions s'intègrent-elles à l'architecture de détection de la fraude déjà en place dans une banque ?

L’avenir des paiements

La capacité d’adaptation est primordiale pour l’avenir des paiements. Les stratégies de détection de la fraude les plus efficaces de demain doivent aller au-delà des approches cloisonnées et adopter une analyse holistique.

S’appuyer uniquement sur les schémas de paiement sortants crée une vision étroite des menaces de fraude dans tous les canaux de paiement. Cet angle mort expose les banques (et leurs clients) à des pertes inutiles dues à la fraude et à des coûts opérationnels qui pourraient être évités si les paiements entrants étaient également surveillés. L’analyse conjointe des flux de données entrants et sortants permet aux responsables de la lutte contre la fraude d’identifier les vitesses suspectes, les anomalies et les menaces cachées, afin de limiter les pertes potentielles et de protéger le système financier.

Pour y parvenir, la détection des fraudes doit intégrer les éléments clés suivants :

Analyse des données en temps réel grâce à l’apprentissage automatique

Les systèmes doivent traiter les transactions en quelques millisecondes et s’adapter à l’évolution des tactiques.

Évaluation holistique des risques sur tous les canaux de paiement

Les clients effectuent des paiements entre les banques et les applis, ce qui nécessite une vue connectée de l’activité pour la détection des fraudes.

Collaboration des données internes et externes

Tirer des enseignements des systèmes bancaires, des commerçants, des sociétés de traitement des paiements et même des flux de réseaux sociaux permettra d’enrichir les modèles de détection.

Les fraudeurs opèrent en temps réel et à travers les écosystèmes. Les banques qui relèvent le défi grâce à une surveillance adaptative, multiforme et vigilante des flux entrants et sortants se protégeront et serviront mieux leurs clients dans un paysage des paiements en évolution rapide.

feedzai

Plus de confiance, moins de criminalité.

Solutions en matière de fraude et de criminalité financière

Feedzai est la première plateforme RiskOps au monde, protégeant les personnes et les paiements grâce à une suite complète de solutions basées sur l'IA conçues pour mettre fin à la fraude et à la criminalité financière.

Les plus grandes institutions financières mondiales font confiance à Feedzai pour protéger des milliards de dollars de transactions et gérer les risques tout en améliorant l'expérience client.

Identité | Gestion de la fraude en entreprise | Lutte contre le blanchiment d'argent

Demandez une démo

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