La fraude en pleine crise d'identité

Comment les comptes vérifiés, les comportements d’apparence anodine et l'IA alimentent la fraude en 2026.

adyen

Sommaire

Méthodologie

Pour ce rapport, nous avons extrait des données de transaction 2025 de la plateforme Adyen (1,6 trillion de dollars US de données), et nous avons également interrogé 1000 décideurs de grandes entreprises marchandes américaines.

Les données d'enquête sont indiquées par Adyen survey.
Les données de plateforme sont indiquées par Adyen platform data.

Contributeurs

JEFF HALLENBECK
VP OF CUSTOMER ADVOCACY, ADYEN

KATIE SUSKIND
GLOBAL HEAD OF POLICY, ADYEN

BRIGETTE KORNEY
GLOBAL HEAD OF PERFORMANCE OPTIMIZATION, ADYEN

JON SHEINFELD
SR. PRODUCT MANAGER, ML/AI, ADYEN

ANDREA FERRARI
SR. PRODUCT MANAGER, FRAUD MANAGEMENT, ADYEN

Avant-propos

« Les entreprises qui réussissent le mieux dans cet environnement ne sont pas celles qui imposent les contrôles les plus stricts. Ce sont celles qui choisissent avec plus de discernement où et comment les appliquer. »

JEFF HALLENBECK
VP OF CUSTOMER ADVOCACY, ADYEN

La fraude a toujours fait partie du commerce. Ce qui a changé, c'est là où elle se dissimule.

Pendant la majeure partie de la dernière décennie, le modèle de travail des équipes risques était relativement simple : signaler ce qui sort de l'ordinaire. Nouveaux appareils, localisations inhabituelles, identifiants suspects. Cette logique reste valable pour ce qu'elle a été conçue à détecter. Mais la fraude qui progresse le plus vite aujourd'hui ne déclenche souvent aucun de ces signaux. Elle vient de comptes vérifiés, d'appareils reconnus, de comportements qui franchissent chaque point de contrôle.

Chez Adyen, nous traitons des paiements dans les plus grands environnements commerciaux au monde. Ce que nos données révèlent, c'est un changement dans la façon dont le risque se comporte. La fraude est devenue automatisée et de plus en plus difficile à détecter. Dans de nombreux cas, elle ressemble à une activité client parfaitement légitime lorsqu'on regarde uniquement la transaction, sans prendre en compte son contexte.

Cela crée un défi d'un genre nouveau pour les équipes risques : une mauvaise décision a un impact commercial immédiat. Un problème qui ne peut pas être résolu en durcissant les contrôles, d'autant que ce sont souvent ces mêmes contrôles qui sont exploités.

Il nous faut une approche différente, une approche qui reflète la façon dont l'identité et le risque se comportent réellement. Plutôt que de traiter l'identité comme une donnée vérifiée une fois pour toutes et censée rester stable, nous devons la voir comme un signal continu, qui évolue dans le temps et nécessite une interprétation constante. Tout aussi important : nous devons reconnaître que les faux refus ne sont pas simplement une nuisance opérationnelle, mais un coût réel pour l'entreprise, avec des conséquences qui méritent d'être évaluées aussi sérieusement que les pertes liées à la fraude.

Ce rapport examine comment cette évolution se manifeste : là où la fraude devient plus difficile à détecter, pourquoi les défenses conventionnelles peinent à suivre, et ce que font différemment les organisations qui s'en sortent bien. La deuxième partie ira plus loin dans la façon dont cette approche se traduit en infrastructure et en stratégie.

Résumé exécutif

Dans le commerce d'entreprise, la fraude ne se présente plus comme une série d'incidents isolés. Elle suit désormais des schémas automatisés et reproductibles, constamment testés, ajustés puis réutilisés dans différents environnements.

Le résultat, c'est non seulement plus de fraudes, mais une fraude conçue pour se fondre dans les comportements clients légitimes. Cette évolution change la nature du risque, la manière de le gérer et le coût qu'il représente lorsqu'il n'est pas maîtrisé.

Ce rapport identifie cinq thèmes qui définissent la stratégie anti-fraude en 2026. Les chapitres 1 à 3 établissent la nature et l'ampleur de ces évolutions. Les chapitres 4 et 5 examinent comment les organisations leaders y répondent (et là où se trouvent désormais les plus grands leviers d'action).

Les entreprises qui prennent de l'avance ne sont pas celles qui ont les contrôles les plus stricts.

Ce sont celles qui ont les contrôles les plus précis.

Cinq tendances qui façonnent la fraude en 2026

01

La fraude est devenue systématique

L'automatisation a transformé la fraude en un cycle continu de test et d'apprentissage.

Les tactiques sont déployées, affinées en temps réel et rapidement mises à l'échelle, les approches réussies étant reproduites dans différents environnements et cibles.

02

Les bons clients ont appris à contourner le système

Les fraudes commises par les clients eux-mêmes et les abus de politique s'insèrent de plus en plus dans des parcours clients légitimes. Les marchands ne doivent plus seulement vérifier l'identité, mais aussi comprendre l'intention derrière chaque action.

03

La précision stimule la croissance

Le coût de la lutte contre la fraude se mesure de plus en plus en valeur client perdue, pas seulement en pertes évitées. Les faux refus, la hausse des coûts de revue manuelle et les contrôles globaux freinent la croissance.

04

L'identité ne peut pas être un indicateur statique

Les vérifications ponctuelles ne sont plus suffisantes. La confiance se construit dans le temps grâce au comportement, à l'historique et à la reconnaissance entre sessions, appareils et environnements.

05

La confiance doit aller au-delà de la transaction

À mesure que les agents IA commencent à agir au nom des clients, la prévention de la fraude doit démarrer plus tôt, avec les systèmes qui régissent le comportement avant que le paiement ait lieu.

CHAPITRE / 1

Le nouveau visage de la fraude

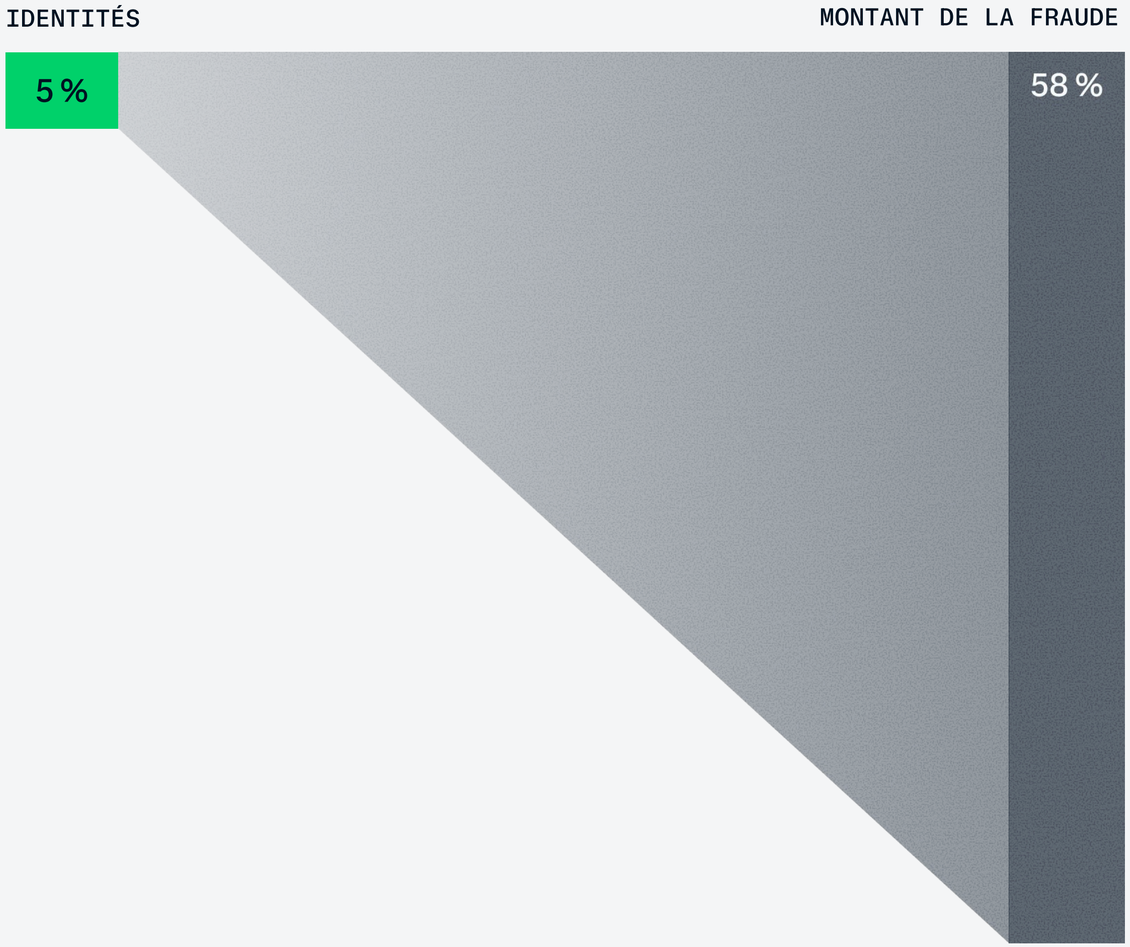
La fraude n’est pas nouvelle. Mais elle n’est plus détectable d’emblée.

Aujourd’hui, les comportements à l’origine de la fraude semblent souvent légitimes au moment de la transaction : un client habituel sur un appareil reconnu. Le schéma ne devient clair qu’avec le temps, à travers les comptes et les interactions.

CHIFFRES CLÉS

SOURCE : PLATEFORME ADYEN

Une minorité d'identités concentre la majorité du montant de la fraude



L'ère du test-and-learn de la fraude

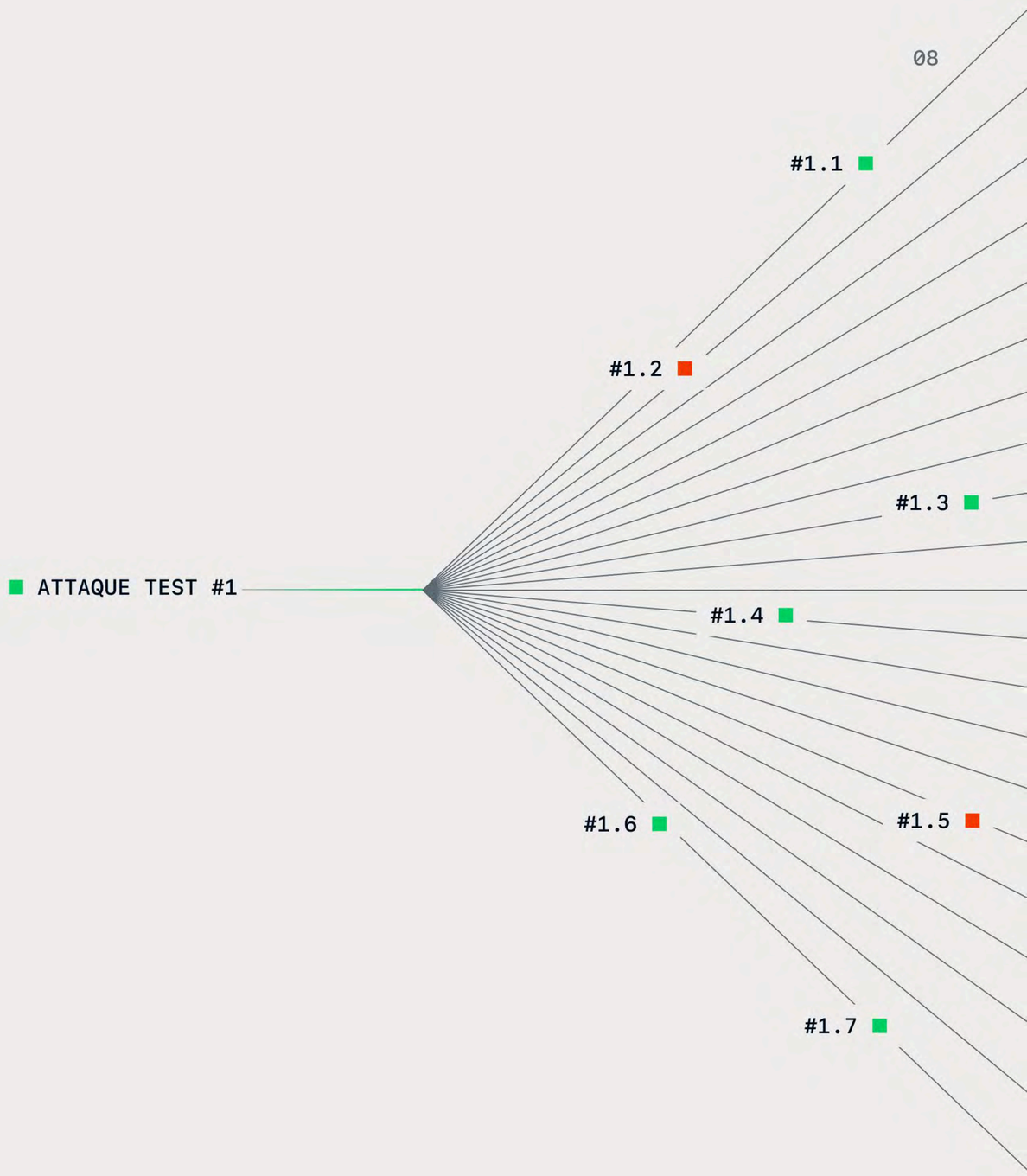
La fraude s'adapte désormais et fonctionne en cycle continu : les tactiques sont déployées et affinées en temps réel. Ce qui marche est répété, ce qui ne marche pas est rapidement abandonné.

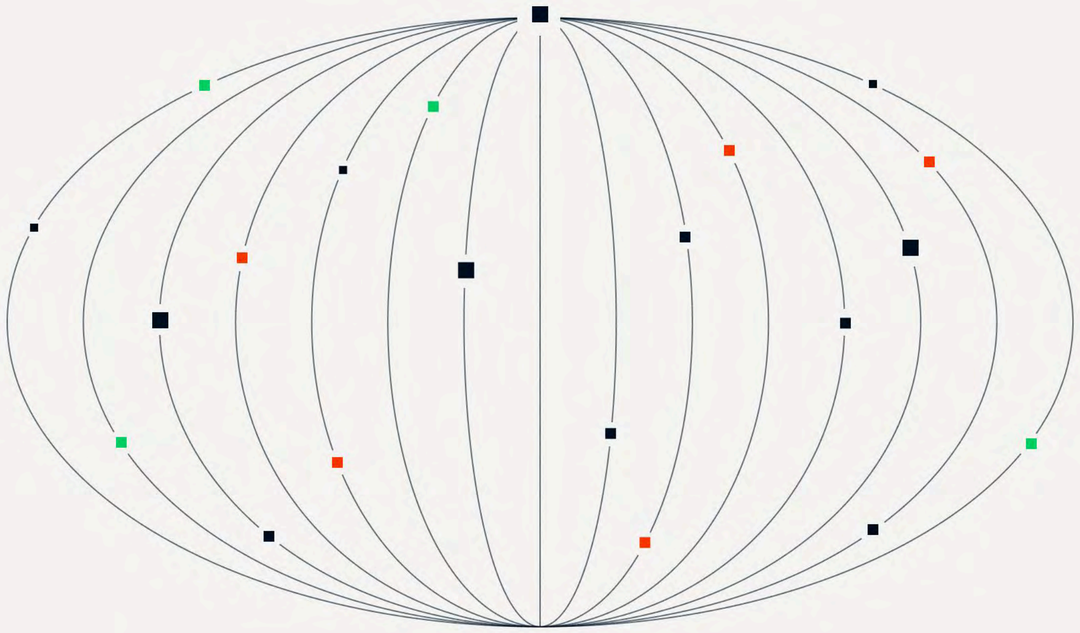
Plutôt que de tester une seule approche, les attaquants peuvent lancer des milliers de variations simultanément (en ajustant les informations d'identité, les moyens de paiement, la vitesse au checkout ou les montants de transaction) pour observer les résultats obtenus.

L'automatisation permet à ces attaques de se répéter en continu, en reproduisant ce qui fonctionne et en l'optimisant en temps réel. Chaque résultat alimente le suivant : autorisations, refus et activités en aval servent à ajuster les tentatives suivantes, jusqu'à contourner les contrôles anti-fraude.

L'automatisation et l'IA ne créent pas ces schémas. Elles les rendent plus rapides, plus constants et plus faciles à déployer à grande échelle.

En parallèle, l'automatisation et l'IA transforment la nature de la fraude. Elles permettent aux fraudeurs de renforcer des identités synthétiques à l'aide de deepfakes, de faux documents et d'autres techniques conçues pour contourner les contrôles de vérification classiques.





La fraude touche tout le monde

Parce que ces attaques sont désormais si faciles à automatiser et à déployer en nombre, les fraudeurs ne ciblent plus seulement les plus grandes plateformes. Les entreprises de toutes tailles, de tous secteurs, de toutes régions peuvent se retrouver exposées aux mêmes menaces, exécutées avec la même vitesse et la même précision. Les fraudeurs ne respectent ni les frontières entre marques ni les segmentations sectorielles ; une fois qu'ils ont découvert une faille chez un marchand, cette vulnérabilité est rapidement testée et exploitée chez tous les autres.

En pratique, cela signifie qu'un même schéma de fraude peut apparaître simultanément dans plusieurs environnements. Un script utilisé pour tester des numéros de carte sur une plateforme peut être répliqué sur une autre. Une même méthode d'abus promotionnel peut être appliquée à plusieurs marques. Et des données d'identité validées une première fois sont réutilisées jusqu'à ce qu'elles ne fonctionnent plus.

Le phénomène n'est pas nouveau, mais ce qui change aujourd'hui, c'est la vitesse et la capacité d'adaptation de ces tactiques, qui peuvent être réutilisées et ajustées en permanence.

Parce que ces schémas couvrent marchands, canaux et secteurs, les entreprises ayant accès à de plus grands ensembles de données de qualité sont mieux positionnées pour détecter et prévenir la fraude de manière proactive.

CAS CLIENT

Comment un retailer mondial de sport a détecté une fraude qui se cachait en pleine lumière

En août 2025, un retailer mondial de sport semblait vivre un mois record, avec des activations de cartes-cadeaux en hausse de plus de 1 000 %. En réalité, le marchand subissait une attaque de fraude coordonnée. Des milliers de bots automatisés imitant de vrais acheteurs testaient des numéros de cartes-cadeaux à grande échelle et en vidaient les soldes. Les pertes ont dépassé 750 000 $ avant que l'attaque ne soit contenue.

Parce que son système de détection ne signalait les transactions qu'après autorisation, le retailer a été touché deux fois : des revenus perdus à cause de la fraude, et des frais de traitement sur chaque transaction frauduleuse.

En passant à un modèle de détection avant autorisation, le retailer a réduit le volume de trafic suspect et a pu se concentrer sur ce qui restait.

Une fois le bruit réduit, un schéma clair est apparu : les mêmes signaux d'appareils, tous liés à des modèles d'iPhone obsolètes, revenaient de façon répétée d'une transaction à l'autre. Une règle ciblée a stoppé l'attaque en une semaine.

La fraude se redistribue

Au lieu d'être concentrée sur un petit nombre de transactions à forte valeur, la fraude s'est élargie aux activités à faible valeur, l'automatisation ayant facilité la mise à l'échelle.

Cela modifie les exigences envers les systèmes anti-fraude. Les contrôles conçus pour des événements isolés à haut risque font face à un flux continu d'activité, augmentant à la fois le volume de décisions et l'ambiguïté entre comportements légitimes et abusifs.

L'impact va au-delà des pertes liées à la fraude. Il se traduit par une hausse des coûts de revue manuelle, une augmentation des faux refus et des opportunités de revenus manquées.

Le prix d'une mauvaise décision

Près de 70 % des entreprises interrogées s'attendent à ce que la fraude et les abus limitent leur capacité à augmenter leur chiffre d'affaires. Plus de la moitié signalent une hausse des coûts de revue manuelle.

Chaque décision anti-fraude est un arbitrage. Bloquer trop lâchement et la fraude passe. Durcir les contrôles trop agressivement, et les clients légitimes sont rejetés, juste au moment où ils souhaitent dépenser.

Alors que 50 % des entreprises signalent une augmentation des faux refus, le coût de la prudence devient visible. Les transactions légitimes sont bloquées, l'expérience client se dégrade et le chiffre d'affaires est perdu.

À grande échelle, ces décisions s'accumulent et la fraude devient une pression continue sur la croissance.

70 %

des entreprises interrogées s'attendent à ce que la fraude et les abus freinent la croissance de leur chiffre d'affaires

SOURCE : ENQUÊTE ADYEN

CHAPITRE / 2

Utilisateurs connus, intention inconnue

La fraude ne concerne plus seulement les identités inconnues

Elle opère désormais à travers des identités et des interactions qui semblent légitimes.

Pendant des années, la détection de fraude s'est concentrée sur un ensemble restreint de questions : est-ce une vraie personne, et est-elle bien qui elle prétend être ? Ces questions restent pertinentes. Mais elles ne suffisent plus.

Le défi n'est plus seulement la vérification d'identité statique à un instant précis, mais la compréhension du comportement à mesure qu'il évolue tout au long du cycle de vie.

Le même compte ou appareil peut représenter un client authentique à un moment donné, puis un comportement abusif dans un autre. Par exemple, un nouveau compte lié à un vrai client, mais créé uniquement pour accéder à une nouvelle promotion, ou un achat légitime retourné plus tard sous un faux prétexte.

ÉCLAIRAGE

La fraude ne ressemble pas à du légitime par accident. Elle a choisi la légitimité comme stratégie. Le secteur a passé une décennie à améliorer la vérification d'identité, et ces fondations restent indispensables.

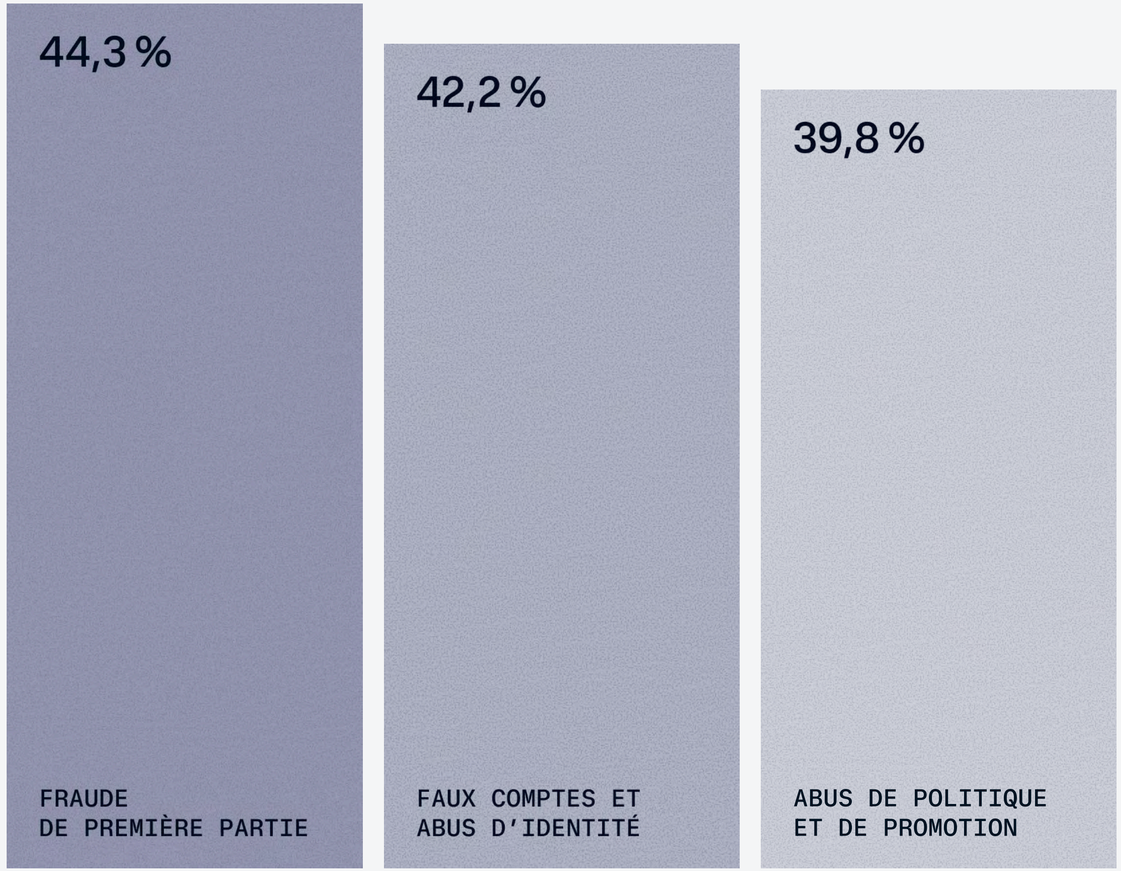
Mais à mesure que la fraude a évolué, le défi a évolué aussi. Lorsqu'un même client vérifié peut être à la fois votre client le plus précieux et votre source de perte la plus importante, l'identité seule ne suffit plus à évaluer le risque.

La prévention de la fraude doit donc passer des vérifications d'identité statiques à l'identité dynamique : des systèmes qui évaluent en continu si le comportement correspond à un usage attendu tout au long du cycle de vie. Ce changement dépasse la seule détection : il concerne la façon dont les entreprises gèrent le risque, en connectant identité, comportement et politique pour façonner les résultats dans le temps.

ANDREA FERRARI
SR. PRODUCT MANAGER,
FRAUD MANAGEMENT, ADYEN

SOURCE : ENQUÊTE ADYEN

Les types de fraude et d'abus les plus signalés



L'augmentation des abus à apparence légitime

Ce changement se reflète dans les types de fraudes auxquels les entreprises font maintenant face.

- **La fraude de première partie**, où les clients effectuent des achats légitimes puis les contestent auprès de leur banque, en invoquant la non-réception, des défauts ou une utilisation non autorisée, est aujourd'hui l'une des formes les plus courantes d'abus, signalée par 44,3 % des entreprises.
- **Les faux comptes et les abus d'identité** suivent de près, affectant 42,2 %, utilisés pour faire tourner des promotions, distribuer l'activité ou accéder à des offres spécifiques à certains segments.
- **Les abus de politique et de promotion,** où les clients exploitent directement les politiques des marchands via des retours en série, le wardrobing, la multiplication des essais gratuits, la collecte abusive de points de fidélité ou le cumul de remises au-delà de leur usage prévu, ne sont pas loin derrière avec 39,8 %.

La fraude commise par des clients légitimes s'est largement répandue, et ces abus sont réalisés sans usurper d'identité ni compromettre de compte. Du point de vue système, ces comportements paraissent souvent parfaitement valides. Ils passent les contrôles conçus pour détecter les accès non autorisés ou les moyens de paiement frauduleux.

Le défi n'est pas seulement d'identifier ces utilisateurs. C'est d'empêcher que l'abus se répète.

Exploiter les failles

Historiquement, la fraude se déplace là où les défenses sont les plus faibles. De l'exploitation des cartes physiques à l'ère de la piste magnétique, elle a migré vers le e-commerce. Aujourd'hui, elle revient progressivement au commerce physique. À mesure que les protections en ligne se sont renforcées, les attaquants s'adaptent en exploitant les failles du retail physique, où moins de signaux et des contrôles moins matures rendent les abus plus difficiles à détecter.

Ce schéma explique pourquoi des problèmes tels que l'abus de remboursement au point de vente (POS) émergent dans le cadre d'une redistribution plus large du risque.

20×

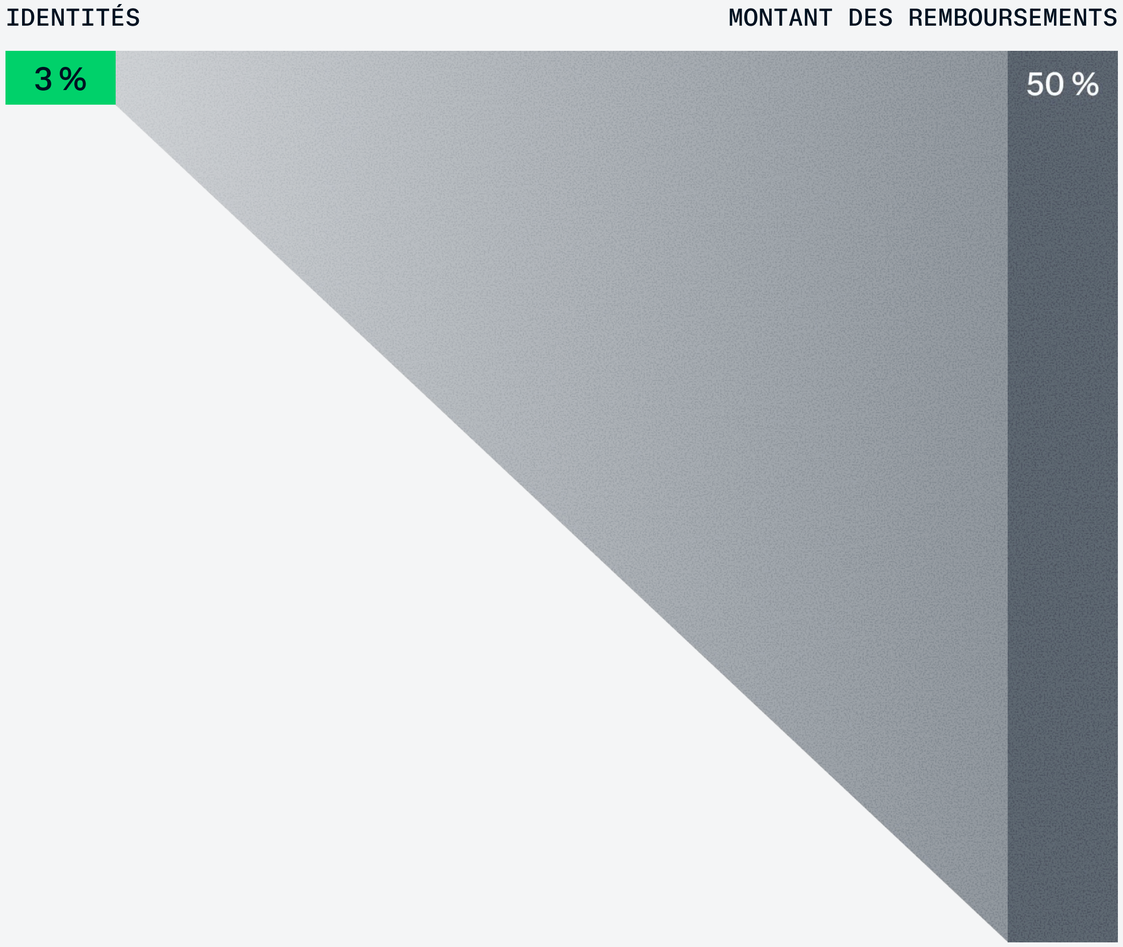
Pour chaque dollar perdu causé par des rétrofacturations frauduleuses, les commerçants traitent environ 20 $ de remboursements

SOURCE : PLATEFORME ADYEN

CHIFFRES CLÉS

SOURCE : PLATEFORME ADYEN

Une minorité d'identités concentre la moitié du montant des remboursements



TACTIQUE ÉMERGENTE

Remboursements non référencés vers des portefeuilles numériques

Fin 2025, un schéma de fraude reproductible a émergé chez des retailers américains, ciblant les flux de remboursement non référencés au point de vente.

Les fraudeurs exploitent des failles dans les processus de remboursement afin d'émettre des paiements vers des portefeuilles numériques. En contournant le flux standard, où les remboursements sont liés à une transaction d'origine, ils peuvent générer des fonds sans achat vérifié. Une fois les fonds versés, les possibilités de récupération sont très limitées.

Ces incidents se multiplient dans plusieurs points de vente et surviennent généralement dans des environnements aux politiques de remboursement plus souples, avec des pertes allant de 10 000 $ à 90 000 $.

La tactique repose sur une apparence légitime. Les attaquants s'approchent du personnel pendant les périodes de forte activité, en usurpant une identité ou en falsifiant des détails de transaction, pour faire passer des remboursements en dehors des protocoles standard.

Dans ces cas, la vulnérabilité ne réside pas uniquement dans le système, mais aussi dans la façon dont il est utilisé en pratique. Les autorisations au niveau du magasin permettent des remboursements non référencés, sans validation ni escalade suffisante, tandis que la pression de maintenir une expérience client fluide rend plus difficile de contester les demandes.

Ces attaques exposent une faiblesse en amont même du paiement. Dans de nombreux cas, le facteur décisif est la façon dont les flux de remboursement fonctionnent sous pression, notamment pendant les périodes de forte activité.

Réduire le risque nécessite des contrôles plus stricts au niveau du magasin : autorisations resserrées, flux d'approbation clairs et sensibilisation continue du personnel à l'identification des comportements suspects. Il est tout aussi important de s'appuyer sur un partenaire de paiement capable d'identifier rapidement les schémas, d'escalader les alertes et de contenir les pertes avant qu'elles ne s'étendent.

Zone grise : quand les bons clients adoptent les mauvais comportements

Tous les abus ne naissent pas d’une intention malveillante.
Dans de nombreux cas, ils sont simplement stimulés par des effets d'aubaine.

Une offre de bienvenue incite naturellement aux inscriptions multiples.
Une politique de retour trop généreuse minimise le coût de l'abus. Quant aux essais gratuits, ils finissent par être cumulés en boucle plutôt que d'être perçus comme un avantage ponctuel. Avec le temps, ces comportements autrefois marginaux finissent par se normaliser.

Sur Internet, des communautés partagent ouvertement des astuces pour « contourner » les règles, qu'il s'agisse de maximiser les codes promotionnels ou d'automatiser les demandes de remboursement.

Ce qui s'apparente à de la fraude est alors requalifié en « astuce », en « hack » ou en simple optimisation. Ainsi, des clients qui ne se considèrent pas du tout comme des fraudeurs adoptent des comportements qui génèrent de lourdes pertes pour les marchands.

Pour les entreprises, cette réalité rend le problème complexe à identifier, et plus encore à résoudre. C’est tout l’enjeu de cette zone grise.

Le défi ne vient pas d'un manque de données. Prise isolément, aucune transaction ne semble suspecte ; le schéma frauduleux n’apparaît qu'en analysant la répétition des actions.

DONNÉES CLÉS

SOURCE : ENQUÊTE ADYEN

Les abus de politique et de promotion les plus communs

CAS CLIENT

Filtrer les abus aux essais gratuits pour sécuriser les revenus récurrents

Début 2025, un leader mondial du logiciel a fait face à une recrudescence des abus liés à ses offres d'essai. De nombreux utilisateurs s’inscrivaient sans la moindre intention de passer à l'offre payante, en utilisant bien souvent des moyens de paiement invalides ou non provisionnés. L'entreprise ne constatait malheureusement le problème que trop tard, au moment où le premier cycle de facturation échouait.

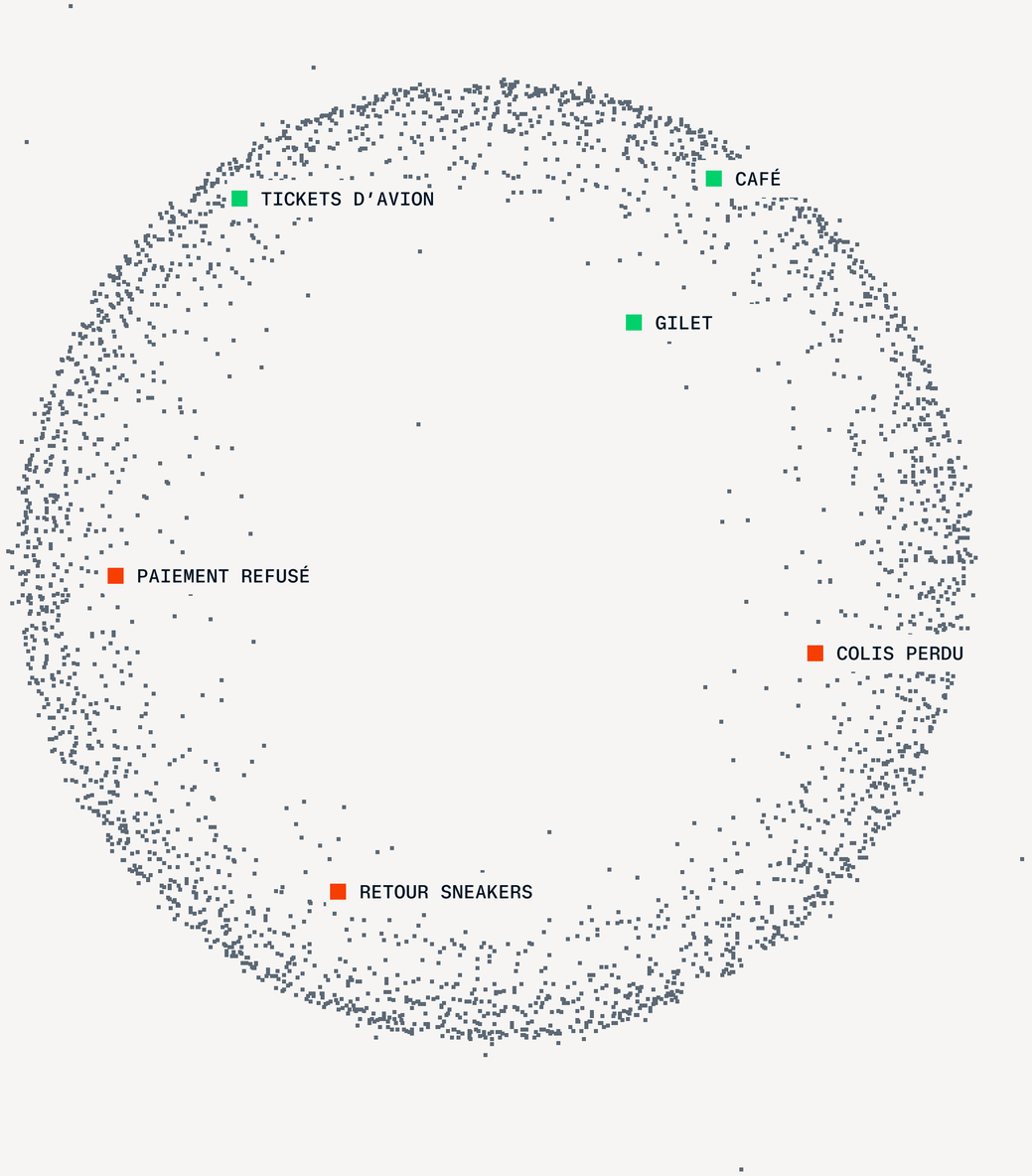
Le problème ne se situait pas au moment du renouvellement, mais apparaissait dès l’inscription.

L’entreprise a donc collaboré avec Adyen pour intégrer la validation plus tôt dans le parcours client. Plutôt que de s'appuyer sur des contrôles rudimentaires – visant simplement à vérifier l'existence d’un numéro de carte –, elle a mis en place une vérification en amont des moyens de paiement dès le début de la période d'essai.

Cette approche a permis de s'assurer que le mode de paiement fourni pourrait couvrir le montant de l’abonnement futur, sans pour autant débiter le client pendant sa période de test.

Ainsi, les cartes invalides, les soldes insuffisants et les profils à risque ont été écartés avant même l’ouverture des accès, tandis que les utilisateurs légitimes continuaient de bénéficier d’un parcours d'inscription fluide.

Ce changement a considérablement renforcé la sécurité sans générer de friction inutile. La qualité des leads à l'inscription s'en est trouvée grandement améliorée, consolidant par la même occasion la base d’abonnés. Au final, les taux de conversion et de rétention ont progressé, offrant une meilleure prévisibilité des revenus.



De l'identité à l'intention

Les systèmes anti-fraude traditionnels reposent essentiellement sur la vérification de l'identité et du moyen de paiement. Ils contrôlent les identifiants, authentifient les utilisateurs et évaluent la légitimité d'une transaction à partir de critères historiques connus. Pourtant, lorsqu'une seule et même identité peut dissimuler à la fois des comportements légitimes et des pratiques abusives, ces indicateurs isolés perdent de leur fiabilité.

Dès lors, l'enjeu ne se résume plus à savoir « Qui achète ? », mais plutôt à déterminer si le comportement observé est cohérent avec un usage légitime sur la durée.

CHAPITRE / 3

La précision comme moteur de croissance

Il devient de plus en plus difficile de distinguer la fraude de l’activité légitime

Le coût d’une mauvaise décision peut rapidement dépasser la perte liée à la fraude elle-même. En réalité, une infime minorité d’utilisateurs représente une part disproportionnée du risque. Pourtant, les contrôles restent appliqués bien trop largement.

En voulant bloquer les abus de quelques-uns, les entreprises imposent une friction qui pénalise l'ensemble de leurs clients.

Le véritable coût de la fraude ne se mesure pas seulement aux transactions frauduleuses acceptées, mais surtout aux ventes légitimes bloquées. Selon les données de la plateforme Adyen, les contrôles statiques rejettent par erreur jusqu’à 10 % des bons clients.

Les faux positifs, la friction inutile et l'explosion des coûts liés aux vérifications manuelles impactent ainsi directement le chiffre d’affaires.

Historiquement, la plupart des stratégies anti-fraude visaient uniquement à minimiser les pertes. Ce modèle est désormais obsolète.

CHIFFRES CLÉS

SOURCE : ENQUÊTE ADYEN

La fraude, un impôt sur la croissance

70 %

DES ENTREPRISES INTERROGÉES ESTIMENT QUE LA FRAUDE ET LES ABUS VONT LIMITER LEUR CROISSANCE

Et cet impôt s'alourdit dans tous les secteurs

79 %

DANS LE VOYAGE ET L’HÔTELLERIE

81 %

DANS LES BIENS NUMÉRIQUES ET LE GAMING

SOURCE : ENQUÊTE ADYEN

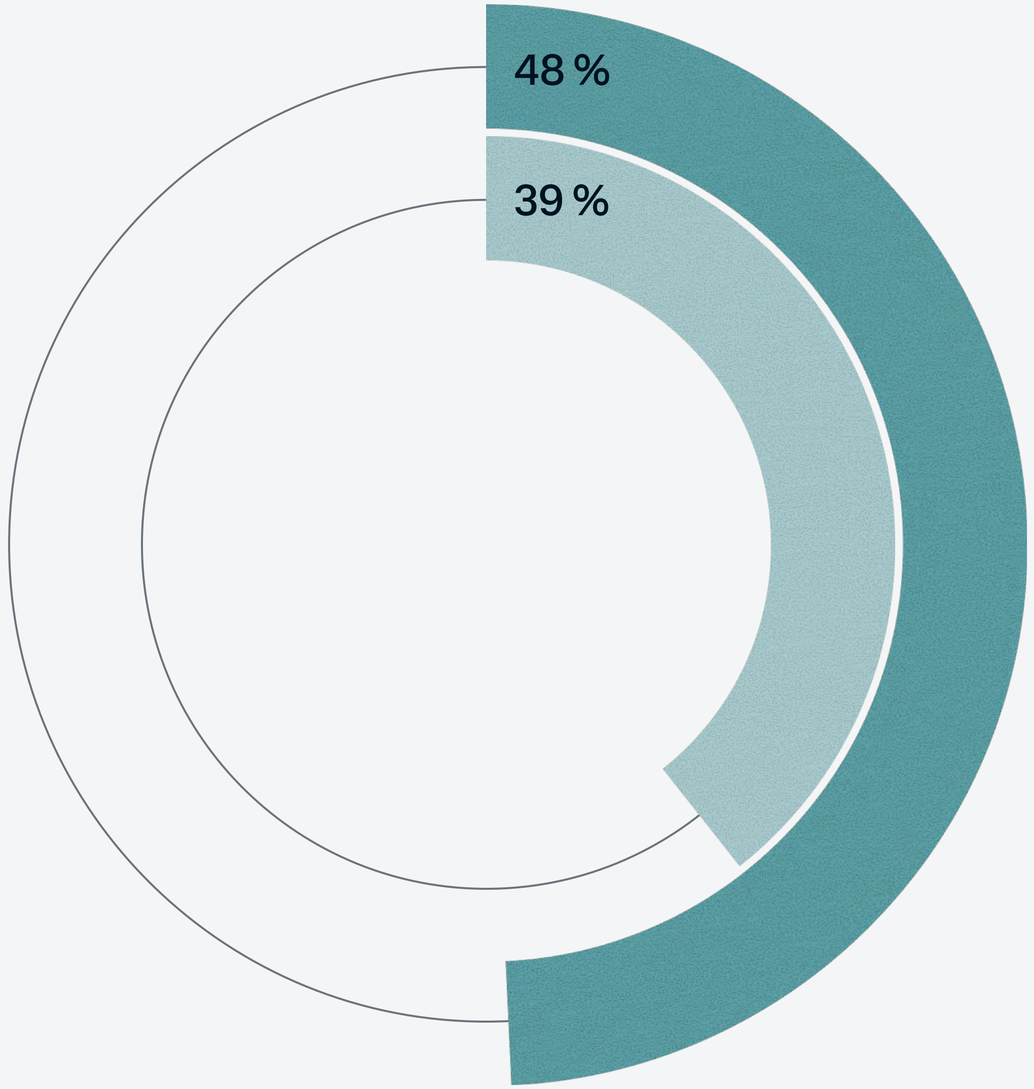
Les entreprises font déjà évoluer leur approche

Notre étude montre d'ailleurs que les entreprises sont déjà en train de redéfinir leur approche du risque :

- **48 %** conçoivent désormais la gestion de la fraude comme un équilibre permanent entre prévention des pertes et croissance.
- **39 %** la considèrent avant tout comme un levier au service de la croissance.

Gérer la fraude est de moins en moins perçu comme une contrainte technique, et de plus en plus comme un ensemble de décisions stratégiques qui déterminent, en fin de compte, la part de revenus légitimes qu'une entreprise est capable de capter.

Désormais, la question n'est plus de savoir quel volume de fraude une entreprise est prête à tolérer, mais plutôt quelle part de revenus légitimes elle accepte de sacrifier pour tenter de la stopper.



L'impératif de contrôles plus précis

Face à la recrudescence de la fraude, durcir les contrôles semble être la réponse la plus évidente. Pourtant, multiplier les règles, ajouter des étapes de vérification, intensifier les revues manuelles ou durcir les politiques ne fait qu'alourdir les coûts et générer de la friction.

L'impact se fait déjà ressentir sur le marché. Selon les données du MRC, la réduction des coûts opérationnels est devenue la priorité absolue pour 29 % des marchands en 2025, contre seulement 10 % en 2024.

Notre étude confirme cette tendance : 58 % des entreprises font face à une hausse des coûts liés aux vérifications manuelles, tandis que 50 % signalent une augmentation de leurs taux de faux positifs (ou faux refus). Ces contrôles supplémentaires reposant souvent sur des critères statiques, jusqu'à 10 % des clients légitimes se retrouvent ainsi bloqués.

Un véritable décalage s'est créé entre le risque perçu et la réalité. En voulant se prémunir contre une minorité de fraudeurs ciblés, les entreprises s'imposent des coûts et de la friction inutiles. Chaque faux positif ne se contente pas de bloquer une vente à l'instant T : il fragilise la confiance, nuit à la rétention et compromet les achats futurs. Au final, cela revient à pénaliser vos clients les plus précieux.

ÉCLAIRAGE

SOURCE : PLATEFORME ADYEN

Face à des politiques trop rigides, l'expérience client trinque

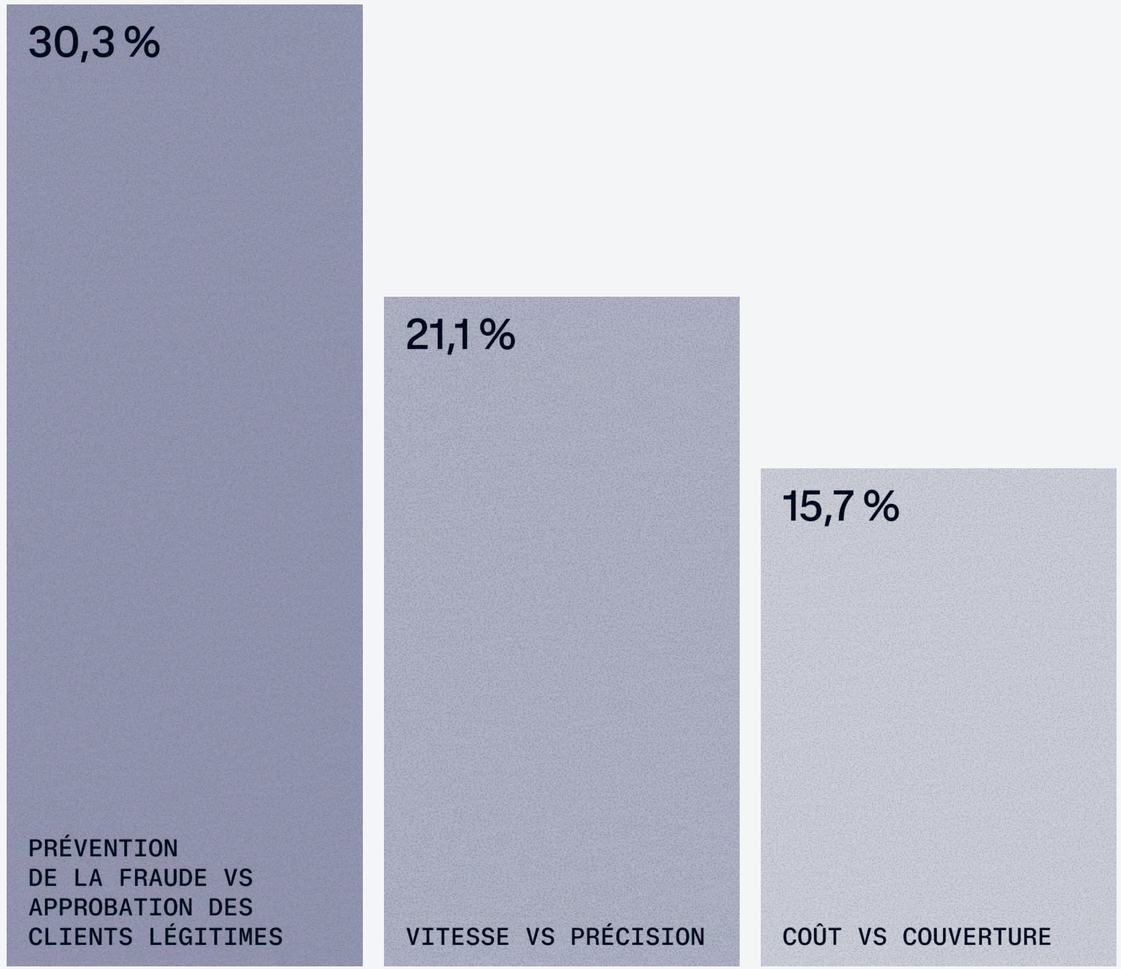
Dans les secteurs de la mode et du luxe, les marchands ont réduit leurs taux de remboursement de 21 à 25 % en 2025, sans pour autant constater une hausse des litiges. En proposant des alternatives comme l'échange ou l'avoir, ils ont réussi à préserver la confiance des acheteurs tout en protégeant leurs marges.

Le scénario est bien différent dans le secteur des sites de rencontres. Une baisse de 38 % des taux de remboursement y a provoqué une explosion de 66 % des contestations de paiement (chargebacks). Faute d'alternatives, les utilisateurs n'ont eu d'autre choix que de contester la transaction.

Si le durcissement des politiques permet de limiter les abus, il montre vite ses limites. Sans options de repli claires, il fragilise la relation avec les clients légitimes et les pousse directement à initier une procédure d'impayé.

SOURCE : ENQUÊTE ADYEN

Les compromis les plus courants en prévention de la fraude



Une quête permanente d'équilibre

Pour la plupart des entreprises, la gestion de la fraude est un exercice d'équilibriste. Selon notre étude, 96,8 % d'entre elles ont dû faire au moins un compromis majeur dans ce domaine au cours de l'année passée.

96,8 %

des entreprises ont fait au moins un compromis lié à la fraude l'an passé

SOURCE : ENQUÊTE ADYEN

ÉCLAIRAGE

Quelle est la meilleure stratégie anti-fraude ?

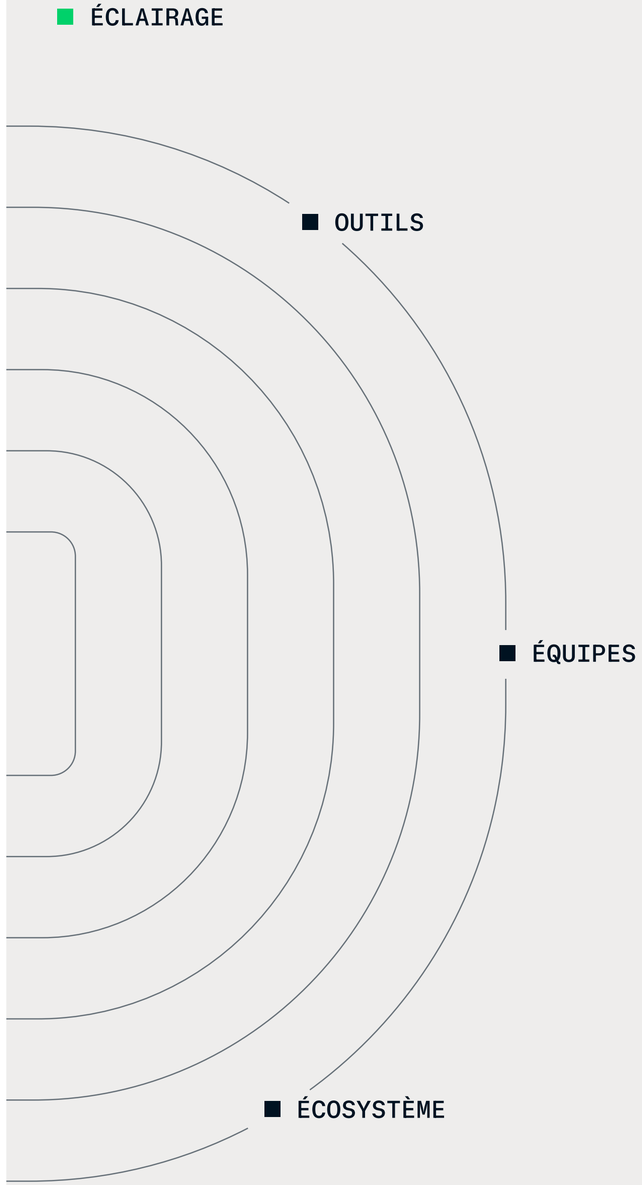
La réponse la plus honnête est pourtant celle que la plupart des entreprises redoutent : tout dépend.

La prévention de la fraude dépasse le cadre de la simple conformité réglementaire. Chaque approche implique de trouver le juste équilibre entre risque, friction, coût et croissance. En réalité, votre stratégie doit s'aligner sur votre modèle économique. Voici les questions clés à vous poser :

- **Votre profil de marge.** Les entreprises dotées de marges élevées peuvent se permettre d'absorber une part de risque plus importante pour maximiser la conversion. À l'inverse, celles qui opèrent sur de faibles marges ont besoin de contrôles plus stricts, mais ne peuvent assumer ni le coût d'une friction généralisée, ni celui d'une révision manuelle intensive.
- **Vos priorités de croissance.** Une entreprise axée sur l'acquisition de nouveaux clients n'arbitrera pas de la même manière qu'une structure cherchant à optimiser la rétention et la valeur vie client (LTV). Votre stratégie anti-fraude doit impérativement s'adapter à ces objectifs.
- **Votre mix client.** Tous les profils n'affichent ni la même valeur, ni le même niveau de risque. C'est souvent là que les stratégies échouent : en appliquant les mêmes contrôles à un nouvel acheteur et à un client fidèle à forte valeur.

Les équipes rencontrent des problèmes quand une stratégie conçue dans un contexte spécifique est appliquée partout, sur tous les marchés, segments et étapes du cycle de vie. Avec le temps, cela génère des coûts additionnels : des taux d'approbation plus faibles, des revues manuelles accrues et de la friction là où elle ne devrait pas être. L'objectif n'est pas d'éliminer le risque, mais d'aligner risque et friction là où ils créent ou détruisent de la valeur.

BRIGETTE KORNEY
GLOBAL HEAD OF PERFORMANCE OPTIMIZATION, ADYEN



Ce que cela signifie en pratique

Bien gérer ces arbitrages repose sur trois piliers fondamentaux :

- **L'agilité de vos outils.** Pour faire face à l'évolution constante de la fraude, les règles statiques ne suffisent plus. Vous devez vous appuyer sur des solutions capables de s'adapter en temps réel, que ce soit pour renforcer la protection sur les zones à haut risque ou pour évaluer la légitimité des transactions avec une précision chirurgicale.
- **L'expertise de vos équipes.** La gestion du risque gagne en efficacité lorsqu'elle sort de son silo. En collaborant avec des spécialistes, en partageant les données en interne et en optimisant vos processus en continu, vous transformez une simple stratégie théorique en un moteur de performance concret.
- **La force de votre écosystème.** Les fraudeurs ne s'attaquent jamais à une seule entreprise. Pour garder une longueur d'avance, la clé réside dans la mutualisation : partage des signaux faibles, exploitation des analyses sectorielles et suivi des grandes tendances à l'échelle mondiale à travers l'ensemble du réseau.

BRIGETTE KORNEY
GLOBAL HEAD OF PERFORMANCE OPTIMIZATION, ADYEN

De la lutte contre la fraude à la stratégie de croissance

La prévention de la fraude n'est plus un simple outil de contrôle.

Lorsqu'ils sont trop globaux, les contrôles augmentent les coûts, nuisent à la conversion et entachent la confiance des utilisateurs. En revanche, s'ils sont ciblés avec précision, ils deviennent un véritable levier de croissance : ils améliorent les taux d'approbation, éliminent la friction inutile et protègent la valeur client à long terme.

L'objectif n'est plus de réagir à des transactions isolées, mais de comprendre les schémas comportementaux. Il ne s'agit pas d'appliquer des blocages uniformes, mais de cibler précisément là où le risque est réel.

Reste à savoir, concrètement, ce que cela implique.

« Le vrai défi n'est plus d'identifier le risque, mais d'allouer le niveau de friction adéquat avec suffisamment de précision pour protéger la marge, sans freiner la croissance. »

JEFF HALLENBECK
VP OF CUSTOMER ADVOCACY, ADYEN

CHAPITRE / 4

L’identité dynamique comme infrastructure

Si les contrôles classiques n'arrivent plus à faire le distingo entre un client et un fraudeur, que faire ?

Les chapitres précédents ont décrit un environnement de fraude dans lequel l'une des plus grandes menaces vient d'utilisateurs pourtant reconnus : comptes vérifiés, appareils familiers et activités qui passent chaque point de contrôle.

Ce basculement rend la distinction entre clients légitimes et abus plus difficile que jamais.

La solution n'est pas de durcir les contrôles. L'identité n'est plus un identifiant à confirmer une fois. Elle est dynamique : c'est un historique qui se construit en continu, tout au long du parcours client, plutôt que de se valider à un instant précis.

52 %

des entreprises ont déjà migré vers une évaluation continue de l'identité

SOURCE : ENQUÊTE ADYEN

De la vérification à la reconnaissance

La vérification répond à une question binaire à un instant donné : cette personne est-elle bien celle qu'elle prétend être ? La reconnaissance, elle, s'inscrit dans la durée : cette activité correspond-elle au schéma d'un client de confiance ?

Cette nuance est cruciale. Aujourd'hui, les fraudeurs savent contourner la vérification. Ce qu'elle ne peut pas facilement reproduire, c'est un historique comportemental cohérent. Un client régulier qui achète dans sa fourchette habituelle sur un appareil reconnu passe sans friction. Mais quand ce même schéma change (retours anormalement fréquents, abus de codes promo ou activité distribuée sur plusieurs comptes), le changement d'intention devient visible, même quand l'identité elle-même n'a pas changé.

La confiance se gagne et s'entretient au quotidien.
Elle ne doit pas être accordée une fois pour toutes.

ÉCLAIRAGE

SOURCE : ENQUÊTE ADYEN + PLATEFORME ADYEN

Quand une meilleure authentification élimine la friction

Les résultats sont clairs dans les marchés qui appliquent déjà cette approche.

Entre 2024 et 2025, les marchands APAC ont signalé la pression la plus forte en matière de prévention de la fraude, toutes régions confondues : environ 70 % ont cité une hausse des coûts de revue manuelle, 60 % une hausse des faux refus, et un sur trois déclarait peiner à trouver l'équilibre entre bloquer la fraude et accepter les clients légitimes.

Chez les marchands Adyen dans des marchés à plus forte pénétration de l'authentification (Japon, Australie et Singapour), le tableau est différent. Les taux d'autorisation ont atteint jusqu'à 99,57 %, en progression moyenne de 17 points de base sur un an, tandis que les taux de chargeback ont baissé régulièrement dans les trois marchés.

La confiance à grande échelle

La valeur de l'identité connectée se démultiplie sur un réseau plus large. Un seul marchand peut se construire un historique client dans son propre écosystème. Mais la reconnaissance au niveau du réseau (en s'appuyant sur des signaux à travers un large éventail de marchands et d'appareils) crée une image plus riche et plus rapide dès la première interaction.

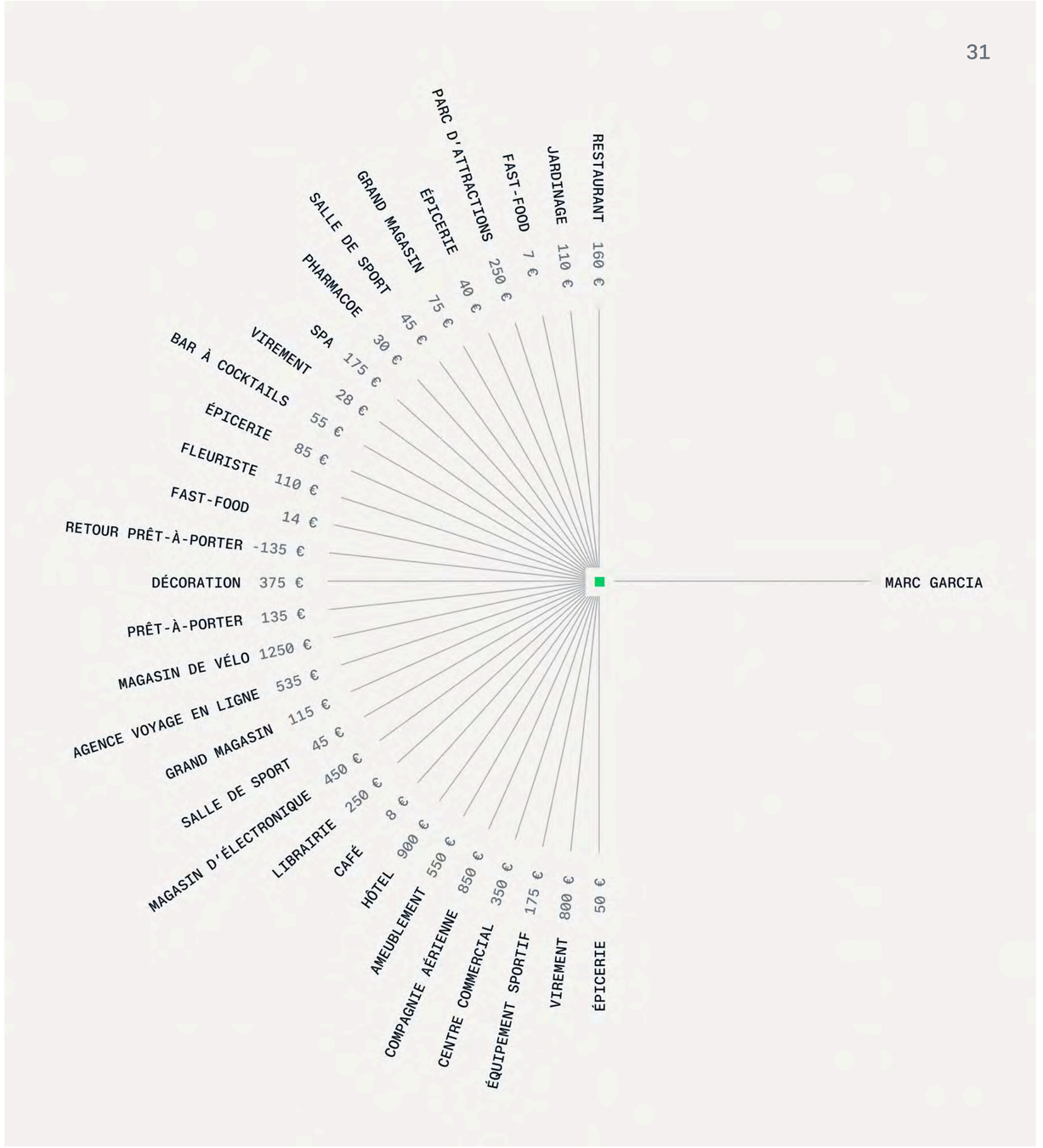
Sur le réseau mondial d'Adyen, il y a 84 % de chances qu'une identité soit déjà apparue dans des transactions, des entreprises, des paiements ou l'émission de cartes. Cela signifie que même de nouvelles relations clients commencent avec un historique, permettant des décisions plus sûres dès le départ et moins de friction pour les clients qui ont déjà démontré leur fiabilité ailleurs.

C'est un système où la reconnaissance devient réputation.

84 %

des identités déjà rencontrées par Adyen

SOURCE : PLATEFORME ADYEN



ZOOM PRODUIT

Construire le moteur anti-fraude de demain avec Protect

Les contrôles anti-fraude traditionnels se concentrent sur le blocage des mauvaises transactions une fois le risque visible. Mais la fraude moderne exploite de plus en plus les systèmes entourant le paiement : promotions, achats sans création de compte (ou commandes invités), création de compte, retours et les cartes cadeaux et avoirs.

L'approche la plus efficace anticipe ces décisions liées au risque. En combinant la cohérence d'identité, la reconnaissance inter-marchands et les signaux de risque avant autorisation, les entreprises peuvent distinguer les comportements de confiance des abus avant que la friction au checkout, les frais d'autorisation ou les pertes ne surviennent.

L'avantage ne se résume pas à de meilleurs taux d'approbation ou à moins de pertes liées à la fraude. C'est un meilleur contrôle sur le dosage de la confiance à travers les profils de marge, les moments de croissance et les parcours clients : réduire les faux refus, minimiser les revues manuelles inutiles, adapter l'appétit pour le risque aux priorités business et détecter les schémas d'abus plus tôt dans le parcours.

L'équilibre le plus difficile en matière de fraude est de maintenir les taux d'autorisation tout en améliorant la prévention. Traditionnellement, ces deux objectifs sont inversement corrélés : attraper plus de fraude, c'est bloquer plus de bons clients.

Mais en 2025, les marchands utilisant le moteur de risque intégré d'Adyen, Protect, ont tout de même constaté :

- **+16 % de détection de fraude sur un an.** Protect a identifié une plus grande part de fraude réelle que l'année précédente.
- **-33 % de faux positifs sur un an.** Malgré une meilleure détection, moins de clients légitimes ont été incorrectement bloqués.
- **2× plus de transactions autorisées** par rapport aux marchands sans Protect.

À mesure que le commerce s'automatise, la stratégie gagnante n'est pas de confier les décisions à une boîte noire. C'est d'anticiper la prévention tout en gardant les équipes aux commandes.

CHAPITRE / 5

Quand le client est un agent

Historiquement, la prévention de la fraude s’est articulée autour de deux défis fondamentaux

Ces challenges en question étant : identifier les bons acteurs par rapport aux mauvais (généralement via des signaux comportementaux) et authentifier l’autorité pour s’assurer que la personne qui initie la transaction y est autorisée.

L’Agentic Commerce introduit un troisième participant, l’agent, qui complique ces problèmes et en crée de nouveaux. Les marchands doivent désormais :

- **Identifier les agents légitimes par rapport aux agents malveillants ou exploiteurs.**
- **Vérifier qu’un agent est autorisé à agir au nom d’un client.**
- **S’assurer que l’agent opère dans les limites de ce que le client a réellement voulu.**

Cette dernière dimension, l’intention, est nouvelle. Même un agent légitime et authentifié peut se comporter d’une manière qui s’écarte des attentes de l’utilisateur, en raison de stratégies d’optimisation, de manipulations malveillantes ou d’incitations mal alignées.

Un nouveau problème d’indiscernabilité

Ce changement fait de l’Agentic Commerce un défi de fraude distinct, et non simplement une version plus rapide de ce qui précédait. Le risque n’est pas seulement que les mauvais acteurs déploient des agents. C’est que les agents de confiance et les agents malveillants sont de plus en plus indiscernables au moment de la transaction, et que les systèmes existants n’ont pas été conçus pour les différencier.

L’Agentic Commerce devrait influencer une part significative du volume de paiements au cours des cinq prochaines années. Mais son impact est inégal selon les secteurs, tout comme le risque.

Détournement de promotions par les agents IA

À mesure que les agents d'achat pilotés par l'IA deviennent plus performants, les systèmes automatisés peuvent exploiter les promotions et les fenêtres d'inventaire plus vite que les marchands ne peuvent réagir.

Dans un scénario type, les agents surveillent les environnements de prix et déclenchent des achats massifs quand les conditions sont remplies (en combinant remises, crédits de fidélité et incitations au paiement d'une manière que les marchands n'avaient jamais prévue). Les transactions elles-mêmes sont individuellement valides, et aucun signal unique ne déclenche une règle. Mais combinées, elles produisent un abus systémique.

Une variante cible les lancements de produits à inventaire limité. Les agents raflent les stocks à grande échelle dans les secondes suivant la mise en vente, devançant les clients légitimes et contournant les contrôles conçus pour les protéger. Ce qui semble être un lancement réussi peut, en réalité, être une extraction partiellement automatisée.

Contrairement aux attaques de bots traditionnelles, ces schémas ne nécessitent souvent pas d'identifiants volés ou d'identités synthétiques. Ils opèrent via des comptes légitimes avec de vrais historiques d'achats.

L'Agentic Commerce ne crée pas une toute nouvelle catégorie de fraude. Il industrialise les cas limites que les entreprises peinent déjà à contenir.

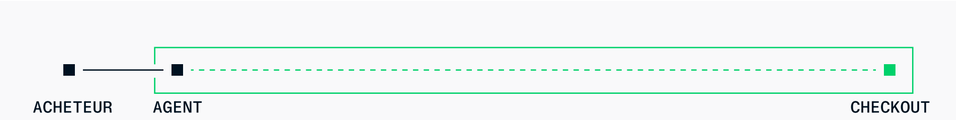
Le déplacement en amont

À l'ère de l'Agentic Commerce, il ne suffit plus d'appliquer des contrôles anti-fraude au checkout. Au moment où un agent arrive à ce stade, de nombreuses décisions ont déjà été prises, souvent dans des systèmes que le marchand ne peut pas observer ni contrôler. Le résultat est une plus grande exposition aux chargebacks, aux abus de remboursement, à l'exploitation des promotions et aux transactions techniquement valides, mais déconnectées de l'intention de l'utilisateur.

En bref, la confiance doit être établie plus tôt entre systèmes, protocoles et participants, et pas seulement au moment du paiement.

TRADITIONNELLEMENT

À L'ÈRE DE L'AGENTIC



Intelligence, identification et authentification

Ces défis continuent d'évoluer, mais quelques approches claires se dessinent :

- **Intelligence comportementale.** Les systèmes anti-fraude doivent s'adapter pour reconnaître les schémas comportementaux spécifiques aux agents, pas seulement ceux des humains. Cela inclut l'entraînement des modèles sur les schémas d'interaction pilotés par les agents, la capture de signaux plus tôt dans le cycle de vie des transactions, et le partage de plus de données entre les participants de l'écosystème : marchands, réseaux, émetteurs et plateformes d'IA.
- **Identification des agents.** Une capacité critique sera de distinguer les agents de confiance des agents non fiables. Cela dépendra probablement de la collaboration avec les réseaux de paiement et les institutions financières, de cadres d'identité partagés ou de registres pour les agents, et de signaux standardisés indiquant la provenance et la réputation des agents.
- **Authentification et délégation.** Les systèmes d'authentification existants n'ont pas été conçus pour le commerce délégué. Des travaux sont en cours pour étendre les protocoles actuels afin de prendre en charge les autorisations basées sur les agents, définir comment le consentement et la délégation sont capturés et vérifiés, et aligner les nouveaux schémas de transaction avec les normes de l'industrie et les cadres réglementaires.

La confiance doit démarrer plus tôt

Selon nos données d'enquête, une part significative des marchands considère déjà le scoring de confiance des plateformes IA comme critique : notamment la capacité d'évaluer non seulement qui effectue la transaction, mais quel système agit, au nom de qui, et si cette délégation a été explicitement autorisée.

Les organisations tournées vers l'avenir répondent en traitant le risque moins comme un point de contrôle au checkout, et plus comme une couche de contrôle continu. Les entreprises les mieux positionnées pour cette transition sont celles qui reconnaissent que l'identité, la délégation et l'intention doivent être modélisées séparément et connectées avant que l'agent n'arrive.

30 %

des commerçants estiment que le scoring de confiance des plateformes IA est le signal le plus important pour l'Agentic Commerce

SOURCE : ENQUÊTE ADYEN

Conclusion

Les mécanismes de la fraude ont fondamentalement changé.

En 2026, les risques les plus significatifs ne se trouvent plus à la périphérie ; ils opèrent à l'intérieur des systèmes et comportements conçus pour les clients légitimes. Ce changement rend les contrôles traditionnels moins efficaces et la friction large plus coûteuse.

Il ne s'agit pas de plus de contrôles, mais de plus de précision : utiliser l'identité dynamique, le comportement et le contexte pour distinguer confiance et risque plus tôt dans le parcours client.

Ce faisant, la gestion de la fraude devient plus qu'une fonction défensive. Elle devient un moyen de protéger les revenus et de stimuler la croissance tout en prenant de meilleures décisions sur où et comment la confiance est appliquée.

Postface

Aujourd'hui, l'essentiel des abus se loge en dehors de la fraude classique sur paiements non autorisés : escroqueries, usurpation d'identité, fraude amicale, abus de politique, comportements d'apparence légitime. Autant d'activités difficiles à repérer à un instant T, mais détectables sur la durée.

Historiquement, la lutte anti-fraude répondait à un problème plus ciblé. Elle se concentrait sur l'authentification du client, l'autorisation de la transaction et l'attribution des pertes. L'approche reste utile, mais ne suffit plus.

L'authentification forte (SCA), par exemple, détecte les identifiants volés mais perd son efficacité quand le consommateur envoie lui-même l'argent. La Vérification du bénéficiaire (VoP) couvre les virements mal orientés et l'usurpation basique, mais pas les comportements qui ne deviennent suspects que dans la durée, entre contreparties ou entre canaux.

KATIE SUSKIND
GLOBAL HEAD OF POLICY, ADYEN

Un cadre centré sur l'authentification et l'autorisation au moment de la transaction arrivera toujours trop tard. Les politiques publiques commencent à le refléter :

- **Le Royaume-Uni** impose un remboursement obligatoire qui couvre la plupart des pertes liées aux escroqueries APP (Authorised Push Payment).
- **L'Australie** construit son cadre autour d'obligations de prévention plutôt que de remboursement, le recours servant de filet de sécurité.
- **Au Brésil**, le mécanisme de retour PIX permet à l'institution destinataire de bloquer les fonds et, depuis peu, de les tracer sur les transferts ultérieurs.
- **En Europe**, le projet DSP3/PSR étend la vérification obligatoire du nom du bénéficiaire et donne aux PSP une base juridique claire pour partager des signaux de fraude, jusque-là dans une zone grise.

Aucun modèle n'est complet, mais tous s'éloignent d'une approche centrée sur un acteur à un instant donné pour s'attaquer aux espaces entre les participants.

La responsabilité est une autre voie législative, et pour cause : elle répare un préjudice réel. Mais c'est une solution a posteriori, elle n'aide ni à repérer les escrocs plus tôt, ni à perturber la fraude, ni à empêcher les fonds de circuler. Pire, elle peut nourrir l'insouciance des consommateurs en suggérant que le système absorbera la perte.

Face aux schémas de fraude actuels, cette réponse reste trop limitée : le vrai problème n'est pas de savoir où vont les pertes, mais que les acteurs légitimes ne peuvent pas stopper la fraude assez tôt. D'où l'enjeu d'un meilleur partage des données, qui s'attaque à la vraie faiblesse du système et offre une chance d'agir en prévention, au lieu de réallouer le coût après l'échec.

L’efficacité de votre stratégie anti-fraude ne se mesure plus au taux de transactions bloquées. Elle se joue dans la précision de vos décisions.

Les entreprises qui voient l'identité comme une infrastructure et le risque comme un levier de croissance transforment leurs résultats. Elles dépassent leurs concurrents qui se concentrent uniquement sur la réduction des pertes.

Évaluez votre stratégie. Mettez votre approche à l'épreuve →

adyen

engineered for ambition