TRANSACTIONS FRAUDULEUSES : UNE DETECTION À PARFAIRE

Les banques et les détaillants en ligne peuvent considérablement améliorer leur capacité à capturer les transactions frauduleuses à haut risque et difficiles à détecter en combinant des renseignements partagés sur la fraude dans leurs évaluations des risques, selon le dernier rapport Global State of Fraud and Identity de LexisNexis Risk Solutions.

Le rapport révèle comment les entreprises peuvent instaurer une confiance numérique solide et prévenir la fraude avant qu'elle ne se produise grâce à des renseignements collaboratifs sur l'identité numérique. Ce même rapport détaille plusieurs exemples de réussite, dont celui d'une organisation qui a porté le taux de reconnaissance des clients à 94 %. Une autre organisation a intégré l'identité numérique et l'intelligence de l'adresse e-mail pour augmenter d'un quart (26 %) les taux de capture des fraudes.

Le rapport explore également l'impact de l'activité criminelle sur la confiance des consommateurs, aggravé par le fait que moins de 10 % des mules financières identifiées par les forces de l'ordre sont arrêtées et moins de 1 % sont inculpées. L'adoption rapide par les fraudeurs de technologies basées sur l'IA pour automatiser le phishing et les deepfakes contribue à rendre les escroqueries plus efficaces et plus convaincantes, érodant ainsi la confiance des consommateurs dans les services numériques. Selon l'analyse de la plateforme LexisNexis Digital Identity Network®, les attaques frauduleuses mondiales ont augmenté de 19 % d'une année sur l'autre.

Vers un réseau collaboratif partagé

Un réseau collaboratif partagé permet aux organisations de signaler les activités suspectes et les cas de fraude confirmés aux autres membres, afin de compliquer la tâche des fraudeurs. Il peut s'agir de données sur l'appareil utilisé, d'adresses IP et d'autres signaux numériques, ainsi que de l'adresse e-mail fournie. L'analyse du risque potentiel associé à ces signaux peut considérablement améliorer l'efficacité des organisations à capturer les transactions à haut risque. Dans un cas, une grande banque mondiale a multiplié par 17 (1700 %) sa capacité de détection. Dans un autre cas, un émetteur de cartes a amélioré son évaluation des risques par un facteur de 23 (2300 %). Dans les deux cas, des données collaboratives ont été utilisées.

La technologie en première ligne

Malgré cela, seulement six organisations sur dix (60 %) ont mis en place des solutions technologiques de prévention de la fraude sur tous les canaux de transaction, et seulement une organisation sur quatre (27 %) dans les régions EMEA et APAC utilise des consortiums ou des initiatives d'échange de données dans le cadre de leurs activités de prévention de la fraude, selon le rapport. Ceci malgré le fait qu'une majorité d'entreprises déclarent que l'intégration de l'expérience numérique et des efforts de prévention de la fraude (72 %) et la réduction des frictions avec les clients lors du passage en caisse (68 %) soient des priorités « critiques ou élevées ».

> « Le désir des consommateurs de bénéficier d'un service plus rapide et instantané entraîne une demande de changement, y compris la création de solutions de paiement alternatives. En réponse, les régulateurs et les banques centrales mettent en place des systèmes, tels que les canaux de paiement instantané, qui facilitent les transactions », souligne Stephen Topliss, vice-président de la fraude et de l'identité, LexisNexis Risk Solutions. « Cependant, chaque tentative de faciliter les transactions pour les consommateurs facilite également la vie des fraudeurs. La demande sociétale de commodité a laissé les institutions financières face à un exercice difficile d'équilibre consistant à offrir l'innovation technologique et la commodité, tout en maintenant la confiance et l'intégrité du système ».

L'humain, toujours le maillon faible

Une vision plus large est également essentielle dans la lutte contre les identités synthétiques, c'est-à-dire les faux profils numériques créés à des fins frauduleuses. Des renseignements solides peuvent révéler des signes révélateurs, comme le fait que les identités synthétiques sont sept fois plus susceptibles de ne pas avoir de parents au premier degré et 20 fois plus susceptibles d'apparaître dans de multiples demandes de crédit sur une courte période. Le rapport indique que les êtres humains continuent d'être un maillon faible dans la chaîne de confiance, avec une armée de mules financières – dont environ 40 % ont généralement moins de 25 ans – qui aident les cybercriminels à blanchir entre 2 et 5 % du PIB mondial chaque année.

> « Le pire scénario serait que les consommateurs cessent de recourir à la technologie numérique par manque de confiance dans le processus », conclut M. Topliss. « Pour s'attaquer à ce problème mondial, il faut adopter une approche à plusieurs niveaux, car il n'existe pas de solution miracle pour lutter contre la fraude. »

SOURCE : IT Channel – Novembre 2024