



LE POINT SUR LE DEUXIÈME
SEMESTRE DE 2026 : PRINCIPALES
TENDANCES EN MATIÈRE DE FRAUDE

La fraude à l'ère de la confiance continue

Évaluer le risque lorsque les identités,
les communications et les relations
établies sont compromises

TransUnion® 

TABLE DES MATIÈRES

3

Résumé

4

Auteurs et contributeurs

5

Au cœur du paysage mondial de la confiance

Les identités synthétiques redéfinissent la confiance

Les communications sont devenues le nouveau champ de bataille en matière de fraude

L'intelligence artificielle permet aux réseaux criminels d'opérer à une échelle industrialisée

23

Perspectives régionales

États-Unis

Canada

30

Façonner la prochaine ère de la confiance numérique

33

À propos de l'étude

Résumé

À l'échelle mondiale, les dirigeants d'entreprise estiment que leur organisation a perdu, en moyenne, 6,5 % de son chiffre d'affaires en raison de la fraude au cours de l'année écoulée. Ces pertes sont le symptôme d'un problème plus vaste : la fraude prospère parce qu'il est devenu plus facile d'exploiter la confiance, et plus difficile de l'instaurer. Et comme la confiance constitue le fondement de la croissance, des relations avec les clients, de l'efficacité opérationnelle et de la réputation de la marque, la fraude a cessé d'être un simple défi opérationnel pour devenir un risque stratégique pour l'entreprise.

Pendant des années, la vérification de l'identité a servi de fondement à la confiance numérique : instaurer la confiance lors de l'entrée en relation, authentifier les utilisateurs et valider les transactions. Ce socle demeure essentiel, mais il ne suffit plus.

La vérification de l'identité ne peut, à elle seule, assumer la charge de la prévention de la fraude. La fraude exploite de plus en plus les identités une fois qu'elles ont été vérifiées, les communications après leur acheminement et les relations une fois qu'elles ont été établies. La question cruciale n'est plus simplement : « S'agit-il de la bonne personne? ». Elle est désormais : « Peut-on accorder sa confiance à cette interaction? ».

La prévention de la fraude doit évoluer : il ne s'agit plus de vérifier l'identité à des moments ponctuels, mais d'évaluer la confiance en continu. Les organisations doivent regrouper des signaux relatifs à l'identité, aux appareils, aux comportements, aux communications et au réseau afin d'obtenir une vision plus complète des risques. Les renseignements liés aident les organisations à détecter les risques plus tôt, à prendre des décisions plus précises et à réduire les frictions inutiles pour les clients légitimes.

Ce rapport s'adresse aux responsables de la lutte contre la fraude, de la gestion des risques, de l'identité, de l'authentification, des canaux numériques et de l'expérience client, qui ont pour mission de préserver la croissance et la confiance des clients. En s'appuyant sur les renseignements mondiaux de TransUnion, sur ses recherches exclusives et sur ses analyses des marchés régionaux, il explique l'évolution des risques de fraude, les raisons pour lesquelles les stratégies de lutte contre la fraude traditionnelles perdent en efficacité, ainsi que les capacités que les organisations devraient privilégier pour bâtir une stratégie de confiance plus résiliente tout au long du cycle de vie des clients.

La prochaine ère de la confiance numérique va au-delà de la simple prévention de la fraude. Elle façonnera la manière dont les organisations acquièrent des clients, préservent leurs relations, réduisent les frictions et prennent des décisions en matière de risques en toute sérénité. Les organisations qui réussiront au cours de la prochaine décennie ne se contenteront pas de détecter la fraude plus efficacement : elles instaureront une confiance continue, véritable socle d'une croissance durable.

Trois axes définissent la nouvelle ère de la confiance numérique :

La confiance ne s'établit plus une fois pour toutes; elle fait l'objet d'une évaluation continue.

La fraude survient de plus en plus souvent après que la confiance a été accordée lors de l'entrée en relation; les organisations doivent donc évaluer en permanence l'identité, le comportement et les intentions tout au long du cycle de vie du client.

Le domaine de la prévention de la fraude s'étend désormais aux communications.

L'usurpation d'identité de marque, les appels frauduleux et l'ingénierie sociale influencent la perception et le comportement des consommateurs avant même que les dispositifs de lutte contre la fraude classiques ne puissent intervenir.

La fraude fonctionne comme un écosystème interconnecté et industrialisé.

L'intelligence artificielle et l'automatisation permettent aux réseaux criminels de concevoir et de perfectionner leurs attaques plus rapidement, de les cibler avec précision, de les personnaliser de manière convaincante et de s'adapter promptement à l'évolution des conditions.

Auteurs et contributeurs

Auteurs



Brian Killeen

**Vice-président,
Gestion de produits
Solutions de gestion de la fraude
et de l'identité**

in



Richard Tsai

**Directeur principal,
Marketing de produit,
Solutions de gestion de la
fraude et de l'identité**

in

Contributeurs



Amritha Reddy

**Directrice principale,
Solutions de gestion de la
fraude et de l'identité, Afrique**

in



Glyn Cowlshaw

**Directeur,
Spécialistes des solutions de lutte
contre la fraude, Royaume-Uni**

in



Andrew Sigfrid

**Directeur principal,
Solutions de gestion de
la fraude et de l'identité, Canada**

in



Manual Pineros

**Directeur,
Développement commercial, Espagne**

in



Anurag Anand

**Directeur,
Solutions de gestion de
la fraude et de l'identité, Inde**

in



Miguel Rivera

**Directeur principal,
Solutions de gestion de la fraude
et de l'identité, Amérique latine**

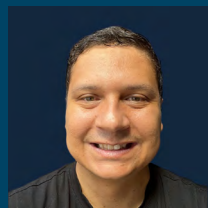
in



Anurag Varma

**Directeur,
Solutions de gestion de la fraude
et de l'identité, Asie-Pacifique**

in



Wallace Massola

**Conseiller principal,
Responsable des solutions de gestion
de la fraude et de l'identité, Brésil**

in

Au cœur du paysage mondial de la confiance



À mesure que la confiance devient plus facile à exploiter, les organisations peinent à suivre le rythme.

La fraude est devenue l'un des risques économiques les plus importants auxquels les organisations sont confrontées. À l'échelle mondiale, 61 % des dirigeants d'entreprise placent la fraude parmi les risques ayant le plus grand effet potentiel sur leur activité, devant les failles de cybersécurité, les questions de conformité, la perte de clientèle, les coûts opérationnels et les risques liés à la réputation. Plus préoccupant encore, 58 % des dirigeants interrogés se disent très ou extrêmement inquiets du fait que la fraude évolue plus rapidement que la capacité de leur organisation à la détecter et à la prévenir.

Cette situation découle d'une transformation fondamentale des modes opératoires de la fraude. Bon nombre des menaces qui progressent le plus rapidement ne visent pas seulement à dérober de l'argent, mais à tirer parti de la confiance. Les identités synthétiques sont conçues pour paraître légitimes. Les escroqueries manipulent les consommateurs pour qu'ils autorisent des activités frauduleuses. L'intelligence artificielle permet aux attaques de devenir plus adaptatives, plus évolutives et plus difficiles à détecter. De plus en plus, la fraude réussit en exploitant des identités, des communications et des relations de confiance.

La fraude est un risque stratégique qui se dissimule au sein des pertes opérationnelles

De nombreuses organisations perçoivent encore la fraude principalement comme un problème financier et opérationnel. Les données suggèrent une réalité plus vaste. Alors que 47 % des dirigeants d'entreprise ont déclaré que les coûts opérationnels et les pertes financières directes avaient eu des répercussions importantes ou graves sur leur entreprise au cours de l'année écoulée, 45 % ont pointé du doigt la réputation de la marque et 42 % ont cité la capacité de croître ou de se développer. La fraude influence de plus en plus l'acquisition et l'expérience client, ainsi que les performances commerciales à long terme.

Les organisations reconnaissent le risque, mais nombre d'entre elles restent mal préparées aux menaces qui remodelent le paysage de la fraude. Plus de la moitié des dirigeants d'entreprise (53 %) ont cerné la fraude par identité synthétique comme la menace qu'ils se sentent le moins préparés à gérer, ce qui en fait le plus grand déficit de préparation recensé dans cette étude.

Dans leur ensemble, ces résultats témoignent d'une évolution plus large. Le défi auquel sont confrontées les organisations ne consiste plus simplement à détecter les activités frauduleuses une fois qu'elles ont eu lieu. Il s'agit désormais de comprendre comment la confiance est exploitée – au niveau des identités, des communications et des interactions avec les clients – puis de se doter des capacités nécessaires pour y répondre.

Les sections qui suivent examinent trois facteurs à l'origine de cette évolution : l'émergence d'identités synthétiques, le rôle croissant des communications dans les attaques frauduleuses, et l'industrialisation de la fraude grâce à l'intelligence artificielle et à l'automatisation.

À propos des données

Sauf indication contraire, les données citées dans le présent rapport sont issues d'études commandées auprès des entreprises et des consommateurs, ainsi que d'enseignements tirés des renseignements exclusifs de TransUnion en matière de fraude, d'identité, de crédit et de communications. Pour plus de détails sur la méthodologie, consultez la section [À propos de l'étude](#).

Les identités synthétiques redéfinissent la confiance

À une époque marquée par les identités synthétiques et les vols d'identité à grande échelle, l'identité ne constitue plus un fondement fiable pour établir la confiance. Partout dans le monde, les fraudeurs semblent prendre une longueur d'avance sur la capacité des organisations à distinguer les identités authentiques de celles qui ont été manipulées ou créées de toutes pièces.

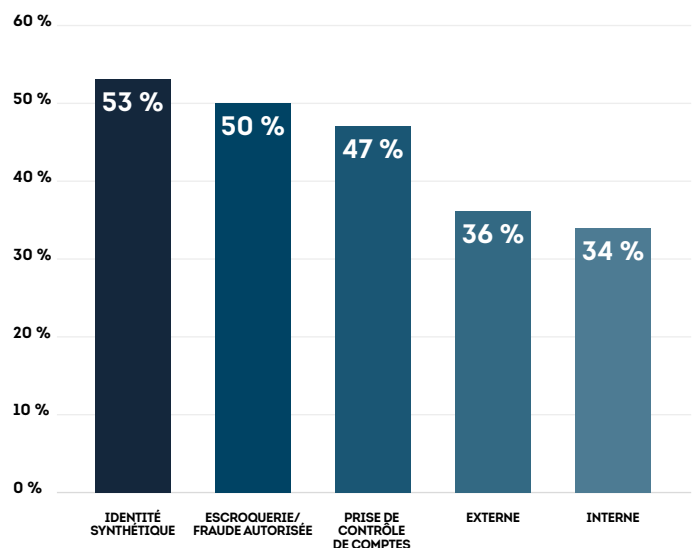
La fraude par identité synthétique dépasse les capacités de détection des organisations

Des réseaux de fraude organisés et des individus malveillants exploitent des renseignements personnels exposés ainsi que l'intelligence artificielle pour créer des identités crédibles et des documents hypertruqués, qu'ils utilisent ensuite pour mener des attaques contre des entreprises dans divers secteurs et marchés. À l'échelle mondiale, 18 % des dirigeants d'entreprise ont indiqué que la **fraude par identité synthétique** constituait, au cours de l'année écoulée, la principale cause des pertes liées à la fraude au sein de leur organisation; par ailleurs, 65 % d'entre eux s'attendent à ce que ce type de fraude connaisse la plus forte progression pour leur entreprise au cours des deux prochaines années.

Malgré les conséquences qu'elle engendre, la fraude par identité synthétique figure en tête de liste des types de fraude face auxquels les dirigeants estiment être les moins bien préparés aujourd'hui (voir figure 1). Une fois que des identités synthétiques parviennent à contourner les contrôles de fraude lors de l'intégration numérique, les organisations sont confrontées au défi de devoir les détecter avant de subir des pertes liées à la fraude, ou de s'exposer à des sanctions réglementaires, des pénalités, voire des poursuites judiciaires.

Figure 1 – La fraude par identité synthétique est la menace face à laquelle les organisations se sentent le moins préparées

Pourcentage de dirigeants d'entreprise ayant indiqué que leur organisation est la moins bien préparée à gérer chaque type de fraude



Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

65 %

des dirigeants d'entreprise
s'attendent à une
augmentation de la fraude par
identité synthétique au cours
des deux prochaines années

L'exposition aux identités synthétiques semble plus étendue que ce que beaucoup d'organisations imaginent

La fraude par identité synthétique est un problème mondial et intersectoriel. Elle sévit aussi bien dans les économies de crédit matures que sur les marchés numériques émergents. Bien que les cas d'exposition et les pertes soient peu signalés à l'échelle mondiale, la prise de conscience du risque s'accroît, car de nombreuses organisations confondent les pertes liées à la fraude à l'identité synthétique avec des fraudes internes ou externes.

Les observations régionales viennent confirmer les répercussions sur l'activité signalées par les dirigeants. Par exemple, à Hong Kong, en Inde, en Espagne et aux États-Unis, les dirigeants d'entreprise étaient plus enclins que la moyenne à estimer que, parmi tous les types de fraude, c'est la fraude par identité synthétique qui connaîtrait la plus forte progression au sein de leur organisation au cours des deux prochaines années. Les données provenant des États-Unis et du Canada, combinées aux observations du Royaume-Uni et d'Amérique latine, suggèrent que la fraude par identité synthétique pourrait être plus répandue que ne le laissent entendre les rapports actuels. À mesure que les organisations améliorent leur visibilité sur les activités liées à l'identité synthétique, nombre d'entre elles pourraient constater que leur exposition a été sous-estimée, ce qui renforce la nécessité d'évaluer en permanence la confiance, même après l'intégration.

La sensibilisation au risque de fraude par identité synthétique est en hausse

États-Unis

L'exposition totale des prêteurs américains au risque de fraude par identité synthétique a atteint 2,4 milliards de dollars US à fin juin 2026. Le secteur du financement automobile a été le plus durement touché, avec une exposition au risque lié aux identités synthétiques s'élevant à 1,5 milliard de dollars US, tandis que d'autres types de crédits – notamment les cartes bancaires et les marges de crédit personnelles – présentaient des niveaux d'exposition plus faibles. Aux États-Unis, les pertes moyennes dues à la fraude synthétique ont plus que doublé entre le premier semestre de 2009 et le premier semestre de 2026. Une étude exclusive de TransUnion indique que les organisations non financières, comme les entreprises de télécommunications, sont également exposées au risque lié aux identités synthétiques.

CANADA

Selon des recherches exclusives menées par TransUnion, la fraude par identité synthétique a connu une progression constante au Canada entre le troisième trimestre de 2021 et le quatrième trimestre de 2023, représentant plus de 14 % des pertes sur crédit liées à l'entrée en relation; ce constat souligne la difficulté croissante à détecter les identités fictives avant qu'elles ne s'ancrent au sein de l'écosystème financier.

Royaume-Uni

TransUnion a constaté que les institutions britanniques détectent activement un grand nombre de cas suspects d'usurpation d'identité synthétique lors d'exams préliminaires. Nombre d'entre elles découvrent que les pertes liées à la fraude par identité synthétique avaient initialement été comptabilisées comme des usurpations d'identité par des tiers ou des défaillances au sein de leur propre organisation.

AMÉRIQUE LATINE

Les problèmes liés à l'identité synthétique sont de plus en plus associés à l'intégration numérique et à l'obtention de crédit. Bien que de nombreux pays d'Amérique latine disposent de registres nationaux d'état civil, TransUnion a constaté que ces mesures n'empêchent pas la manipulation d'identité, la falsification de documents et l'utilisation de l'intelligence artificielle pour reproduire des pièces d'identité comme les permis de conduire et les passeports.

Les violations de données fournissent la matière première nécessaire à des fraudes par identité synthétique plus sophistiquées

Les violations de données alimentent en permanence la chaîne de la fraude fondée sur l'identité. Les cyberattaques ciblant des organisations dans le but d'obtenir des renseignements sur l'identité et des identifiants authentiques exposent des millions, voire des milliards, de personnes à travers le monde à des risques de fraude (voir figure 2). Alors que l'intelligence artificielle permet des attaques plus rapides et mieux ciblées, la menace que font peser les identités synthétiques sur la confiance ne fera que s'accroître.

Les rapports sur les violations de données aux États-Unis mettent en évidence l'ampleur des données d'identité à la disposition des fraudeurs pour la création d'identités synthétiques. Au premier semestre de 2026, des numéros de sécurité sociale ont été exposés dans 73 % des violations de données aux États-Unis, tandis que des permis de conduire et des cartes d'identité délivrées par les États l'ont été dans 34 % des cas. Les cybercriminels ont également pris pour cible des renseignements tels que les antécédents médicaux (37 % des violations aux États-Unis) ainsi que les numéros de comptes bancaires courants ou d'épargne (34 %). À mesure que des données d'identité authentiques deviennent disponibles à la suite de violations de données, les fraudeurs sont de plus en plus en mesure de créer des identités synthétiques convaincantes; cela rend plus complexe la distinction entre les consommateurs légitimes et les identités fictives, et souligne la nécessité d'une confiance continue, tant lors de l'entrée en relation qu'au-delà.

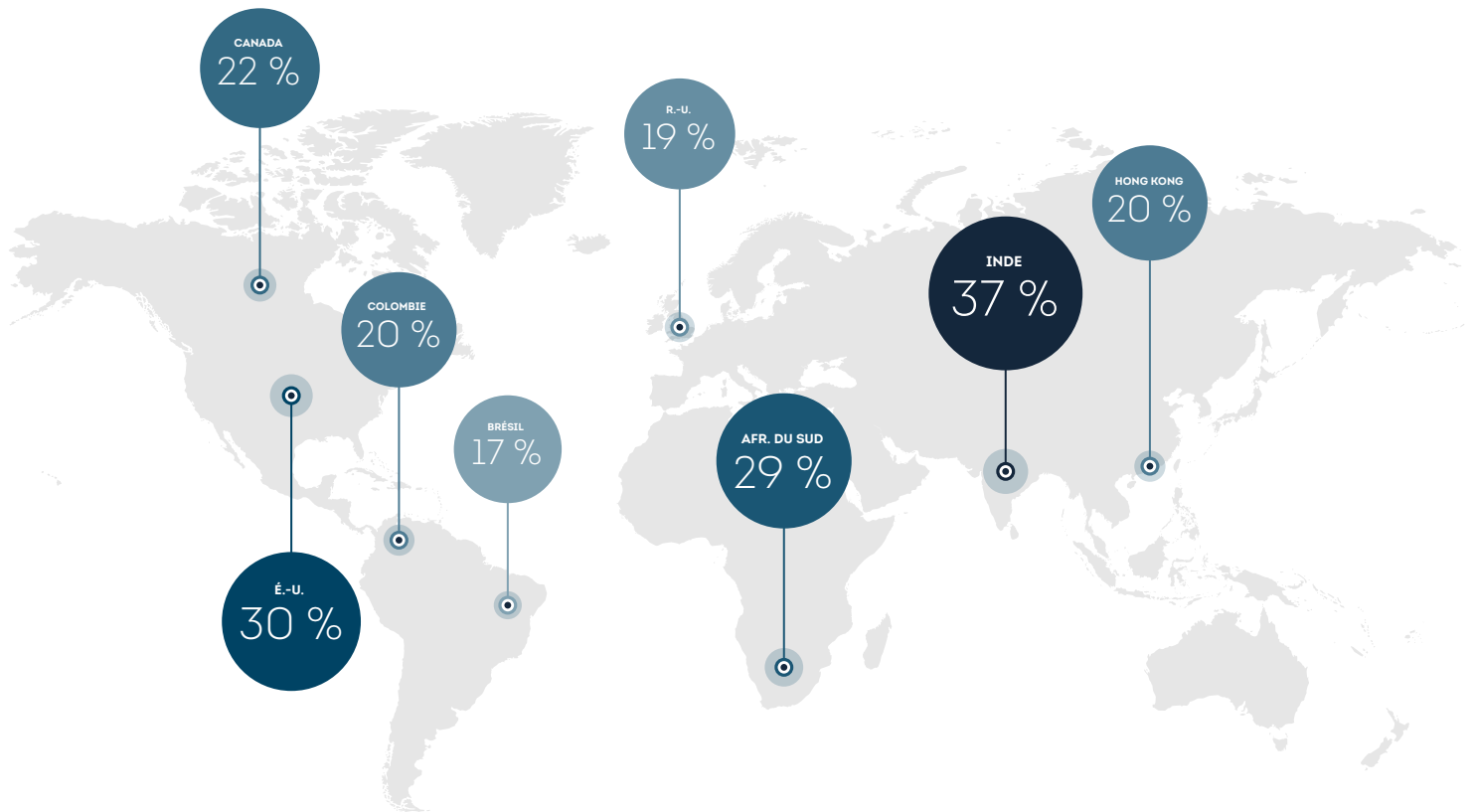
73 %

des violations de données aux États-Unis ont exposé des numéros de sécurité sociale complets au cours du premier semestre de 2026

Source : réseau mondial de renseignement de TransUnion

Figure 2 – À l'échelle mondiale, des consommateurs continuent de signaler l'exposition de leur identité à la suite de violations de données

Pourcentage de consommateurs ayant déclaré que leurs renseignements personnels ou les données de leurs comptes en ligne avaient été exposés lors d'une violation de données au cours d'une période récente de trois mois



Source : sondage Consumer Pulse, TransUnion, mai et juillet 2026

Aux États-Unis, le blanchiment de fiche de crédit accroît les risques liés aux identités synthétiques une fois que ces dernières sont utilisées pour des fraudes

Les criminels s'attaquent aux processus de confiance pour faciliter la fraude par falsification. L'une des stratégies employées par les fraudeurs pour maintenir des identités synthétiques au fil du temps est le **blanchiment de fiche de crédit**, une escroquerie qui exploite la procédure de contestation de crédit pour supprimer des renseignements négatifs légitimes d'un historique de crédit en faisant de fausses déclarations d'usurpation d'identité.

Le blanchiment de fiche de crédit compromet l'évaluation du risque de crédit en supprimant des renseignements défavorables des modèles de pointage. Il a été démontré que les suppressions de créances irrécouvrables à l'initiative du consommateur sont étroitement liées à cette pratique. Aux États-Unis, ces suppressions ont enregistré un taux de croissance annuel composé de 29,2 % entre 2017 et 2026 (voir figure 3).

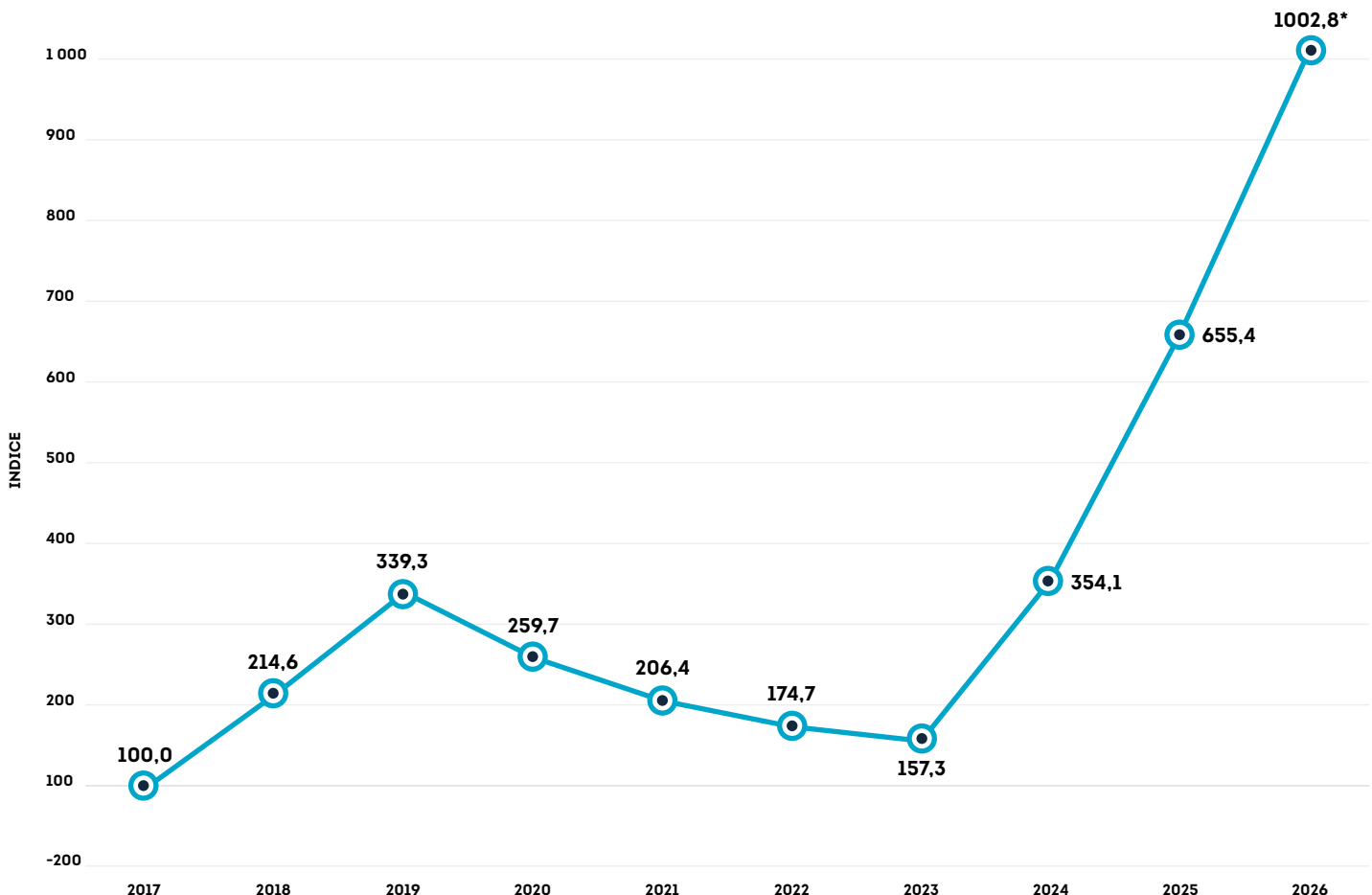
29,2 % –

Le taux de croissance annuel composé des suppressions de créances irrécouvrables à l'initiative des consommateurs aux États-Unis, de 2017 à 2026

Source : réseau mondial de renseignement de TransUnion

Figure 3 – La forte augmentation des suppressions de créances irrécouvrables pourrait prolonger la durée de vie des identités synthétiques

Croissance annuelle des suppressions de créances irrécouvrables à l'initiative des consommateurs, indexée sur l'année 2017



* 2026 : projections basées sur les chiffres réels du premier semestre de 2026

Source : réseau mondial de renseignement de TransUnion

Le risque lié à l'identité s'étend bien au-delà de la création de compte et devient un problème de cycle de vie

Les attaques par fraude fondées sur l'identité surviennent souvent avant que les organisations ne disposent de renseignements suffisants pour établir une relation de confiance avec de nouveaux clients. Bien que la création d'un compte constitue une étape déterminante pour instaurer cette confiance, la majeure partie des risques de fraude se manifeste une fois la relation client déjà établie.

Des profils de risque distincts apparaissent au niveau de la création de comptes, de la connexion et des transactions financières, notamment dans le contexte de la fraude assistée par l'intelligence artificielle. L'intelligence artificielle peut, par exemple, permettre aux fraudeurs de générer ou de modifier rapidement des identités, des identifiants et des interactions, afin de cibler les points de contrôle les plus vulnérables tout au long du parcours client. Bien que la création de compte représente souvent la part la plus élevée de fraudes numériques présumées parmi toutes les étapes du cycle de vie (voir figure 4), 81 % de l'ensemble des fraudes numériques présumées au cours du premier semestre de 2026 sont survenues lors d'interactions courantes avec les clients (connexion au compte et transactions financières).

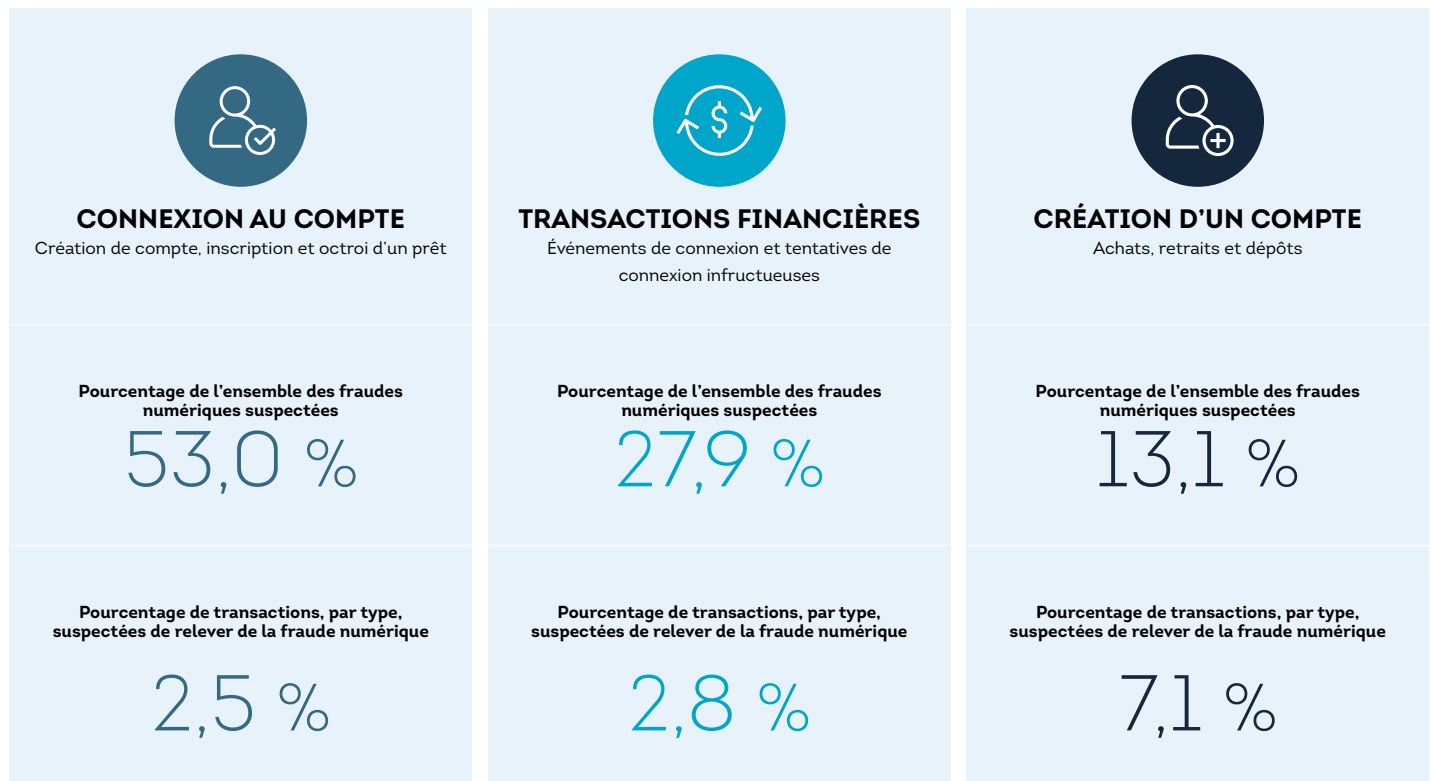
81 %

de l'ensemble des fraudes numériques suspectées sont survenues lors d'interactions en cours avec des clients au cours du premier semestre de 2026.

Source : réseau mondial de renseignement de TransUnion

Figure 4 – La plupart des fraudes numériques suspectées surviennent après la création d'un compte

Fraude numérique tout au long du parcours client au premier semestre de 2026



Source : réseau mondial de renseignement de TransUnion

Le risque d'usurpation d'identité tout au long du cycle de vie du client constitue une menace persistante pour tous les secteurs d'activité

Face à l'expansion des attaques de fraude numérique pilotées par l'intelligence artificielle, les criminels cherchent de plus en plus à exploiter les défenses les plus faibles, se déplaçant d'un secteur à l'autre et d'une organisation à l'autre à la recherche des cibles les plus faciles. Par exemple, une seule identité synthétique peut servir à obtenir un crédit de type « acheter maintenant, payer plus tard » auprès d'un commerçant, à souscrire un abonnement de téléphonie mobile incluant la location d'un appareil, à décrocher une carte de crédit avec un plafond plus élevé auprès d'une banque, ou encore à créer un compte sur un site de paris en ligne.

Bien que l'étape du cycle de vie où se concentre le risque varie selon le secteur et le modèle économique (voir figure 5), les organisations doivent prendre conscience que combler les lacunes en matière de vérification d'identité tout au long du cycle de vie du client est essentiel pour réduire les pertes liées à la fraude.

Par exemple :

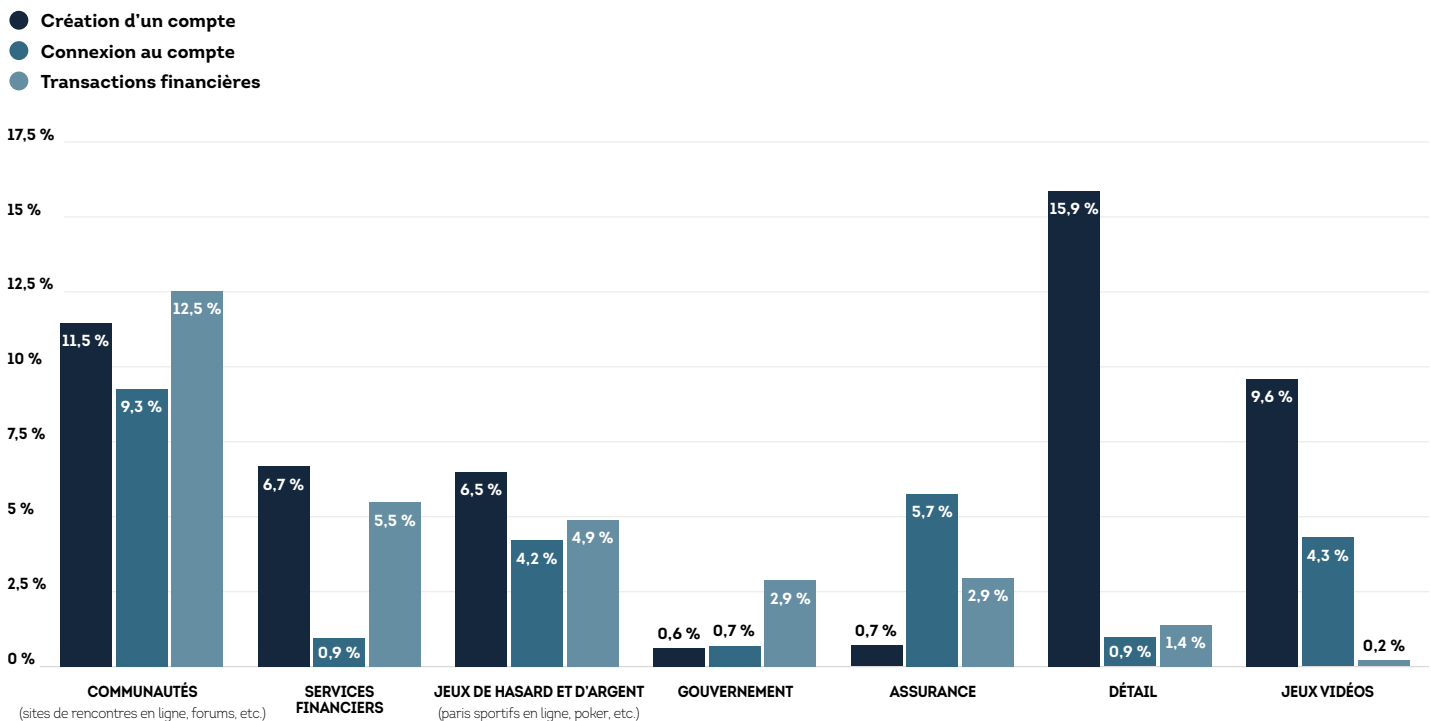
Le secteur du commerce de détail présente un risque extrêmement élevé de création de comptes en raison des abus liés aux promotions, car les comptes sont souvent nécessaires pour bénéficier des réductions annoncées. Pourtant, une vérification d'identité à faible niveau de sécurité est utilisée afin de minimiser les frictions avec les clients dans ce secteur extrêmement concurrentiel.

Le secteur des services financiers est confronté à un risque accru lors de la création de comptes, en raison du gain financier immédiat recherché par les fraudeurs. Par ailleurs, le risque de fraude lié aux transactions financières (notamment les dépôts, les retraits et les paiements) y est plus élevé que dans la plupart des autres secteurs; cela montre que les défis liés à la vérification de l'identité persistent bien après l'établissement de la relation avec le client.

Dans le secteur des jeux de hasard et d'argent, les risques sont élevés à plusieurs étapes de l'interaction. Malgré des procédures de vérification d'identité hautement sécurisées, les fraudeurs prennent pour cible les nouveaux comptes afin de détourner des points bonis. Toutefois, les risques persistent tout au long du cycle de vie du client. Ainsi, des risques liés à la connexion peuvent survenir lorsque plusieurs personnes utilisent un même compte, tandis que des risques liés aux transactions peuvent apparaître lorsqu'un fraudeur utilise une carte bancaire volée pour approvisionner un compte.

Figure 5 – Le risque de fraude se concentre à différentes étapes du parcours client, selon le secteur d'activité

Pourcentage des tentatives de transaction suspectées de constituer une fraude numérique, par étape du parcours client, dans certains secteurs au premier semestre de 2026



Source : réseau mondial de renseignement de TransUnion

MESURES RECOMMANDÉES

Ce que cela implique pour les organisations

La garantie de l'identité ne peut plus se limiter à la seule phase d'intégration. À mesure que la fraude par identité synthétique gagne en sophistication et que les fraudeurs exploitent des comptes légitimes tout au long du cycle de vie du client, les organisations doivent adopter une approche plus globale pour évaluer la confiance. Les mesures suivantes peuvent contribuer à réduire l'exposition aux risques, tout en garantissant des expériences client fluides et adaptées.

1

Mettre en place une confiance continue, plutôt qu'une vérification ponctuelle

La confiance liée à l'identité doit être envisagée comme un processus d'entreprise continu, et non comme une décision prise une seule fois lors de l'intégration. Les organisations doivent réévaluer cette confiance en permanence, à mesure que les comportements des clients, leurs identifiants et les signaux de risque évoluent tout au long de la relation.

2

Adapter la sécurité d'identité aux risques évolutifs

Priorisez la protection des identités là où la confiance est la plus susceptible d'évoluer, et pas seulement là où elle est initialement établie. Si l'intégration des nouveaux clients demeure essentielle, les organisations doivent renforcer la sécurité d'identité tout au long du parcours client : connexion, gestion des comptes, paiements et récupération.

3

Lier les renseignements sur l'identité entre les différents canaux de service

Réorientez les investissements des outils de vérification isolés vers des renseignements sur l'identité liés qui unifient les signaux d'identité à travers les interactions clients afin de détecter les fraudes émergentes tout en réduisant les frictions inutiles pour les clients légitimes sur tous les canaux utilisés pour les servir.

Les communications sont devenues le nouveau champ de bataille en matière de fraude

La fraude commence de plus en plus souvent en amont de l'événement frauduleux traditionnel, par le biais de l'usurpation d'identité de marque, de l'ingénierie sociale et de la manipulation de la confiance. Les canaux de communication sont devenus un signal d'alerte précoce, influençant souvent le comportement des consommateurs avant même que les dispositifs antifraude classiques puissent intervenir.

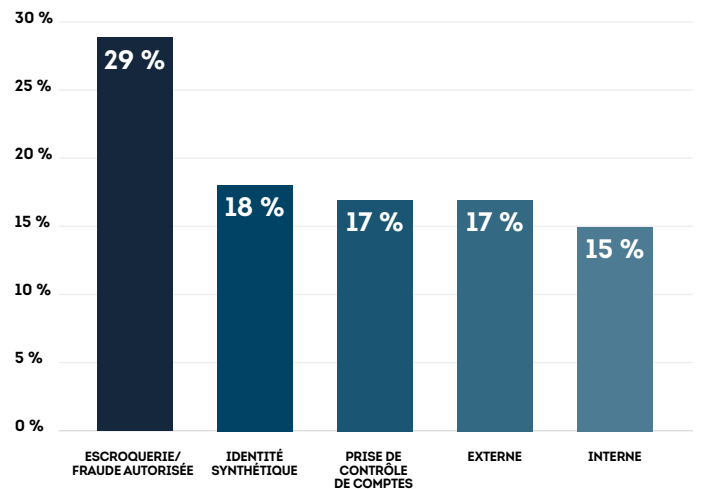
Les escroqueries s'imposent comme la principale source de pertes liées à la fraude, et celle qui connaît la croissance la plus rapide

La plupart des consommateurs ciblés par la fraude numérique ont déjà été confrontés à des courriels, des messages textes ou des appels téléphoniques frauduleux. Mais le fait d'en avoir conscience ne rend pas ces attaques moins efficaces pour autant. Les dirigeants d'entreprise ont indiqué que les escroqueries et les fraudes autorisées représentaient la principale cause de pertes liées à la fraude au sein de leur organisation au cours de la dernière année (voir figure 6)

Avec des escroqueries par usurpation d'identité sophistiquées, dopées à l'intelligence artificielle, les risques ne cessent de croître. Près de la moitié (48 %) des dirigeants d'entreprise ont signalé une augmentation des escroqueries – ou fraudes autorisées – au cours de l'année écoulée (voir figure 7); il s'agit, et de loin, de la catégorie de fraude ayant connu la plus forte progression.

Figure 6 – Les escroqueries et les fraudes autorisées engendrent les pertes les plus importantes pour les entreprises

Pourcentage de dirigeants d'entreprise ayant indiqué que ces types de fraude avaient engendré les pertes les plus importantes pour leur organisation au cours de l'année écoulée

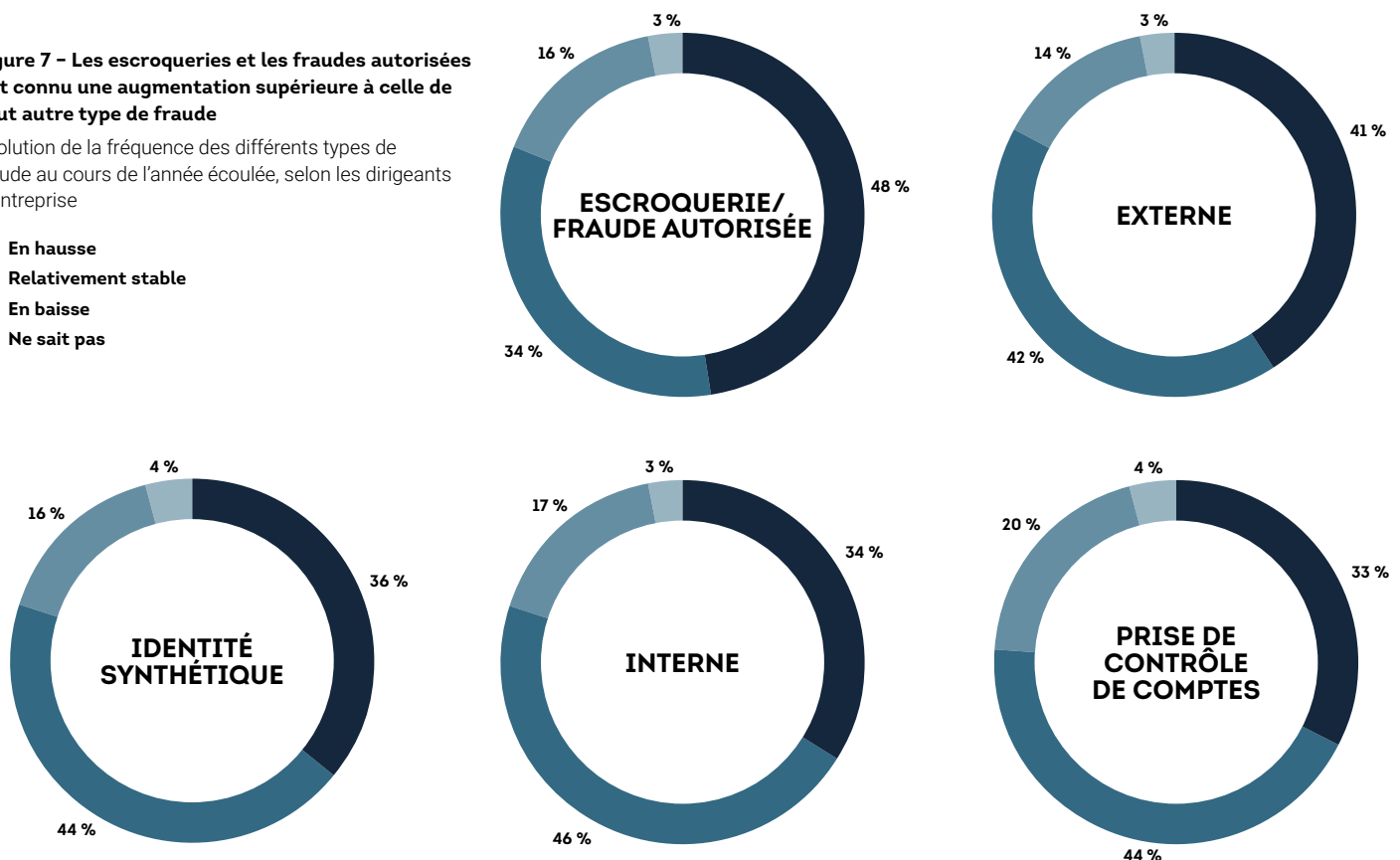


Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

Figure 7 – Les escroqueries et les fraudes autorisées ont connu une augmentation supérieure à celle de tout autre type de fraude

Évolution de la fréquence des différents types de fraude au cours de l'année écoulée, selon les dirigeants d'entreprise

- En hausse
- Relativement stable
- En baisse
- Ne sait pas



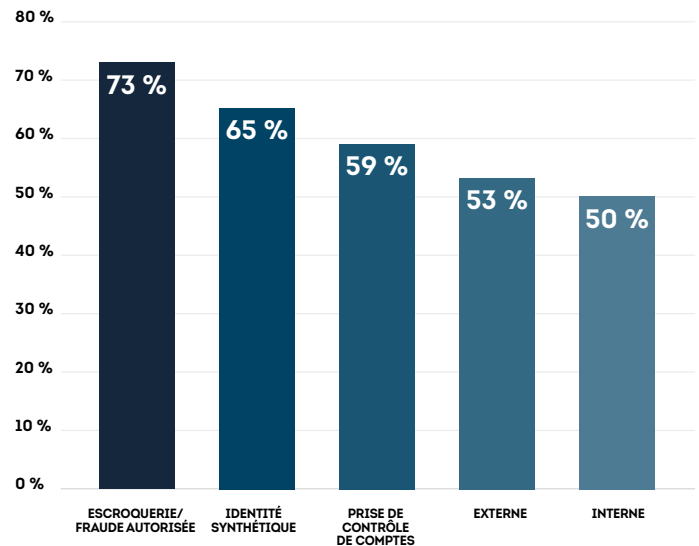
Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

L'usurpation d'identité d'entreprise est un indicateur avancé des futures attaques de fraude

Les organisations doivent considérer le risque lié aux communications comme un signal d'alerte précoce en matière de fraude, précédant les attaques par fraude fondées sur l'identité telles que la prise de contrôle de compte, l'escroquerie ou la fraude autorisée et la fraude à la création de nouveaux comptes. Si de nombreuses attaques se traduisent par une perte financière immédiate pour les consommateurs, elles aboutissent plus souvent encore à la collecte, par les criminels, de données destinées à être exploitées ultérieurement. Plus de la moitié (56 %) des victimes d'escroqueries ayant communiqué des renseignements personnels ou financiers ont déclaré ne pas avoir subi de perte financière¹. Parallèlement, les pertes financières liées aux escroqueries visant les consommateurs ont nettement diminué d'une année à l'autre; un signe manifeste que les escrocs cherchent davantage à dérober des renseignements personnels qu'à obtenir un gain financier immédiat². Malgré la baisse des pertes liées à la fraude aux consommateurs l'an dernier, les escroqueries – ou fraudes autorisées – constituent le type de fraude dont la progression est la plus attendue par les dirigeants d'entreprise au cours des deux prochaines années (voir figure 8).

Figure 8 – Les organisations s'attendent à ce que les escroqueries et les fraudes autorisées progressent plus rapidement que tout autre type de fraude

Pourcentage des trois principaux types de fraude que les dirigeants d'entreprise s'attendent à voir le plus progresser au cours des 24 prochains mois



Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

34 %

des consommateurs ayant déclaré avoir été la cible d'une fraude numérique ont indiqué avoir été victimes d'une attaque par hameçonnage – soit une proportion supérieure à celle observée pour tout autre type de fraude

Source : sondage Consumer Pulse, TransUnion; février, mars, mai, juillet et août 2026

Les communications fiables constituent une surface d'attaque courante pour les escroqueries par usurpation d'identité

Les consommateurs attendent des organisations qu'elles rendent les communications légitimes faciles à vérifier et les communications frauduleuses faciles à détecter. Les criminels s'efforcent de saper cette confiance, et l'usurpation d'identité d'une entreprise est devenue une tactique répandue (voir figure 9). Alors que de nombreux foyers disposent de plusieurs appareils numériques, pour la plupart des organisations dans le monde, en particulier celles des économies en développement, les communications numériques sortantes fiables sont centrées sur le téléphone mobile du consommateur. Pourtant, les marques ne contrôlent pas le cheminement vers l'appareil du client. Les vulnérabilités liées à l'interopérabilité des réseaux de télécommunications font des téléphones mobiles des cibles privilégiées pour des escroqueries par usurpation d'identité, impliquant des appels et des messages textes frauduleux.

Les fraudeurs exploitent des vulnérabilités au sein des réseaux téléphoniques pour dissimuler leur identité et **usurper les numéros de téléphone** d'entreprises de confiance, notamment des banques, des prestataires de soins de santé et des assureurs. En se faisant passer pour des représentants légitimes, ils peuvent amener les consommateurs à communiquer des codes à usage unique, à « confirmer » des renseignements personnels, à réinitialiser les identifiants de leur compte ou à rediriger des paiements, dans le cadre de manœuvres visant à prendre le contrôle de comptes.

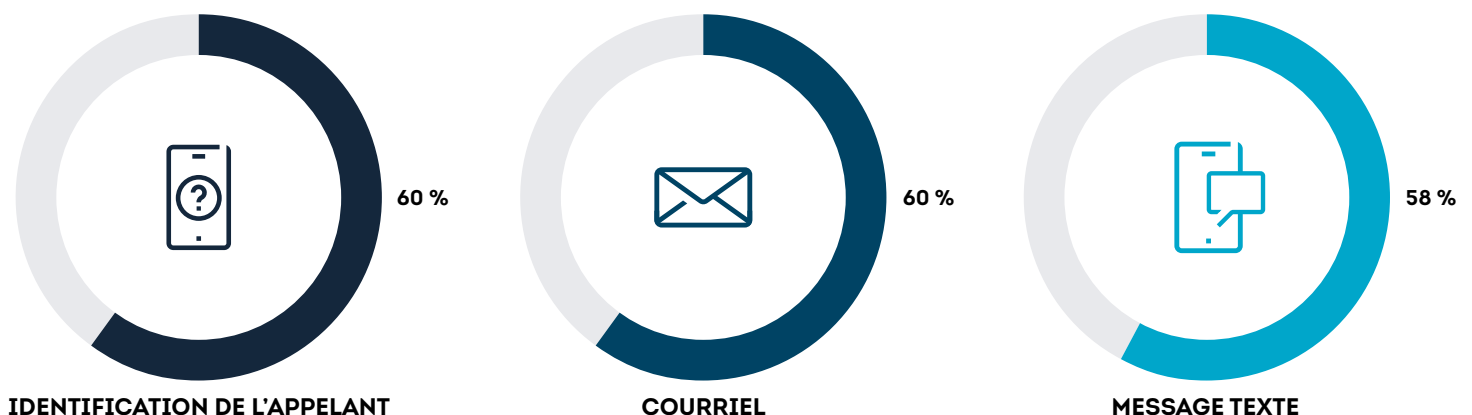
Une communication sortante fiable est essentielle pour assurer le suivi et renforcer les relations avec la clientèle. Les organisations misent généralement sur la sensibilisation pour aider à protéger leurs clients contre la fraude; elles établissent des politiques et des canaux de communication clairs, précisant dans quelles situations et pour quelles raisons elles sont amenées à contacter leurs clients – par exemple, dans le cadre d'alertes liées à la fraude. Toutefois, compte tenu de l'ampleur et de la croissance attendue des pertes liées aux escroqueries et aux fraudes autorisées, elles ont besoin de moyens plus efficaces pour protéger leurs communications sortantes avec les clients.

19,4 %
des appels sortants vers les particuliers, effectués via des opérateurs de réseau mobile américains, étaient usurpés au premier semestre de 2026

Source : réseau mondial de renseignement de TransUnion

Figure 9 – L'usurpation de marque affecte les clients sur tous les principaux canaux de communication

Pourcentage de dirigeants d'entreprise ayant indiqué que des fraudeurs avaient usurpé l'identité de leur organisation sur ces canaux au cours de l'année écoulée



Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

MESURES RECOMMANDÉES

Ce que cela implique pour les organisations

Alors que la fraude émane de plus en plus de canaux de communication considérés comme dignes de confiance, les organisations doivent élargir leur approche de la prévention des fraudes. L'objectif ne se limite plus à la simple authentification des utilisateurs ou à l'approbation des transactions. Il s'agit de déceler toute manipulation avant que la confiance ne soit compromise. Cela implique de détecter les fraudes plus en amont, en exploitant des signaux de communication associés à l'identité, à l'appareil et aux données comportementales, puis d'utiliser ces renseignements pour préserver – ou rétablir – une relation de confiance avec le client.

1

Détecter les fraudes plus tôt grâce aux signaux de risque liés aux communications

Exploitez les signaux révélateurs d'usurpation d'identité ou de falsification dès leur apparition, afin de pouvoir neutraliser la fraude avant même que les contrôles en aval ne soient sollicités.

2

Associez les signaux de risque liés aux communications aux renseignements sur l'identité

Intégrez les signaux de risque issus des communications aux données relatives aux identités, aux appareils et aux comportements, afin d'obtenir une vision plus dynamique et prédictive de la confiance accordée par les clients.

3

Combattre les escroqueries pour rétablir la confiance et améliorer la relation de confiance avec le client

Investissez dans des capacités qui rétablissent un engagement de confiance en dehors des frontières organisationnelles, bloquent les tentatives de compromission d'identifiants par des acteurs malveillants et permettent des réponses coordonnées à l'échelle de l'écosystème de la fraude.



L'intelligence artificielle permet aux réseaux criminels d'opérer à une échelle industrialisée

Les mesures traditionnelles de lutte contre la fraude numérique ne rendent plus compte de toute l'ampleur de la menace, car les réseaux criminels exploitent habilement la confiance pour contourner ou déjouer les contrôles classiques. L'intelligence artificielle a modifié les fondements économiques de la fraude. Elle permet aux fraudeurs d'automatiser des activités qui, par le passé, exigeaient un effort humain considérable (comme la création d'identités et de contenus, le ciblage des attaques ou les interactions avec les victimes), renforçant ainsi la précision, l'ampleur et la capacité d'adaptation de ces attaques. Elle a permis aux criminels d'accroître leurs taux de réussite avec une rapidité et une envergure inédites, allant jusqu'à industrialiser l'ensemble de la chaîne de valeur de la fraude. En fait, 42 % des dirigeants d'entreprise ont indiqué que l'ampleur ou la sophistication croissantes de la fraude font peser une pression importante, voire sévère, sur leur organisation.

La chaîne de valeur de la fraude repose sur la confiance que les organisations accordent aux identités numériques et que les consommateurs témoignent aux marques (voir figure 10). Des processus de création d'identités aux investissements à long terme dans des identités synthétiques conçues comme des actifs infrastructurels, l'intelligence artificielle est en train de remodeler la chaîne de valeur de la fraude. Elle réduit le coût de mise en œuvre de stratagèmes sophistiqués et permet aux criminels d'exploiter des processus d'entreprise légitimes dans divers secteurs, de dérober des actifs et de blanchir le produit de leurs forfaits en le convertissant en actifs difficiles à tracer.

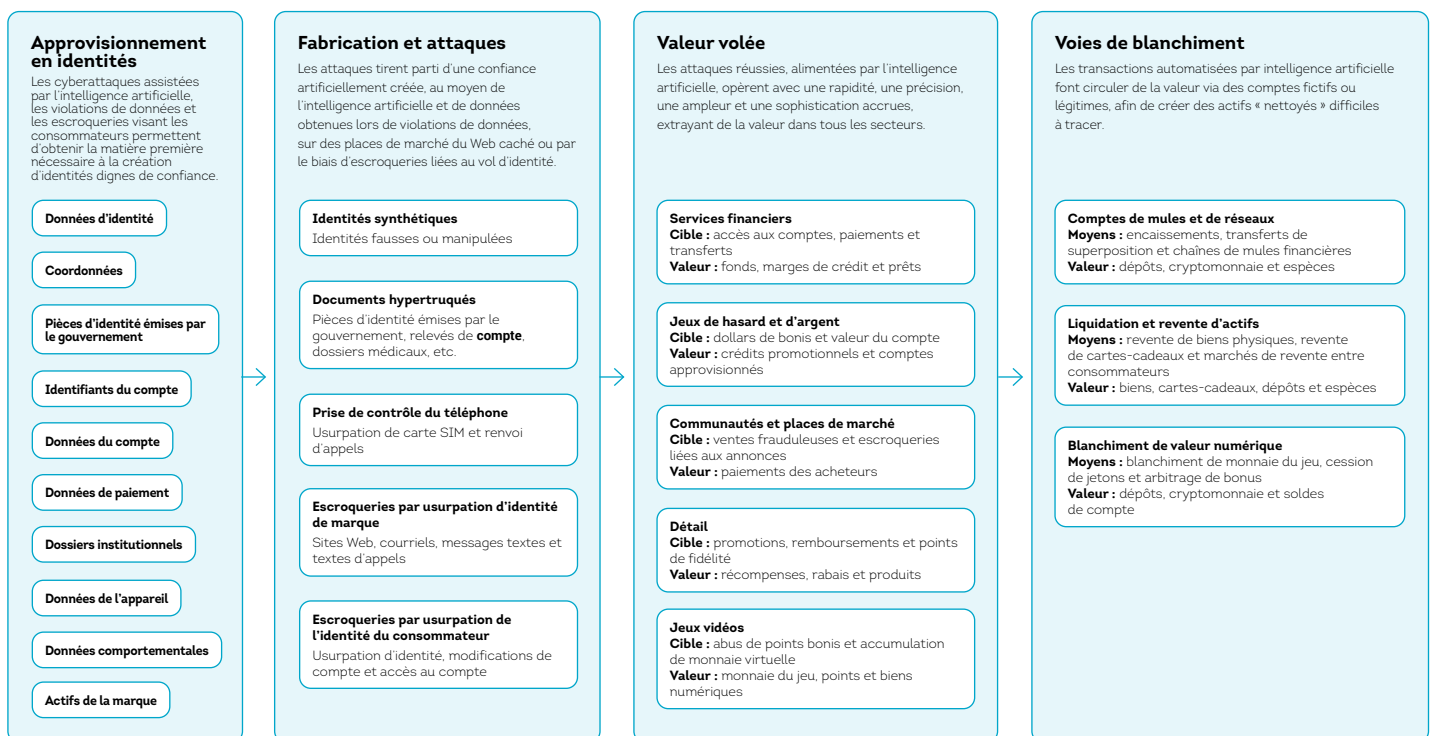
42 %

des dirigeants d'entreprise ont déclaré que l'ampleur ou la sophistication croissantes de la fraude font peser une pression importante, voire sévère, sur leur organisation

Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

Figure 10 – Comment la fraude industrialisée transforme des données d'identité en valeur financière

Illustration de la manière dont l'intelligence artificielle soutient chaque étape de la chaîne de valeur de la fraude industrialisée



Les fraudeurs exploitent la confiance numérique en s'adaptant aux environnements de prévention de la fraude

Les opérations de fraude industrialisées ciblent de plus en plus les interactions numériques au sein desquelles la confiance s'établit et où, à terme, de la valeur peut être extraite. Toutefois, les fraudeurs ne s'en prennent pas de la même manière à chaque étape du cycle de vie du client (voir figure 11).

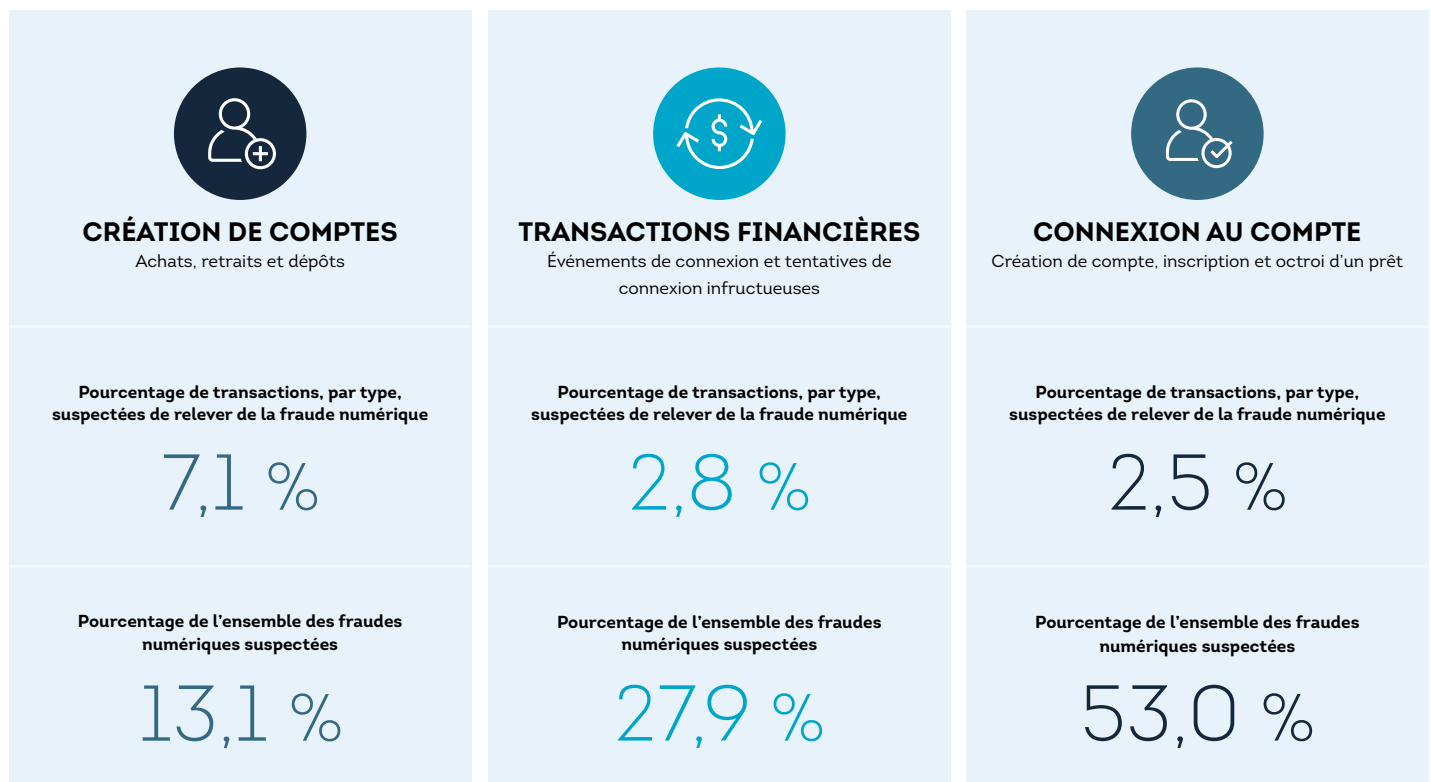
Au cours de la dernière décennie, les organisations ont investi massivement dans des mécanismes d'authentification client robustes, rendant les attaques reposant sur de simples identifiants moins accessibles aux fraudeurs. Toutefois, à mesure que les contrôles de connexion se sont renforcés, les fraudeurs se sont adaptés. Ils ciblent de plus en plus les processus d'authentification secondaire – tels que la récupération de compte et les demandes de service – au moyen d'attaques de type « adversaire au milieu ». L'industrialisation de l'intelligence artificielle a rendu ces attaques plus efficaces et plus facilement extensibles, réduisant ainsi le recours aux campagnes d'attaques à grande échelle traditionnellement associées aux processus d'authentification initiaux.

L'examen de trois points spécifiques de confiance numérique met en lumière les risques auxquels les organisations sont confrontées :

- **La création de comptes** présente le risque le plus élevé, malgré un volume relativement plus faible
- **Les transactions financières** constituent le deuxième risque le plus important, car c'est à ce stade que les attaques sont monétisées.
- La **connexion aux comptes** représente la majeure partie de l'activité, mais un risque comparativement plus faible.

Figure 11 – La création de comptes présente le risque de fraude le plus élevé, tandis que les connexions sont à l'origine de la majeure partie des activités frauduleuses

La fraude numérique tout au long du parcours client au premier semestre de 2026



Source : réseau mondial de renseignement de TransUnion

Pourquoi la création de comptes numériques demeure une étape critique présentant un risque élevé

La création de comptes ne représente que 4,9 % du volume des transactions, mais affiche le taux de fraude suspectée le plus élevé, soit 7,1 % (voir figure 12). L'intelligence artificielle réduit les efforts nécessaires pour créer des identités synthétiques, remplir des formulaires de demande, générer des documents issus d'hypertrucages et automatiser l'intégralité du processus d'intégration.

Si les fraudeurs ouvrent principalement des comptes pour monétiser des identités volées ou synthétiques, ils le font également pour faciliter des mécanismes de blanchiment – permettant ainsi de « nettoyer » des fonds illicites tout en dissimulant leur identité lors de la réalisation d'activités illégales. Certains secteurs ne privilégient pas une vérification rigoureuse de l'identité lors de la création d'un compte, car cela entrave les taux de conversion. Les entreprises mettent souvent en place des mécanismes de contrôle au moment de la création d'un compte, en fonction de la valeur offerte au consommateur. Par exemple, un commerçant ne demandera probablement pas à un client de créer un compte pour obtenir un code de réduction de 10 % en

échange de son adresse courriel. Bien qu'aligner l'échange de valeur sur les frictions subies par le client constitue une décision commerciale rationnelle, cette approche risque d'accorder une certaine confiance à une identité potentiellement frauduleuse.

Pour atténuer ce risque, les organisations pourraient devoir adopter des mécanismes de vérification d'identité comparables à ceux en vigueur dans des secteurs réglementés, tels que le secteur bancaire, le crédit ou les jeux de hasard et d'argent. Ces organisations doivent appliquer des mesures de conformité réglementaire – notamment les procédures « connaissance du client » et de lutte contre le blanchiment d'argent – aux processus de création de comptes, afin de contribuer à stopper les activités de blanchiment d'argent et de réduire les possibilités de fraude aux étapes ultérieures de la chaîne de valeur.

La fraude industrialisée permet de créer des milliers de nouveaux comptes en utilisant des identités synthétiques ou volées qui semblent légitimes. Si les processus traditionnels valident les attributs d'identité pris individuellement, ces derniers sont souvent examinés de manière isolée, ce qui empêche de détecter les signaux de confiance susceptibles de révéler des réseaux criminels et des organisations frauduleuses.

Figure 12 – Les secteurs présentant un niveau de garantie d'identité plus faible sont davantage exposés au risque de fraude lors de la création de comptes
Les cinq secteurs affichant le taux le plus élevé de fraudes numériques présumées lors de la création de comptes au premier semestre de 2026

Secteur	Tentatives de création de comptes suspectées de relever de la fraude numérique	Approche de vérification d'identité
 TOUS LES SECTEURS	7,1 %	
 COMMERCE DE DÉTAIL	15,9 %	Vérification d'identité simplifiée, afin de rendre la création de comptes aussi fluide que possible
 COMMUNAUTÉS	11,5 %	Vérification de l'identité, allant d'un niveau léger à un niveau rigoureux, afin de contribuer à protéger les membres de la communauté, en fonction de la valeur perçue du service
 JEUX VIDÉOS	9,6 %	Vérification d'identité simplifiée, afin de rendre la création de comptes aussi fluide que possible
 SERVICES FINANCIERS	6,7 %	Vérification d'identité renforcée pour répondre aux exigences réglementaires et réduire le risque de crédit
 JEUX DE HASARD ET D'ARGENT	6,5 %	Vérification d'identité robuste pour répondre aux exigences réglementaires et géographiques

Les attaques frauduleuses optimisées en vue d'une monétisation mettent en évidence les risques liés aux phases avancées du cycle de vie

Bien que les transactions financières et la connexion aux comptes présentent, dans l'ensemble, un niveau de risque comparable – à l'exception des secteurs de l'assurance et des jeux vidéos –, ce sont les transactions financières qui affichent le risque de fraude le plus élevé (voir figure 13). La fraude industrialisée vise avant tout la monétisation.

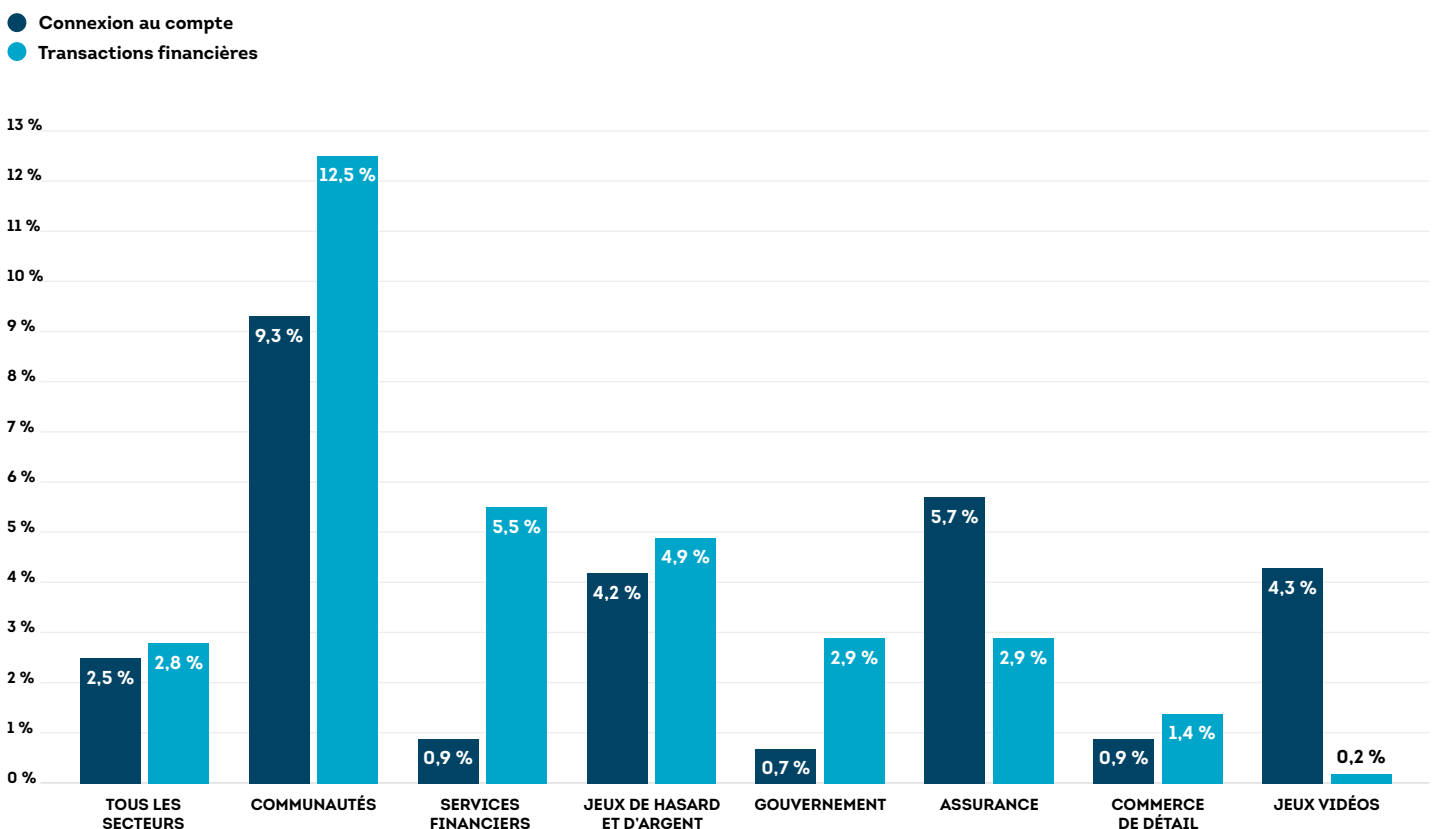
Les risques inhérents aux transactions financières confirment cette réalité. L'intelligence artificielle peut favoriser davantage cette monétisation en déterminant des cibles, en hiérarchisant les occasions et en automatisant des actions destinées à extraire de la valeur depuis des comptes existants ou au sein de secteurs où les mécanismes d'authentification continue sont moins rigoureux.

Bien que le secteur des services financiers ait consenti des investissements importants dans l'authentification des comptes et la surveillance des transactions, une optimisation excessive de l'expérience client peut rendre les transactions financières vulnérables. Parallèlement, les communautés en ligne et le secteur des jeux de hasard et d'argent sont tous deux exposés à des risques accrus en matière de transactions financières et de connexion aux comptes.

Pour les jeux de hasard et d'argent, le risque de fraude est similaire, tant pour la connexion que pour les transactions financières. Bien que la plupart des plateformes aient mis en place des règles de géolocalisation empêchant les utilisateurs d'accéder à leurs comptes dans les territoires où les jeux de hasard et d'argent sont illégaux, le vol d'argent reste problématique car les joueurs conservent des soldes en espèces et des bonis. Si les jeux de hasard et d'argent sont soumis à des réglementations anti-blanchiment similaires à celles des services financiers, un secteur reposant sur un volume important de transactions financières reste une cible privilégiée. Les communautés reposent sur la confiance entre leurs membres et proposent souvent des processus de création de comptes simplifiés; il en résulte un risque supérieur à la moyenne en matière de connexion aux comptes et de réalisation de transactions. Selon le modèle économique de la communauté, ces plateformes offrent aux criminels des occasions d'agir à chaque étape de la chaîne de valeur de la fraude. Amplifiées par l'intelligence artificielle, ces communautés sont particulièrement vulnérables aux identités synthétiques, à l'usurpation d'identité, aux escroqueries liées aux achats et à la liquidation d'actifs.

Figure 13 – La fraude liée aux transactions financières rivalise souvent avec le risque de fraude à la connexion, voire le dépasse

Pourcentage de types de transactions suspectés de fraude numérique dans certains secteurs au premier semestre de 2026



Source : réseau mondial de renseignement de TransUnion

MESURES RECOMMANDÉES

Ce que cela implique pour les organisations

La fraude industrialisée transforme la dynamique économique de l'attaque et de la défense. L'intelligence artificielle permet aux fraudeurs de tester, d'affiner et de déployer des attaques à grande échelle, plus rapidement que la plupart des organisations ne peuvent adapter leurs mécanismes de contrôle. Par conséquent, le risque se déplace de plus en plus vers le maillon le plus faible du parcours client, plutôt que de rester concentré sur une étape unique.

La fraude est devenue adaptative et industrialisée. Par conséquent, la prévention de la fraude doit elle aussi devenir adaptative et interconnectée. Les organisations qui s'appuient sur des contrôles statiques, des signaux isolés et des mises à jour périodiques risquent de peiner à suivre le rythme de menaces qui évoluent rapidement. Elles devraient, au contraire, tirer des enseignements en continu des nouveaux modes opératoires de fraude, centraliser les renseignements tout au long du cycle de vie du client et automatiser les prises de décision autant que possible.

1

S'aligner sur la vitesse et l'ampleur des attaques assistées par l'intelligence artificielle

Partez du principe que les attaques frauduleuses gagneront encore en efficacité, et mettez en place des défenses capables de s'adapter à un rythme équivalent.

2

Moderniser la prise de décision grâce à l'intelligence adaptative

Complétez les contrôles traditionnels par une intelligence adaptative qui apprend en continu à partir des signaux de fraude émergents et de l'évolution des techniques d'attaque.

3

Mettre en place des opérations antifraude polyvalentes et agiles

Modernisez la détection des fraudes, mais aussi les enquêtes, les prises de décision et les réponses. Le succès dépendra de plus en plus de la combinaison de données fiables, d'analyses avancées et d'automatisation pour protéger les clients tout en leur offrant une expérience optimale.

Perspectives régionales



Aperçu des États-Unis



Aux États-Unis, la fraude ne se limite plus aux tentatives de contournement des contrôles. L'exploitation de la confiance – dans les identités, les relations, les communications et les processus financiers – accélérée par l'intelligence artificielle en est désormais la caractéristique principale. Sur l'ensemble du marché, des fraudeurs, grâce à des données d'identité compromises, manipulent les procédures de règlement des litiges légitimes, usurpent l'identité d'organisations de confiance et développent progressivement des identités synthétiques.

En l'absence d'un cadre national de prévention de la fraude – tel qu'une identité numérique nationale officielle –, les fraudeurs continueront de tirer parti de la fragmentation des dispositifs de défense sur le marché américain, en orientant leurs attaques vers les canaux, processus et organisations les plus lucratifs. Dans leur ensemble, ces dynamiques font du risque lié à l'identité un défi persistant tout au long du cycle de vie du client.

PRINCIPAUX POINTS À RETENIR

La confiance dans les communications remise en question

35 %

des dirigeants d'entreprise américains ont désigné les escroqueries – ou fraudes autorisées – comme étant, pour leur organisation, la principale source de pertes liées à la fraude

Le risque lié à l'identité synthétique est important

2,4 milliards de dollars US

d'exposition des prêteurs américains liée à des identités synthétiques à la fin de juin 2026

La manipulation des systèmes de confiance est en augmentation

595 %

L'augmentation, entre janvier 2024 et juin 2026, des suppressions de créances irrécouvrables à l'initiative des consommateurs américains (pratique généralement associée au « blanchiment de fiche de crédit »)

Les communications de confiance constituent une surface d'attaque critique pour la fraude

Les fraudeurs exploitent avec succès les canaux de communication de confiance utilisés par les clients; les escroqueries – ou fraudes autorisées – représentent désormais la principale source de pertes liées à la fraude (voir figure 14). Aux États-Unis, 51 % des dirigeants d'entreprise indiquent que ce type de fraude a progressé au cours de l'année écoulée, et 67 % s'attendent à ce qu'il connaisse la plus forte augmentation au cours des deux prochaines années.

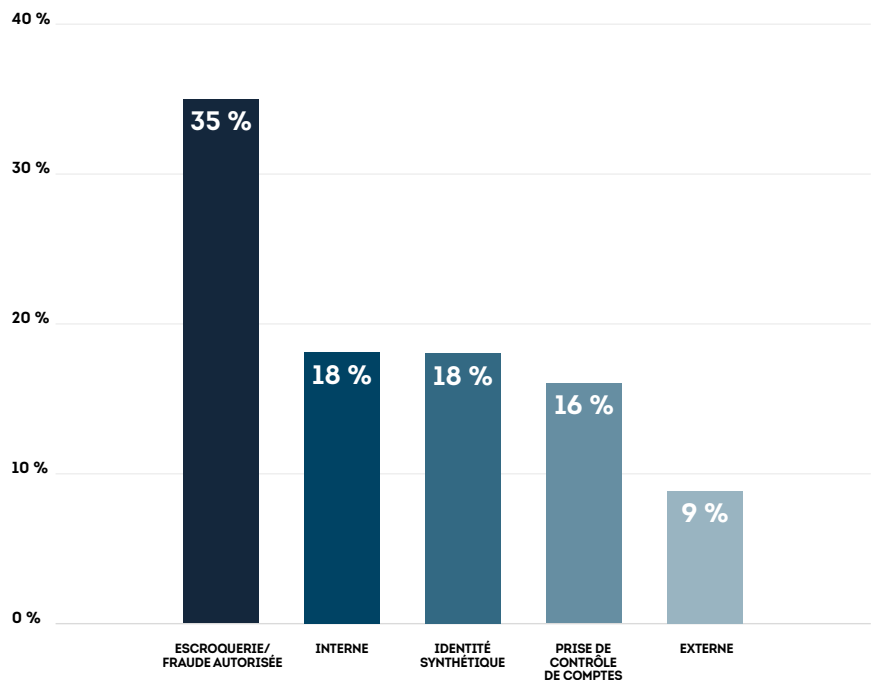
Des fraudeurs se font passer pour des organisations légitimes dans le cadre d'escroqueries téléphoniques, transformant ainsi la communication elle-même en un élément de l'usurpation d'identité. Parmi les 43 % de consommateurs américains ayant déclaré avoir été la cible de tentatives de fraude par courriel, en ligne, par appel téléphonique ou par message texte au cours d'une période récente de trois mois, 39 % ont indiqué avoir été visés par hameçonnage par courriel, 38 % par hameçonnage par message texte et 34 % par hameçonnage par appel téléphonique. Les fraudeurs ne cherchent pas toujours à tirer un profit immédiat de leurs cibles. Trois quarts des victimes d'escroqueries ont déclaré avoir communiqué des renseignements personnels – tels qu'une adresse courriel, un numéro de téléphone ou des coordonnées bancaires – à l'escroc³.

Les organisations font face à un risque croissant de fraude par identité synthétique

Les prêteurs américains restent fortement exposés au risque de fraude par identité synthétique (voir figure 15). Parmi les dirigeants d'entreprise aux États-Unis, 67 % s'attendent à ce que la fraude par identité synthétique connaisse la plus forte progression au sein de leur organisation au cours des deux prochaines années; elle se hisse ainsi, à égalité avec les escroqueries et les fraudes autorisées, au premier rang des catégories pour lesquelles une telle augmentation est anticipée. Malheureusement, 53 % d'entre eux estiment que leur organisation est mal préparée à gérer ce type de fraude, soit le pourcentage le plus élevé de toutes les catégories.

Figure 14 – Les escroqueries et les fraudes autorisées constituent la principale source de pertes liées à la fraude en entreprise aux États-Unis

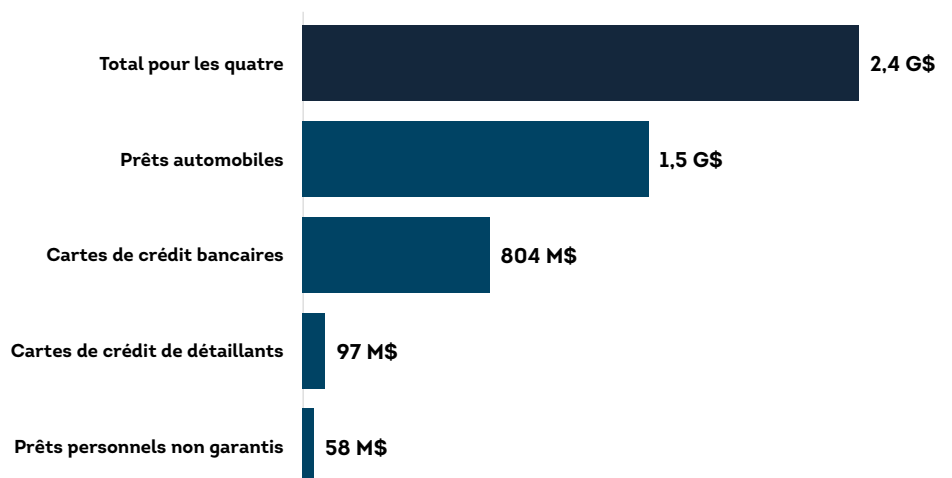
Pourcentage de dirigeants d'entreprise ayant indiqué que ces types de fraude avaient engendré les pertes les plus importantes pour leur organisation au cours de l'année écoulée



Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

Figure 15 – Les identités synthétiques exposent les prêteurs américains à des pertes sur crédit potentielles se chiffrant en milliards

Le montant total du crédit (en dollars américains) auquel les identités synthétiques ont accès pour des prêts automobiles, des cartes de crédit bancaires, des cartes de crédit de détaillants et des prêts personnels non garantis aux États-Unis, au 30 juin 2026



Source : réseau mondial de renseignement de TransUnion

Le blanchiment de fiche de crédit accroît la valeur et l'utilité des identités synthétiques

Les fraudeurs manipulent de plus en plus les systèmes de confiance sur lesquels les prêteurs s'appuient pour évaluer les risques. Plutôt que de simplement passer inaperçus, les individus mal intentionnés exploitent les procédures légitimes de règlement des litiges et de protection des consommateurs pour blanchir leur identité au moyen de fausses déclarations de fraude ou de blanchiment de fiche de crédit. Ces contestations de crédit frauduleuses peuvent entraîner la suppression de créances irrécouvrables, effaçant ainsi le compte ou la transaction litigieux du profil de crédit d'une personne. Les suppressions de créances irrécouvrables à l'initiative des consommateurs américains ont augmenté de 595 % entre janvier 2024 et juin 2026, s'accompagnant d'une hausse substantielle des pertes (voir figure 16).

Les renseignements négatifs supprimés peuvent masquer des pertes antérieures, ce qui augmente l'exposition des prêteurs. Une analyse exclusive de TransUnion indique que les comptes ouverts à la suite de la suppression de créances irrécouvrables présentent des taux de radiation précoce nettement plus élevés (12,5 % contre 3,7 % pour les populations de référence). Ce phénomène met en évidence l'écart croissant entre le risque perçu et le risque réel, tout en prolongeant la durée de vie d'identités synthétiques qui ont réussi à passer entre les mailles du filet.

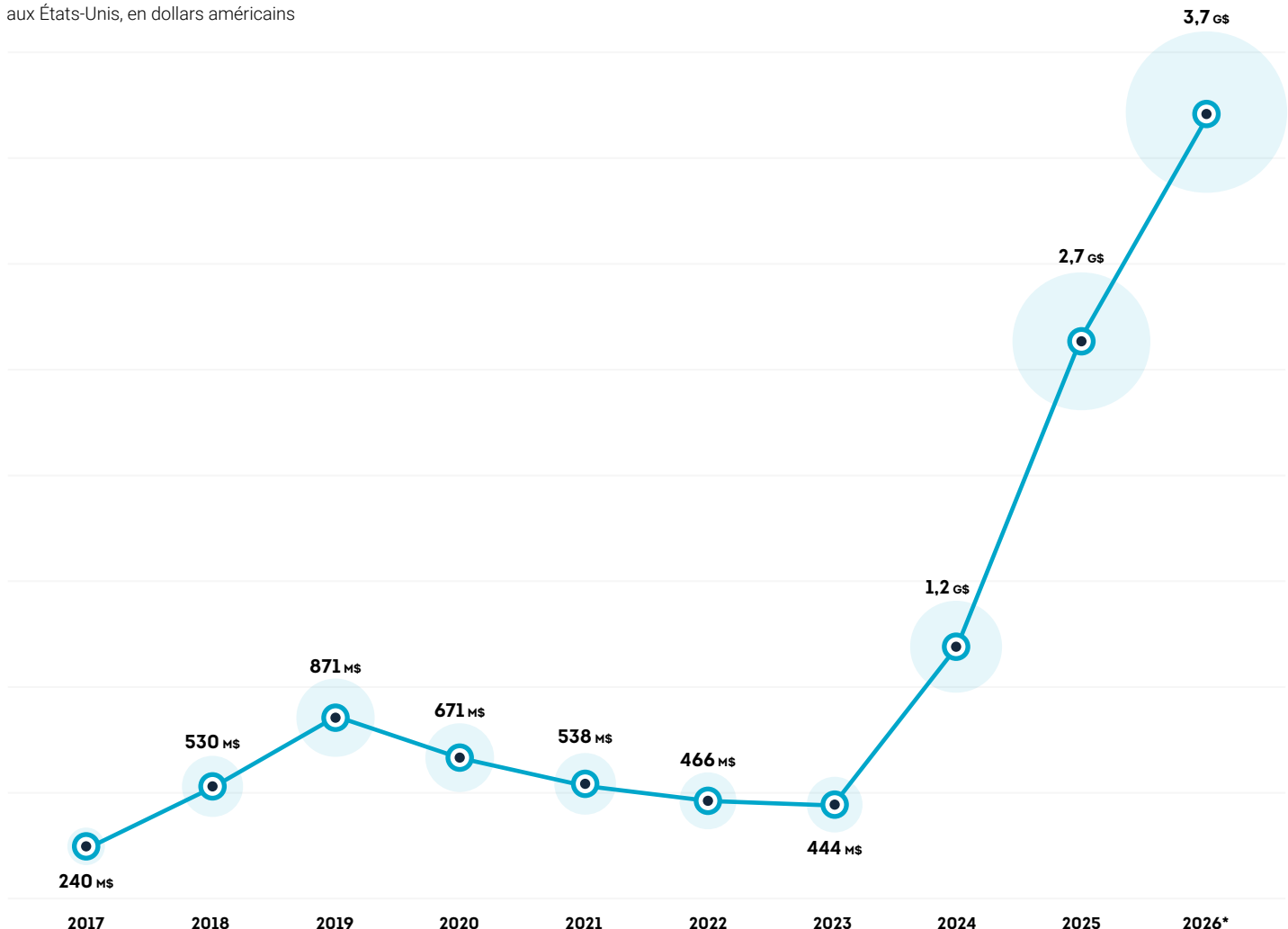
595 %

L'augmentation des suppressions de créances irrécouvrables à l'initiative des consommateurs américains sur une période récente de 18 mois

Source : réseau mondial de renseignement de TransUnion

Figure 16 – Les suppressions de données à l'initiative des consommateurs masquent des milliards de pertes sur créances historiques

Pertes liées aux créances irrécouvrables effacées des fiches de crédit en raison de suppressions atypiques effectuées par les consommateurs aux États-Unis, en dollars américains



Source : réseau mondial de renseignement de TransUnion

* Estimation pour l'ensemble de l'année 2026 fondée sur la tendance du premier semestre

Aperçu du Canada



Au Canada, le défi lié à la fraude se concentre de plus en plus sur les relations clients existantes, plutôt que sur l'étape de l'entrée en relation. La confiance établie lors de l'intégration ne suffit plus, car le risque de fraude apparaît désormais bien avant la création du compte et persiste tout au long des phases de connexion, de gestion du compte et des transactions. Les communications avec les clients sont devenues une vulnérabilité critique : les fraudeurs s'en servent pour gagner en crédibilité, recueillir des identifiants et faciliter, par la suite, la compromission de comptes. Plus d'un tiers (34 %) des dirigeants d'entreprise canadiens ont indiqué que l'ampleur ou la sophistication croissantes de la fraude font peser une pression importante, voire sévère, sur leur organisation; par ailleurs, 47 % d'entre eux se disent extrêmement ou très préoccupés par le fait que le risque de fraude évolue plus rapidement que la capacité de leur organisation à le détecter et à le prévenir.

PRINCIPAUX POINTS À RETENIR

Le risque lié à l'identité ne se limite plus à l'ouverture de compte

226 %

L'augmentation, pour les abonnés canadiens, de la part des tentatives de transactions financières suspectées de fraude numérique, entre la première période analysée (premier semestre de 2022) et le premier semestre de 2026

Les communications exposent les clients à des risques de fraude sur leur compte

42 %

des dirigeants d'entreprise canadiens ont indiqué que les escroqueries et les fraudes autorisées avaient augmenté au cours de l'année écoulée, ce qui en fait le type de fraude le plus fréquent

La connexion au compte constitue le principal point d'exposition à la fraude tout au long du cycle de vie du client

La concentration de la fraude autour de l'étape de connexion reflète des évolutions plus larges du paysage de la fraude au Canada. L'activité de connexion aux comptes représente la part la plus importante des tentatives de fraude numérique suspectées au Canada (voir figure 17). Plutôt que de miser uniquement sur la création de comptes frauduleux, les criminels exploitent des comptes existants en utilisant des identifiants dérobés, des campagnes d'hameçonnage et des techniques d'ingénierie sociale.

Les tendances en matière de fraude numérique révèlent une importance croissante accordée à la monétisation. Au Canada, la part des tentatives de transactions financières suspectées de fraude numérique a augmenté de 226 % entre le premier semestre de 2022 (période la plus ancienne prise en compte dans l'analyse) et le premier semestre de 2026, contre une hausse de 108 % pour les tentatives de connexion à des comptes.

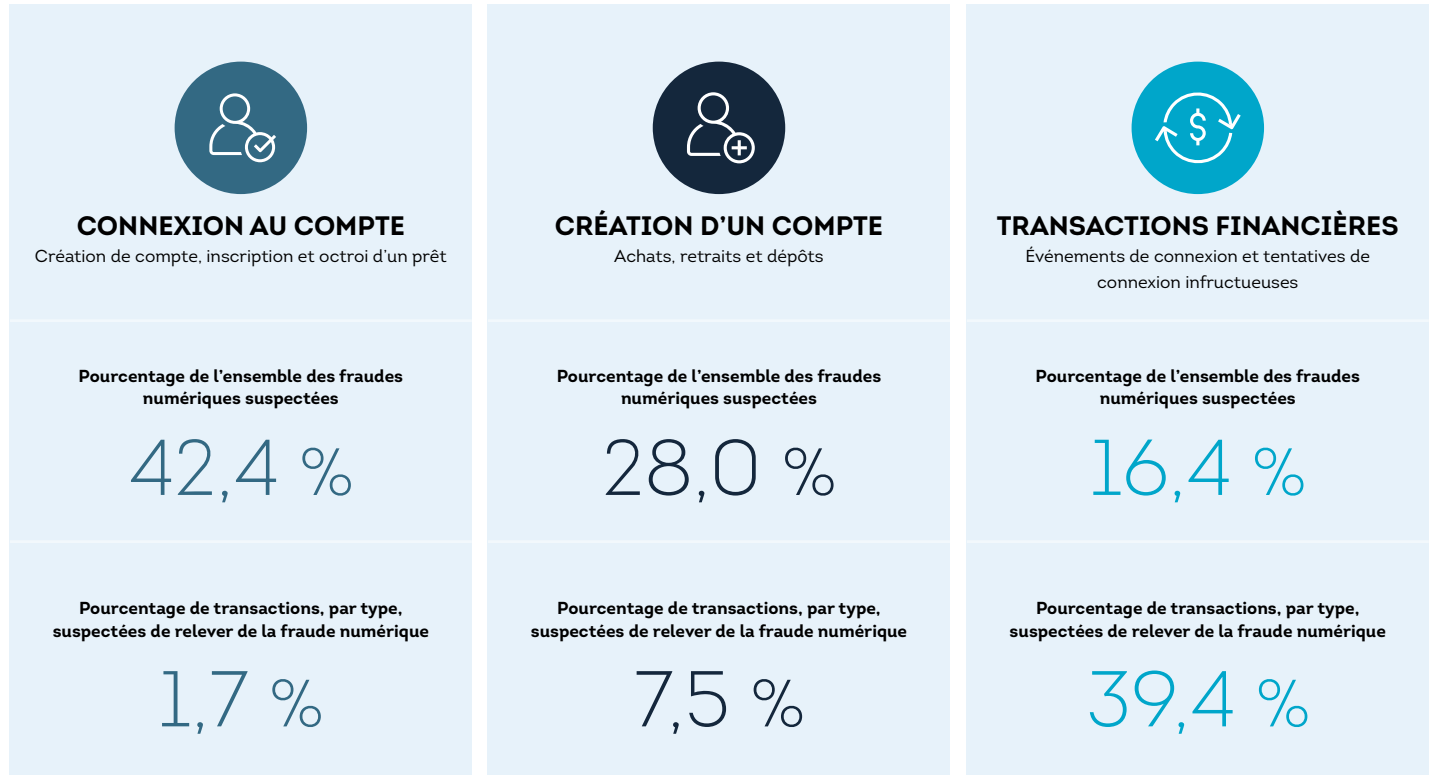
44 %

des dirigeants d'entreprise canadiens ont indiqué que la prise de contrôle de compte figurait parmi les types de risques de fraude auxquels leur organisation est la moins préparée à faire face

Source : enquête de TransUnion sur la fraude en entreprise, juin 2026

Figure 17 – La connexion aux comptes constitue le principal point d'exposition à la fraude numérique au Canada

Fraude numérique tout au long du parcours client au premier semestre de 2026



Source : réseau mondial de renseignement de TransUnion

L'exposition à la fraude demeure généralisée, les consommateurs étant confrontés à des escroqueries de plus en plus sophistiquées

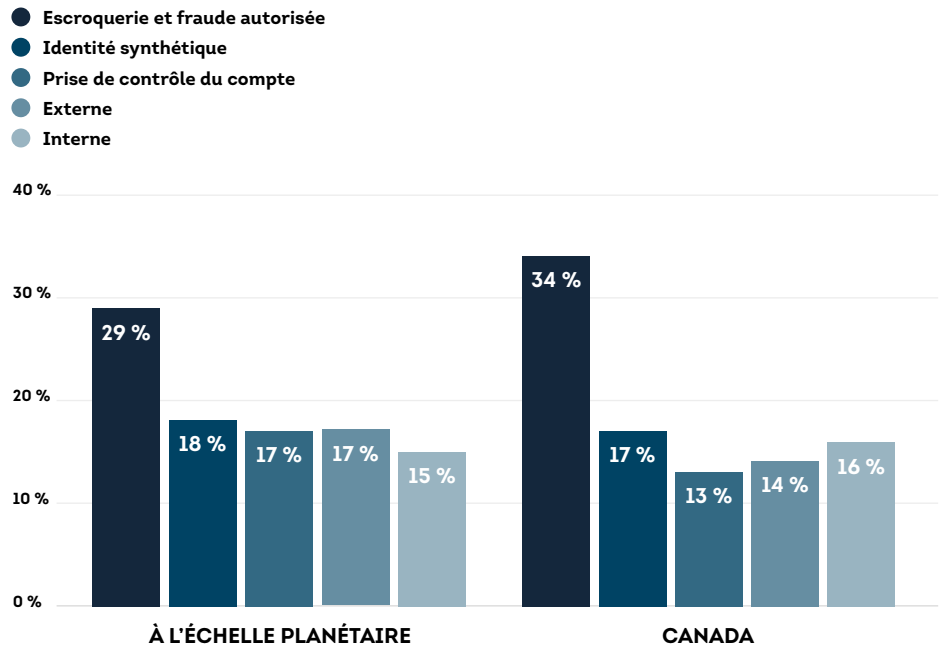
Les organisations doivent redoubler d'efforts pour renforcer la protection de la confiance de leurs clients. Au Canada, les dirigeants d'entreprise désignent les escroqueries – ou fraudes autorisées – comme la source la plus fréquente de pertes liées à la fraude. Ce constat rejoint les tendances observées à l'échelle mondiale et témoigne d'une évolution croissante vers des attaques qui exploitent la confiance (voir figure 18).

Près de la moitié (49 %) des consommateurs canadiens ont déclaré avoir été ciblés par une tentative de fraude – par courriel, en ligne, par appel téléphonique ou par messagerie texte – au cours d'une période récente de trois mois; 6 % d'entre eux ont indiqué en avoir été victimes (voir la figure 19). Bien qu'une faible majorité ait affirmé ne pas s'être rendu compte qu'elle était ciblée, ces données soulignent à quel point les tentatives de fraude sont devenues courantes dans les interactions numériques quotidiennes des Canadiens.

Les mécanismes de fraude les plus fréquemment signalés illustrent le rôle croissant des communications dans les attaques fondées sur l'usurpation d'identité. Près de la moitié (47 %) des consommateurs canadiens ayant déclaré avoir été la cible de fraudes numériques au cours d'une période récente de trois mois ont mentionné des tentatives d'hameçonnage par courriel, suivies de près par l'hameçonnage vocal (44 %) et l'hameçonnage par message texte (40 %). Par ailleurs, 42 % des dirigeants d'entreprise canadiens ont indiqué que les escroqueries avaient augmenté au cours de l'année écoulée, plus que tout autre type de fraude.

Figure 18 – Les escroqueries ou fraudes autorisées constituent la principale source de pertes liées à la fraude signalées

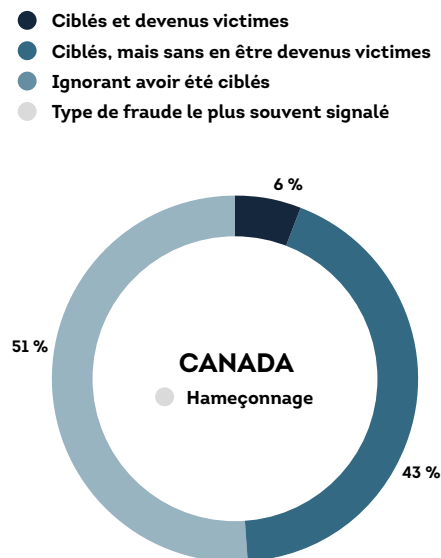
Pourcentage de dirigeants d'entreprise ayant indiqué que ces types de fraude avaient engendré les pertes les plus importantes pour leur organisation au cours de l'année écoulée



Enquête de TransUnion sur la fraude en entreprise, juin 2026

Figure 19 – Près de la moitié des Canadiens ont déclaré avoir été la cible de fraudes

Pourcentage de consommateurs canadiens ayant déclaré avoir été ciblés par des fraudeurs au cours des trois derniers mois – par le biais de courriels, d'activités en ligne, d'appels téléphoniques ou de messages textes – ainsi que le type de fraude le plus souvent signalé

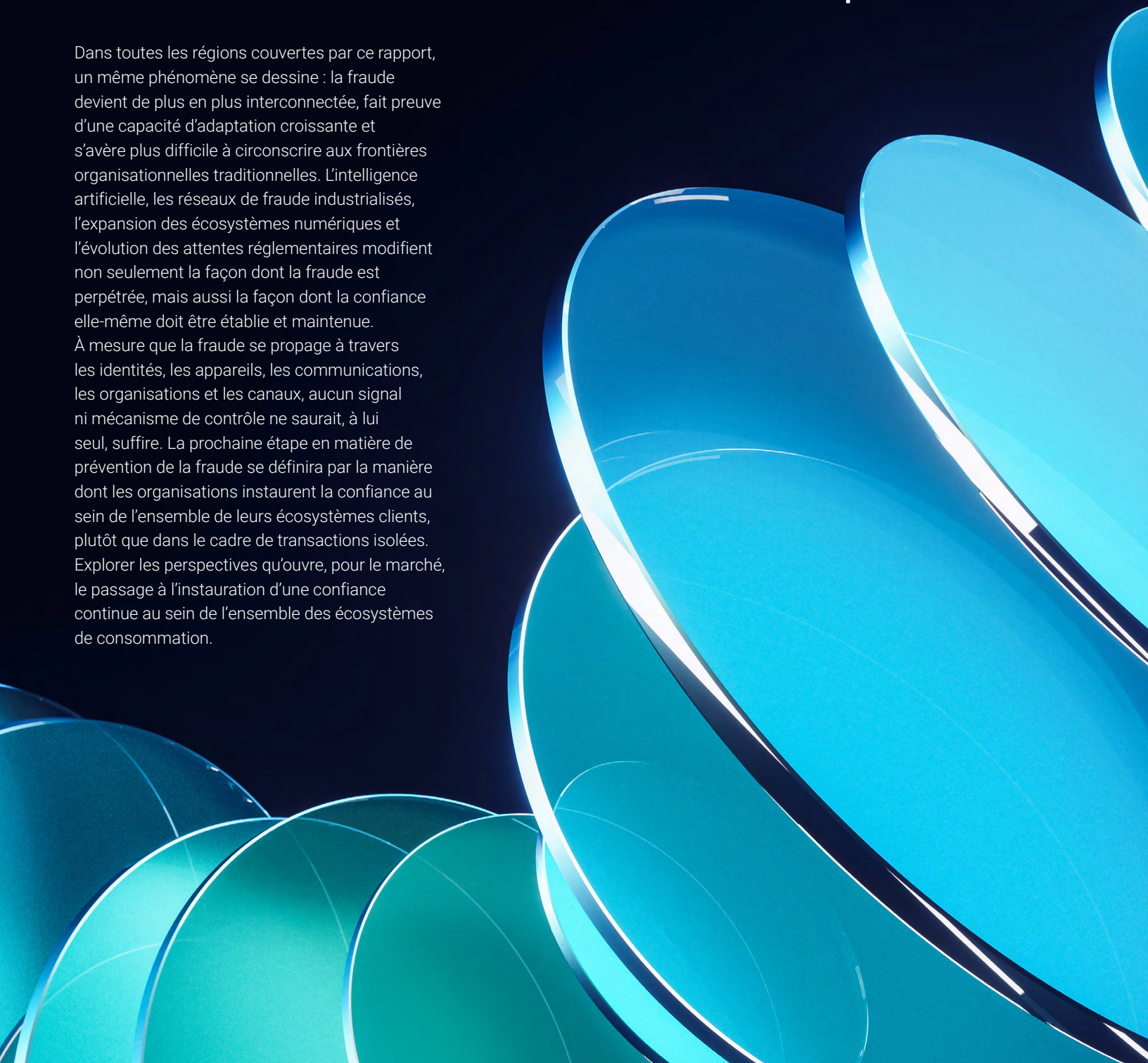


Source : sondage Consumer Pulse, TransUnion, juillet 2026

Façonner la prochaine ère de la confiance numérique

Dans toutes les régions couvertes par ce rapport, un même phénomène se dessine : la fraude devient de plus en plus interconnectée, fait preuve d'une capacité d'adaptation croissante et s'avère plus difficile à circonscrire aux frontières organisationnelles traditionnelles. L'intelligence artificielle, les réseaux de fraude industrialisés, l'expansion des écosystèmes numériques et l'évolution des attentes réglementaires modifient non seulement la façon dont la fraude est perpétrée, mais aussi la façon dont la confiance elle-même doit être établie et maintenue.

À mesure que la fraude se propage à travers les identités, les appareils, les communications, les organisations et les canaux, aucun signal ni mécanisme de contrôle ne saurait, à lui seul, suffire. La prochaine étape en matière de prévention de la fraude se définira par la manière dont les organisations instaurent la confiance au sein de l'ensemble de leurs écosystèmes clients, plutôt que dans le cadre de transactions isolées. Explorer les perspectives qu'ouvre, pour le marché, le passage à l'instauration d'une confiance continue au sein de l'ensemble des écosystèmes de consommation.



1

Les consommateurs se protègent des risques numériques grâce à des applications de sécurité conçues à cet effet

La prochaine génération de protection de l'identité reposera sur des boucliers numériques fondés sur l'intelligence artificielle, qui aideront les consommateurs à déterminer si des interactions sont dignes de confiance avant d'agir.

Signaux du marché

Les applications mobiles destinées aux consommateurs évaluent déjà l'identité de l'appelant, la réputation des entreprises, les signalements d'escroquerie ainsi que la vérification des messages.

Comment se préparer

Il faut aller au-delà de la surveillance de l'identité et de la restauration après un incident, et privilégier une protection proactive des consommateurs qui détecte les manipulations précocement et les aide à éviter des actions irréversibles.

2

La connexion, telle qu'on la connaît, est appelée à disparaître.

Les clés d'accès, les appareils de confiance, les portefeuilles numériques et les identifiants réutilisables rendront les méthodes de connexion traditionnelles moins visibles et moins centrales.

Signaux du marché

Les clés d'accès sont disponibles au sein des principaux écosystèmes technologiques. Les portefeuilles numériques et les systèmes d'identité nationaux – notamment Apple Wallet, le portefeuille d'identité numérique de l'UE, Aadhaar et Singpass – continuent de se développer.

Comment se préparer

Concevez l'authentification autour d'une identité établie en continu – à travers les appareils, les identifiants et les interactions – plutôt qu'au moment d'une connexion unique

3

La lutte contre la fraude devient alors un réseau, et non plus un simple produit.

L'intelligence collective révélera des relations, des schémas et des menaces qu'aucune organisation ne peut détecter seule.

Signaux du marché

Les réseaux de partage de données, tels que Cifas⁸, Stop Scams UK⁹ et l'Anti-Scam Centre de Singapour¹⁰, illustrent cette évolution. La réglementation américaine favorise également l'échange de renseignements¹¹.

Comment se préparer

Déterminez dans quelle mesure les renseignements échangés au sein d'un consortium, la collaboration préservant la confidentialité et les partenariats intersectoriels peuvent renforcer vos dispositifs de défense propriétaires.

4

Prouver son identité ne suffira plus à instaurer une confiance numérique

La confirmation de l'identité restera indispensable, mais elle ne prouvera pas pour autant qu'une interaction est digne de confiance.

Signaux du marché

La multiplication des escroqueries et des fraudes autorisées met en évidence les limites de la seule vérification d'identité.

Comment se préparer

Associez la vérification d'identité aux données relatives aux appareils, aux comportements, aux communications et au réseau tout au long du cycle de vie client. Posez-vous non seulement la question « Est-ce la bonne personne ? » mais aussi « Peut-on faire confiance à cette interaction ? »

5

Le renseignement en matière de fraude adoptera un langage opérationnel commun

Le secteur adoptera des méthodes plus cohérentes pour décrire les tactiques, techniques et comportements liés à la fraude.

Signaux du marché

Le « Fight Fraud Framework » de MITRE propose une taxonomie fondée sur les comportements pour les acteurs de la fraude financière¹².

Comment se préparer

Alignez les classifications de la fraude sur les cadres émergents et concevez des architectures de données qui prennent en charge des renseignements sur la fraude exploitables par des machines et interopérables.

L'avenir connecté de la prévention de la fraude

La leçon la plus importante à tirer du paysage mondial de la fraude n'est pas que celle-ci est devenue plus sophistiquée, mais que la confiance a pris davantage de valeur.

Pendant des décennies, les organisations ont considéré la confiance comme un événement ponctuel, établi lors de l'intégration, de l'authentification ou de la validation d'une transaction. Ce modèle est de plus en plus en décalage avec la réalité de la fraude numérique actuelle.

La fraude exploite désormais les identités une fois qu'elles ont été vérifiées, les communications après leur acheminement et les relations une fois qu'elles ont été établies. Les organisations ne peuvent plus traiter l'expérience client, la gestion des risques et la prévention de la fraude comme des domaines indépendants. Ces éléments sont devenus des composantes interdépendantes d'un même défi : déterminer si une interaction numérique est digne de confiance.

Les organisations qui réussiront ne seront pas nécessairement celles qui détecteront le plus grand nombre de fraudes. Ce seront celles qui inspireront la plus grande confiance à leurs clients, élimineront les frictions inutiles et prendront de meilleures décisions grâce à des renseignements liés.

Dans la prochaine ère du commerce numérique, la confiance ne sera plus un mécanisme de contrôle. Elle constituera un atout. Et, de plus en plus, elle représentera un avantage concurrentiel.

1,2,3 Javelin Group. 2026 Identity Fraud Study the Illusion of Progress, avril 2026.

4 International Development Bank. *Beyond Cash: The Digital Payments Revolution in Latin America and the Caribbean*, septembre 2025.

5 Merchant Risk Council. 2026 Global eCommerce Payments & Fraud Report, mars 2026.

6 INTERPOL. Édition 2026 du rapport INTERPOL sur l'évaluation des cybermenaces en Afrique, août 2026.

7 MSN, SIM card Aadhaar fraud alert: How your biometric verification could be misused during SIM activation, juillet 2026.

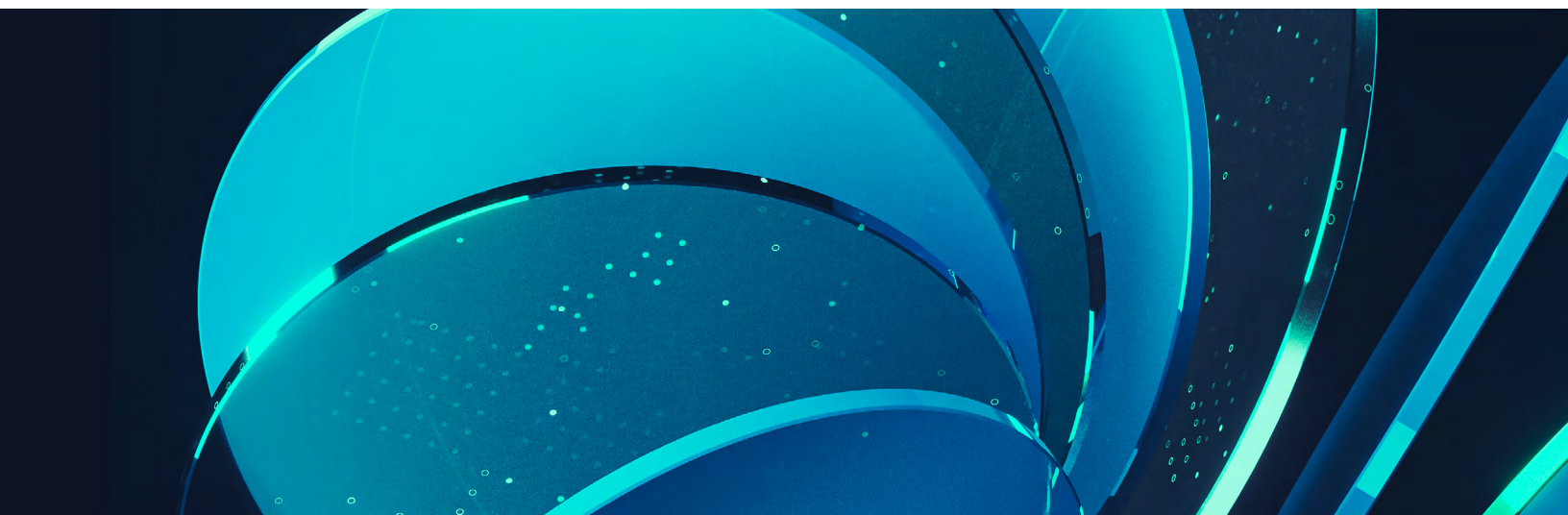
8 Cifas.

9 Stop Scams UK.

10 Anti-Scam Centre Singapore.

11 Département du Trésor des États-Unis, Financial Crimes Enforcement Network (FinCEN), *Patriot Act* des États-Unis, article 314(b), fiche d'information, 12 juin 2026.

12 Center for Threat Informed Defense de MITRE, Fight Fraud Framework, avril 2026.



À propos de l'étude

Ce rapport combine les résultats d'enquêtes menées auprès des entreprises et des consommateurs avec des enseignements tirés des données exclusives de TransUnion en matière de fraude, d'identité, de crédit et de communications.

Enquête sur la fraude en entreprise

Les résultats de l'enquête présentée dans ce rapport reposent sur les réponses de 1 600 décideurs en matière de fraude et de risques, issus de grandes organisations en contact direct avec les consommateurs, réparties dans les pays et territoires suivants : Brésil, Canada, Hong Kong, Inde, Philippines, Espagne, Royaume-Uni et États-Unis.

L'enquête a été menée en ligne du 5 au 12 juin 2026 par TransUnion, en partenariat avec le fournisseur de recherche tiers Dynata. Les répondants exerçaient des responsabilités de gestion liées à la fraude ou aux risques, au sein d'organisations réalisant un chiffre d'affaires annuel supérieur à 300 millions de BRL au Brésil, 300 millions de CAD au Canada, 200 millions de HKD à Hong Kong, 1 milliard d'INR en Inde, 1 milliard de PHP aux Philippines, 150 millions d'EUR en Espagne, 200 millions de GBP au Royaume-Uni et 200 millions d'USD aux États-Unis.

L'enquête a été menée auprès d'un panel de recherche en ligne; les participants y ont répondu depuis un ordinateur, un appareil mobile ou une tablette.

La somme des pourcentages peut ne pas atteindre 100 % en raison des arrondis, du fait que certaines questions autorisaient des réponses multiples, ou parce que les réponses « ne sait pas » et « aucune de ces propositions » ont été exclues.

Sondage Consumer Pulse

Les résultats du sondage auprès des consommateurs présentés dans ce rapport reposent sur les réponses de plus de 13 500 adultes âgés de 18 ans et plus, répartis sur 19 marchés à travers le monde.

Le sondage a été mené par TransUnion, en partenariat avec le fournisseur d'études tiers Dynata, via un panel de recherche en ligne. La collecte des données s'est déroulée entre le 10 février et le 7 août 2026 au Botswana, au Brésil, au Canada, au Chili, en Colombie, en République dominicaine, au Guatemala, à Hong Kong, en Inde, au Kenya, au Mexique, en Namibie, aux Philippines, au Rwanda, en Afrique du Sud, en Espagne, au Royaume-Uni, aux États-Unis et en Zambie. Les répondants ont rempli le sondage au moyen d'ordinateurs, d'appareils mobiles et de tablettes.

Les questions du sondage étaient proposées en chinois (Hong Kong), en anglais, en français (Canada), en portugais (Brésil) et en espagnol (Colombie, République dominicaine, Guatemala et Espagne). Afin de garantir des résultats représentatifs, des quotas ont été utilisés pour équilibrer les réponses en fonction de caractéristiques démographiques clés, notamment l'âge, le sexe et le revenu.

La somme des pourcentages peut ne pas atteindre 100 % en raison d'arrondis ou du fait que certaines questions permettaient des réponses multiples.

Violations de données

Les conclusions relatives aux violations de données présentées dans ce rapport sont issues de la base de données exclusive de TransUnion sur les violations de données, gérée en partenariat avec l'Identity Theft Resource Center. Cette base de données recense les incidents d'exposition de données survenus aux États-Unis et rendus publics, en s'appuyant sur des renseignements provenant de diverses sources, notamment les procureurs généraux des États, les déclarations des organisations, les cabinets d'avocats et les experts en cybersécurité.

Chaque violation est évaluée à l'aide de l'outil TransUnion TruEmpower^{MD} Identity Threat Profile, qui analyse les identifiants exposés, les caractéristiques de la violation ainsi que le risque qui en découle pour les consommateurs. Un score de gravité, allant de 1 à 10, est attribué à chaque violation; 1 correspond au niveau de risque le plus faible et 10 au niveau le plus élevé.

Les pourcentages communiqués concernant les données d'identité exposées sont calculés uniquement à partir des violations ayant entraîné la divulgation d'identifiants compromis; ils ne reflètent donc pas l'ensemble des violations de données signalées.

Les données relatives aux violations constituent l'un des multiples indicateurs de risque utilisés pour élaborer l'« Identity Safety Score » de TransUnion, lequel permet d'évaluer le profil de risque global lié à l'identité d'un individu et de hiérarchiser les mesures de protection recommandées.

Fraude numérique

Les conclusions relatives à la fraude numérique présentées dans ce rapport sont issues des données de TransUnion, qui portent sur des milliards de transactions effectuées sur plus de 40 000 sites Web et applications à travers le monde.

Le taux de fraude numérique suspectée correspond au pourcentage de transactions détectées par les clients de TransUnion comme étant frauduleuses ou contraires aux politiques de leur organisation. Cela inclut les transactions refusées en temps réel en raison d'indicateurs de fraude ou de violations de politique, ainsi que les transactions confirmées ultérieurement dans le cadre d'investigations menées par le client ou par TransUnion.

Les analyses par pays et par région reposent sur des transactions liées à des clients exerçant leurs activités sur le marché concerné. Les résultats mondiaux reflètent l'activité transactionnelle dans l'ensemble des pays représentés au sein du réseau TransUnion et ne se limitent pas aux marchés mis en avant dans ce rapport.

Lors de l'analyse du volume des transactions par étape du parcours client, les transactions classées dans la catégorie « autre » ont été exclues. Par conséquent, la somme des pourcentages correspondant aux différentes étapes du parcours client peut ne pas atteindre 100 %.

Appels sortants

Les résultats des appels sortants présentés dans ce rapport sont dérivés des données des opérateurs de téléphonie mobile associées aux appels vers des consommateurs américains au cours desquels des fraudeurs se sont fait passer pour des institutions financières légitimes.

Le taux d'appels usurpés signalé reflète les cas dans lesquels les renseignements d'identité de l'appelant ont été falsifiés pour donner l'impression que les appels provenaient d'une institution financière de confiance.

Étant donné que les opérateurs de téléphonie mobile peuvent tenter de rétablir à plusieurs reprises des appels ayant échoué, les volumes et les taux d'appels usurpés signalés pourraient être légèrement plus élevés.

Fraude par identité synthétique

Les conclusions relatives à la fraude par identité synthétique présentées dans ce rapport sont principalement issues de la base de données sur le crédit à la consommation de TransUnion aux États-Unis, qui contient des renseignements sur le crédit concernant environ 400 millions de consommateurs répartis dans les États, territoires et installations militaires des États-Unis, ainsi qu'à l'étranger.

La base de données intègre plus de 50 ans d'historique de crédit des consommateurs. Les analyses relatives à la fraude par identité synthétique ont porté sur les activités de crédit aux États-Unis enregistrées entre le 1^{er} janvier 2009 et le 30 juin 2026.

Les estimations de l'exposition des prêteurs ont été calculées selon une méthodologie exclusive de TransUnion, conçue pour quantifier les pertes potentielles des prêteurs liées à la fraude par identité synthétique.

À PROPOS DE TRANSUNION (NYSE : TRU)

TransUnion est une entreprise mondiale de renseignements et de connaissances qui compte plus de 13 000 associés en activité dans plus de 30 pays. Nous rendons la confiance possible en veillant à ce que chaque personne soit représentée de manière fiable sur le marché. Nous le faisons avec une image fidèle (Tru^{MD}) de chaque personne : un aperçu exploitable des consommateurs, géré avec soin. Grâce à nos acquisitions et à nos investissements technologiques, nous avons développé des solutions innovantes qui vont au-delà de notre compréhension approfondie du crédit de base, dans des domaines tels que le marketing, la fraude, le risque et l'analyse avancée. Par conséquent, les consommateurs et les entreprises peuvent effectuer des transactions en toute confiance et réaliser de grandes choses. Nous appelons cela l'information au service du bien^{MD} et cela permet à des millions de personnes dans le monde entier de bénéficier d'occasions économiques, de vivre des expériences extraordinaires et de s'émanciper.

Associez une détection des fraudes performante à des analyses approfondies pour protéger votre entreprise et vos clients. Découvrez dès aujourd'hui les [solutions de prévention de la fraude de TransUnion.](#)
