Deloitte.

Commerce agentique : comprendre les risques de fraude et saisir les occasions

Composer avec les nouvelles réalités du commerce et des paiements agentiques

Décembre 2025

SOMMAIRE : LA FRAUDE À L'ÈRE DE L'IA AGENTIQUE

Nous estimons que l'intelligence artificielle (IA) agentique générera environ 17,5 billions de dollars[1] en marchandises brutes d'ici 2030. Dans un contexte où les commerçants s'adaptent à l'évolution du comportement des consommateurs, atténuer les risques de fraude est un besoin essentiel. Pour évaluer l'incidence de l'augmentation connexe de la fraude reposant sur l'IA dans le commerce de détail, Deloitte a mené une étude auprès d'un vaste éventail de commerçants. Il en ressort que **69 % d'entre eux ont été ciblés par des fraudes commises à l'aide de l'IA au cours de la dernière année, alors que seulement 3 % s'estimaient bien préparés pour faire face à ces attaques, de plus en plus nombreuses**. Ces constatations mettent en lumière le besoin urgent, pour les commerçants, d'adopter des stratégies proactives et globales de lutte contre la fraude, non seulement pour assurer la pérennité de leurs activités, mais aussi afin de tirer parti de la valeur croissante que l'IA agentique peut générer pour leurs clients.

Principaux constats

Adoption de l'IA agentique

Augmentation des fraudes de 37 % du T2 2025 au T3 2025 chez les commerçants dont une part importante de la fréquentation est assistée par l'IA.

*Nous avons observé qu'au T3, **la facilitée ou assistée par des outils utilisant l'IA générative présente plus de risques que la fréquentation assistée par des moteurs de recherche traditionnels et qu'elle est 1,7 fois plus susceptible** d'être de nature frauduleuse[2].*

Menaces qui évoluent

87 % des commerçants qui ont répondu au sondage de Deloitte prévoient une augmentation modérée à forte des attaques à l'aide de l'IA au cours des 12 prochains mois.

*La « fraude en tant que service » est de plus en plus répandue et les obstacles empêchant les fraudes sophistiquées sont en voie de disparaître, ce qui risque non seulement d'entraîner des pertes financières pour les commerçants, **mais aussi de nuire à leur croissance et d'effriter la valeur offerte aux clients et leur loyauté**.*

Priorités stratégiques

95 % des commerçants qui ont répondu au sondage de Deloitte planifient d'adapter leur stratégie de lutte contre la fraude et d'inclure l'IA agentique à leurs priorités stratégiques.

*Même si la majorité des commerçants (82 %) croient que l'analytique avancée est l'outil le plus efficace pour atténuer les risques, ils estiment également qu'il est primordial d'adopter une approche globale axée sur les piliers de la fraude **pour tous les points de contact avec les clients afin de soutenir le déploiement d'une stratégie liée à l'IA agentique**.*

Surmonter les obstacles

52 % des commerçants ayant répondu au sondage de Deloitte ont indiqué que le financement pour la mise en œuvre des capacités de gestion de la fraude constituait leur principal obstacle, suivi des compétences et des limites technologiques.

*Une stratégie efficace pour surmonter ces obstacles consiste à aligner les **indices clés de performance (ICP) des activités** et **des opérations avec les indicateurs de risque clés (IRC) liés à la gestion de la fraude**, afin de favoriser une croissance innovante et centrée sur le client.*

L’IA agentique devrait générer 17,5 billions de dollars pour les commerces[1].

Grâce à l’IA agentique, les consommateurs bénéficient de recommandations personnalisées, d’une résolution plus rapide des problèmes et d’expériences de paiement harmonieuses.

Cet outil offre une nouvelle occasion de répondre aux attentes croissantes des clients en matière de rapidité et de personnalisation, tout en tirant parti de nouvelles occasions de croissance et en rehaussant l’efficacité opérationnelle.

Le commerce agentique fait référence aux expériences de magasinage qui se font à l'aide de l'IA : des agents autonomes agissant au nom des consommateurs trouvent, comparent et achètent des produits en fonction des préférences des consommateurs et des données contextuelles recueillies grâce aux requêtes. Les paiements agentiques complètent ce type de commerce en effectuant des transactions sur la base d'autorisations et de mandats intégrés, créant ainsi un processus d'achat harmonieux de bout en bout. Les consommateurs adoptant de plus en plus cette approche, les commerçants doivent entreprendre de vastes chantiers pour, entre autres, réinventer leur modèle d'engagement, mettre l'accent sur la personnalisation et intégrer des systèmes intelligents afin de répondre aux attentes des consommateurs.

70 %

des consommateurs sont à l'aise avec l'idée que des agents d'IA fassent leurs achats à leur place[3]

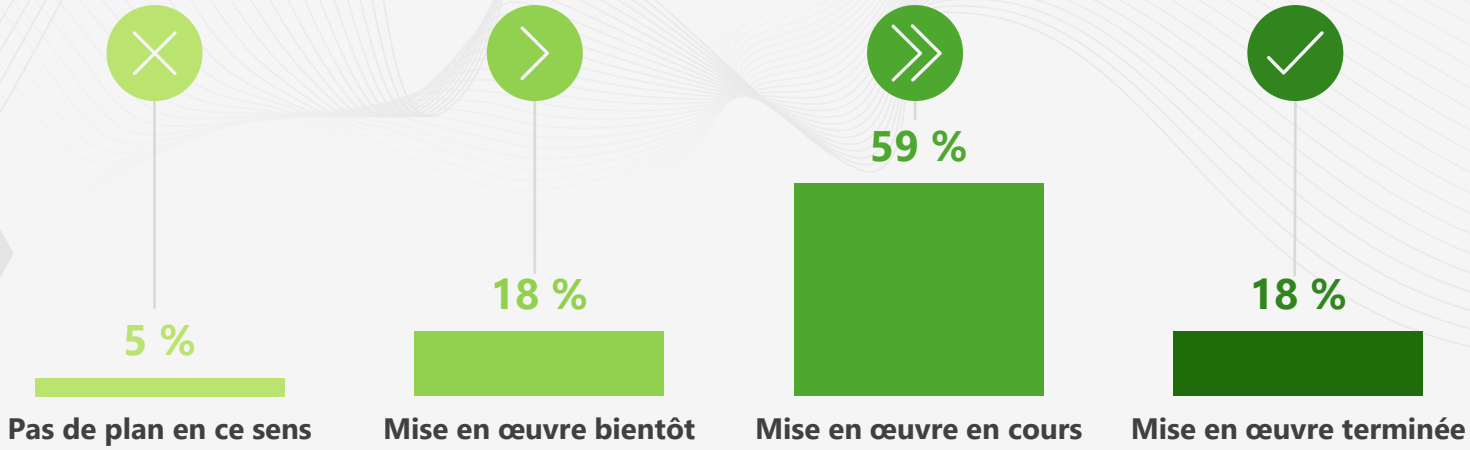
3 X

augmentation des commandes passées avec l'IA auprès de commerçants de janvier à septembre 2025[4]

30 %

de la valeur prévue des transactions de commerce numérique sera influencée par l'IA agentique d'ici 2030[1]

59 % des commerçants ont affirmé avoir entamé leur parcours d'adoption de l'IA agentique et 18 % d'entre eux croient avoir mis en œuvre un ensemble complet de capacités d'IA agentique.



Même si le commerce et les paiements fondés sur l'IA agentique gagnent rapidement en popularité auprès des consommateurs, la technologie sous-jacente ajoute également de nouvelles dimensions aux risques de fraude. L'IA agentique peut servir de moteur clé en main pour commettre des fraudes facilitées par l'IA : un système autonome capable d'exécuter des séquences complexes, ce qui en fait un outil puissant pour les fraudeurs. Les mêmes fonctions qui améliorent l'expérience des clients et la rapidité des opérations, tout en réduisant au minimum la supervision humaine, peuvent également être exploitées afin de contourner les contrôles traditionnels utilisés pour lutter contre la fraude. Dans un contexte où l'adoption de ces technologies s'accélère, les commerçants doivent reconnaître que les risques évoluent et que la mise en œuvre de stratégies de prévention de la fraude proactives et habilitées par l'IA est nécessaire pour maintenir la confiance et protéger leurs revenus.

L'innovation amenée par l'IA transforme les risques de fraude

2023 :
Montée de l'IA générative

Explosion des outils fondés sur des GML, par exemple ChatGPT

2024 :
Émergence de l'IA agentique

Premières solutions fondées sur des actions autonomes et des intégrations de GML

2025 :
Adoption des agents d'IA

De janvier 2025 à août 2025, la fréquentation facilitée par l'IA agentique a augmenté de plus de 1 300 %[5]

Fraudes avant l'ère de l'IA agentique

- Les grands modèles de langage (GML) ont élargi l'accès aux connaissances et compétences requises pour commettre des fraudes, mais celles-ci se font encore par l'intermédiaire de l'humain.
- Les attaques sont plus sophistiquées, mais **l'orchestration et la répétition de tâches sont toujours limitées par les actions humaines**.
- L'IA générative simplifie les tentatives d'hameçonnage et la création d'hypertrucages et d'identités synthétiques, mais l'observation et les modifications nécessaires pour que les attaques s'adaptent en fonction des défenses nécessitent l'intervention d'un humain.

Fraudes à l'ère de l'IA agentique

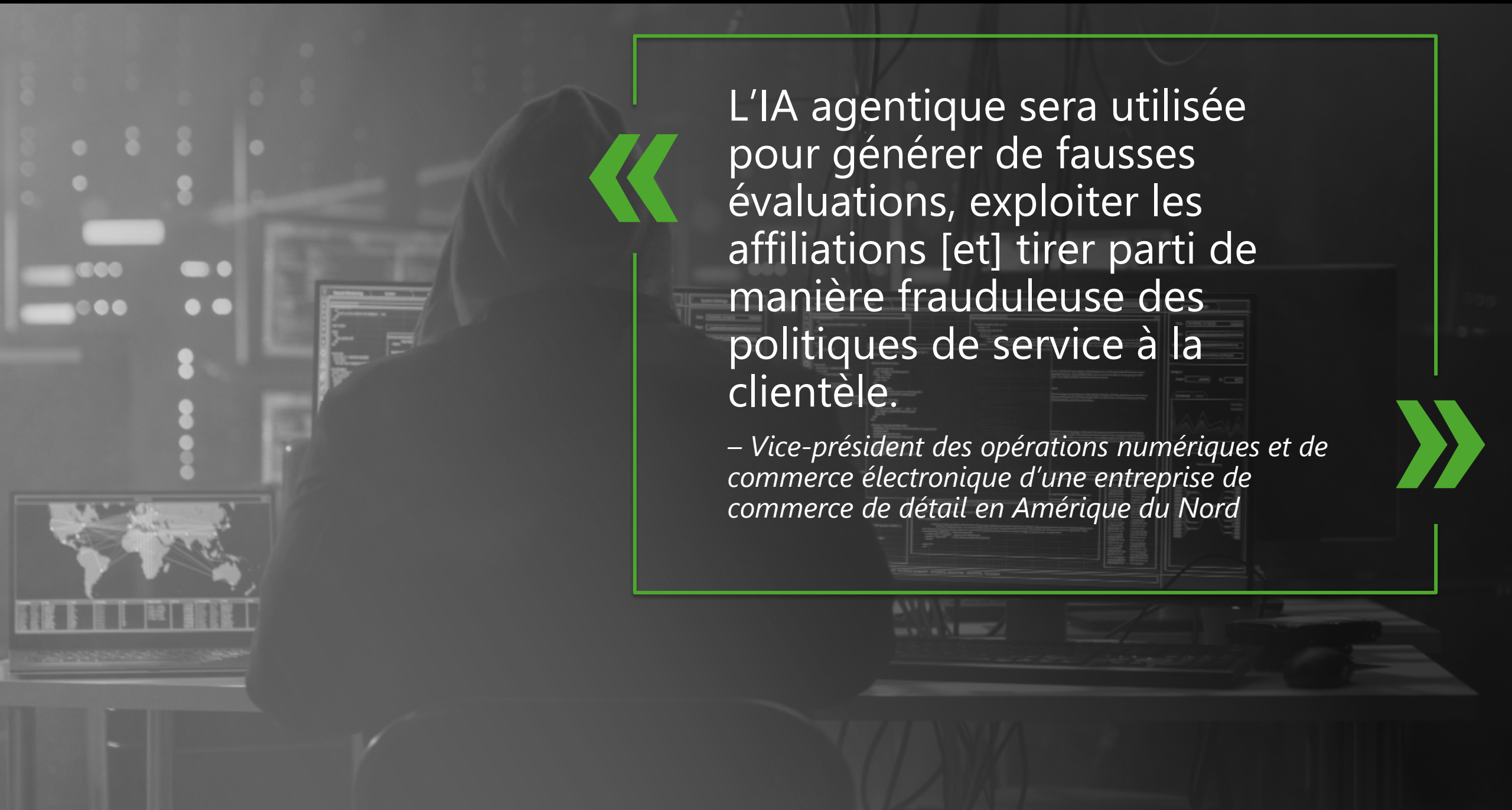
1. **Autonomie**
   Des fraudes à plusieurs étapes **peuvent être planifiées et exécutées de façon autonome** avec un minimum d'interventions.
2. **Adaptabilité**
   Les tâches automatisées peuvent être reproduites facilement.
3. **Capacité d'adaptation**
   Les tactiques peuvent évoluer ou être adaptées afin de repérer et d'exploiter **les vulnérabilités dans les nouvelles méthodes de détection**

37 %

Augmentation, du T2 de 2025 au T3 de 2025, de la fréquentation frauduleuse auprès de commerçants dont une part importante des commandes sont faites à l'aide de GML[2]

De 110 % à 170 %

plus risquée que la fréquentation humaine au T3 2025[2]



« L'IA agentique sera utilisée pour générer de fausses évaluations, exploiter les affiliations [et] tirer parti de manière frauduleuse des politiques de service à la clientèle. »

– Vice-président des opérations numériques et de commerce électronique d'une entreprise de commerce de détail en Amérique du Nord

Au cours de la dernière année, les commerçants ont été la cible de diverses tentatives de fraude reposant sur l'IA, ce qui démontre que les menaces changent en raison de la montée de l'IA agentique. La majorité des commerçants s'attendent à ce que **les risques de fraude continuent de s'accroître** et à ce que les fraudeurs utilisent davantage des outils d'IA agentique.

69 %

des commerçants ont signalé avoir été la cible de fraudes reposant sur l'IA au cours de la dernière année.

Au cours de la dernière année, les répondants à l'enquête ont subi ces attaques rendues possibles par l'IA:

- Hameçonnage vocal par hypertrucage ciblant des hauts dirigeants
- Agents conversationnels habilités par l'IA qui volent l'identité d'agents de service à la clientèle et clonent leurs voix pour tromper des employés
- Campagnes de harponnage tirant parti de GML
- Tentatives automatisées d'achats à l'aide de cartes de crédit frauduleuses et d'identités synthétiques
- Abus liés à l'utilisation de coupons/promotions à l'aide d'identités fabriquées

Hausse des attaques des agents d'IA

La « fraude en tant que service » commise avec l'IA agentique sera plus courante, et les attaques de ce genre seront plus étendues, automatisées, personnalisées et dommageables; pour limiter les dégâts, il est donc plus urgent que jamais d'adopter des stratégies de prévention de la fraude rigoureuses et adaptées.

87 %

des commerçants s'attendent à une augmentation marquée des fraudes reposant sur l'IA d'ici 12 mois.

Principaux risques de fraude reposant sur l'IA que l'IA agentique viendra aggraver, selon les répondants au sondage :

- Création d'identités synthétiques
- Ingénierie sociale fondée sur des hypertrucages
- Hameçonnage automatisé
- Fraudes liées aux paiements / aux cartes
- Programmes de récompenses et de fidélisation

La fraude reposant par l'IA présente un vaste éventail de menaces pour les détaillants, et ses conséquences se font sentir partout, du **rendement financier** à **l'efficacité opérationnelle,** en passant par la **confiance des clients** et la **croissance à long terme**.

S'attaquer à ces risques n'est plus facultatif; les commerçants doivent protéger leur marque, leur réputation et leur réussite à long terme.

Fréquentation sans valeur ou frauduleuse

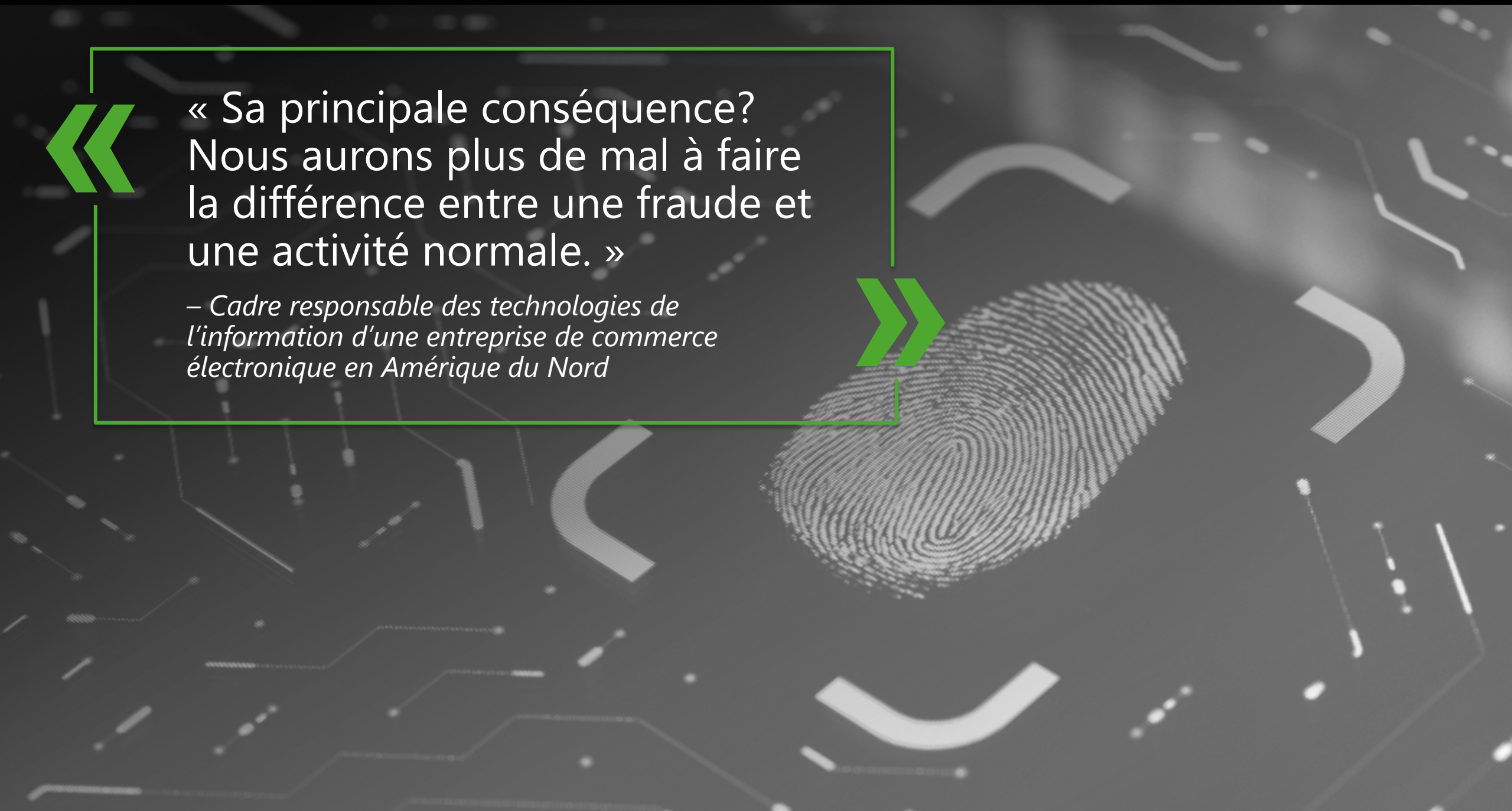
Les fraudes habilitées par l'IA entraînent un gaspillage important en générant un fort volume d'engagement et de fréquentation en apparence humaine, en plus d'accroître inutilement les dépenses de marketing des entreprises, puisque celles-ci paient pour des impressions, des clics ou des pistes qui ne découlent pas de véritables clients ou clients potentiels. En outre, l'augmentation fulgurante de la fréquentation alimentée par des robots peut augmenter l'utilisation de l'infrastructure de sites web et les coûts sans produire de valeur correspondante pour les entreprises.

Perturbations des activités

La complexité croissante et la fréquence accrue des fraudes facilitées par l'IA exigent des investissements plus importants dans la détection et la réponse, ce qui met sous tension les ressources opérationnelles et perturbe les processus métiers. Ces perturbations détournent l'attention des activités principales ciblant les clients et ajoutent des contraintes qui entravent la réalisation des stratégies de croissance (p. ex., restrictions liées aux promotions).

Érosion du lien de confiance et de la fidélité

Les fraudes reposant sur l'IA nuisent à la confiance des clients et à la réputation de la marque en mettant en péril la sécurité. En se contentant d'ajouter des contrôles supplémentaires pour contrer la fraude, des étapes de vérification par exemple, on nuit à la fluidité de l'expérience des clients et cela peut diminuer sa loyauté et la valeur à long terme.



« Sa principale conséquence? Nous aurons plus de mal à faire la différence entre une fraude et une activité normale. »

– Cadre responsable des technologies de l'information d'une entreprise de commerce électronique en Amérique du Nord

Selon les résultats de l'étude de Deloitte, même si près de **67 %** des répondants ont mis à jour leur stratégie de gestion des fraudes ou mis en œuvre de nouveaux contrôles, seulement **3 % d'entre eux se sentent « très préparés »** à lutter contre les fraudes reposant sur l'IA.

Les environnements de contrôle actuels des commerçants n'ont pas ce qu'il faut pour composer avec l'évolution des risques de fraude. Les méthodes traditionnelles de prévention de la fraude, qui dépendent de modèles prévisibles et de la surveillance humaine, sont de moins en moins efficaces contre les menaces de l'IA générative et agentique. Ces technologies avancées permettent d'imiter plus facilement des comportements d'utilisateurs humains et de s'adapter rapidement pour exploiter les contrôles statiques de prévention et de détection de la fraude à grande échelle.

Contrôles traditionnels	Méthodes employées dans les fraudes reposant sur l'IA
Authentification statique	Automatise la saisie des identifiants, exploite les données personnelles et peut intercepter ou manipuler les méthodes d'authentification multifacteur de base afin de contourner rapidement les mécanismes d'authentification statiques et fondées sur des connaissances.
Surveillance fondée sur des règles	Apprend et adapte de façon dynamique un modèle de comportement pour éviter de déclencher les règles statiques.
Suivi et analyse de l'information liée aux séances	Termine les séances beaucoup plus rapidement qu'un humain; en outre, l'IA avancée peut imiter les comportements humains en lien avec la navigation, les boutons à l'écran, le clavier et la souris, ce qui complique de plus en plus la détection.
Blocage d'appareil ou d'adresse IP	Automatise des mystifications/changements d'appareils et modifie fréquemment l'adresse IP pour contourner le blocage d'appareils et d'adresses IP.
Revue manuelle	Submerge les équipes des opérations de fraude par la vitesse et le volume, et profite des retards dans la détection et la réponse à la fraude causés par des opérations cloisonnées.

Selon l’information que nous avons recueillie, **82 % des commerçants s’attendent à ce que des outils sophistiqués de détection de la fraude soient le type de mesure d’atténuation le plus efficace contre les fraudes reposant sur l’IA**. De plus, pour être efficaces dans leur combat contre la fraude reposant sur l’IA, les commerçants doivent étendre leur rayon d’action à l’ensemble des piliers de la gestion de la fraude, et tenir compte de la rapidité, de l’étendue et de l’adaptabilité des fraudes reposant sur l’IA.

Stratégie et gouvernance

Évaluez votre tolérance aux risques et votre prise en charge des risques en mesurant de même qu’en surveillant votre exposition à des risques accrus, et en évaluant votre volonté d’adopter de nouveaux contrôles pour lutter contre la fraude reposant sur l’IA.

Diligence à l’égard des agents

Assurez-vous de détecter, de classer et d’encadrer tous les agents d’IA qui empruntent vos différents canaux afin de pouvoir mieux prévenir les fraudes reposant sur l’IA et préserver tant la fiabilité des interactions que la bonne qualité de l’expérience client.

Authentification adaptative

Évaluez les risques grâce à des signaux en temps réel pour resserrer de façon dynamique les étapes de vérification afin que seuls les utilisateurs ou les agents autonomes légitimes puissent accéder aux canaux ou effectuer des transactions.

Détection dynamique de la fraude

Déployez des outils de détection ou mettez à niveau vos règles et vos modèles d’analytique pour pouvoir analyser l’évolution des comportements des utilisateurs et les tendances liées aux transactions en temps réel, puis identifier et bloquer les fraudes reposant sur l’IA.

Réponses et litiges

Adoptez des pratiques d’enquête efficaces, effectuez des analyses et des interventions en temps opportun, et utilisez efficacement vos ressources pour contrer le comportement adaptatif de l’IA agentique et réduire autant que possible les impacts de ses attaques sur les finances et les activités de l’entreprise.

Infrastructure et sécurité

Utilisez une infrastructure solide et des protocoles de sécurité multiniveaux (par exemple, des contrôles d’accès, des pistes d’audit, des moyens de gestion des données avancés) pour améliorer la détection d’activités frauduleuses menées par des agents.

Pour atteindre leurs buts et déployer les solutions de gestion des fraudes souhaitées, les commerçants doit relever différents défis, notamment sur le plan du budget, des ressources et des technologies. Plus de la moitié des répondants ont affirmé que de tous les défis, ce sont le financement et le budget qui sont les plus importants pour eux. En usant de stratégies dans la définition des priorités et en établissant des partenariats avec des experts, les commerçants peuvent surmonter ces obstacles et optimiser leurs défenses contre les fraudes, tout en gardant leur orientation client et en se donnant les moyens nécessaires permettant de favoriser leur croissance.

Principaux obstacles à la mise en œuvre de mesures efficaces d’atténuation des risques de fraude

52 % **mentionnent l’obtention de financement/le budget**

38 % **mentionnent le manque de ressources ou de compétences**

34 % **mentionnent les limites de la technologie actuelle**

Approches pour éviter les obstacles

Concilier la lutte contre la fraude et l’expérience client en arrimant les initiatives de gestion des fraudes aux objectifs de croissance du commerce électronique

S’associer à des experts et tirer parti de leurs connaissances **grâce à des partenariats externes et à des consortiums**

Accorder la priorité aux cas d’utilisation à forte incidence qui allient les avantages immédiats et la transformation à long terme de l’entreprise

Augmenter les moyens et les connaissances à l’interne grâce à l’analytique et des **initiatives ciblées d’amélioration des compétences à l’échelle de l’entreprise**

Kevin Luh
Leader de la gestion des fraudes, Crimes financiers

416-824-1663
kluh@deloitte.ca

Shaunna Conway
Leader de la gamme de services, Marketing, commerce et produits

416-807-0611
shconway@deloitte.ca

Andrew J. Lee
Associé,
Cybersécurité

416-702-5532
andrlee@deloitte.ca

Diksha Pai
Directrice principale,
Crimes financiers

437-218-6384
dpai@deloitte.ca

David Kao
Directeur,
Crimes financiers

416-202-2891
dakao@deloitte.ca

Eden Sorrell
Conseiller principal,
Crimes financiers

437-331-6159
esorrell@deloitte.ca

L'équipe des Crimes financiers de Deloitte est composée de professionnels chevronnés qui ont une vaste expérience pratique des projets transformateurs de gestion de la fraude réalisés pour des détaillants, des institutions financières et le secteur public.

Deloitte aide ses clients à concevoir, à réaliser et à administrer des programmes dynamiques de gestion de la fraude adaptés aux besoins des entreprises et de leurs secteurs d'activités. Vous avez ainsi l'assurance d'accéder aux connaissances et aux moyens nécessaires pour répondre aux attentes, tout en continuant à vous concentrer sur ce que vous faites le mieux : gérer votre entreprise.

- **Leadership à l'échelle mondiale :** Deloitte est un leader mondial en matière de services-conseils dans le domaine de la stratégie de gestion de la fraude. Nous offrons un leadership distinctif dans le domaine et une solide expérience sectorielle.
- **Écosystèmes et alliances :** nous avons forgé de solides alliances avec des fournisseurs de technologies de pointe, des organisations sectorielles et des entités de recherche afin de fournir des pistes de réflexion, des renseignements de premier plan, de favoriser la diffusion de l'information et la collaboration.
- **Quantification des risques de fraude :** grâce à l'intégration des données et à des modèles statistiques conçus sur mesure pour la quantification des risques, nous aidons les organisations à bonifier leur expérience à l'aide des outils technologiques afin de développer des interventions en matière d'évaluation des risques.
- **Solutions fondées sur des données :** en combinant nos perspectives techniques et sectorielles approfondies à notre analytique de pointe, nous identifions les solutions de lutte contre la fraude en se basant sur des données probantes, ce qui permet de traiter les enjeux les plus complexes de votre entreprise.

En savoir plus sur la série *Commerce de détail réimaginé*

- **L'avenir du magasinage**
  Les magasins connectés transforment le secteur du commerce de détail. Votre organisation est-elle prête pour le magasin du futur?
- **Innovation liée aux programmes de fidélisation des détaillants**
  Les Canadiens ont des attentes élevées envers les programmes de fidélisation des détaillants. Sont-ils satisfaits du vôtre?

Annexe

Sommaire de notre approche et sondage 2025 de Deloitte sur la fraude reposant sur l'IA dans le commerce au détail

Objectifs

Nous avons effectué cette étude pour comprendre et qualifier l'évolution du contexte des risques de fraude en raison de la montée du commerce et des paiements agentiques. Elle vise également à donner aux commerçants une bonne compréhension de l'augmentation des risques de fraude reposant sur l'IA dans le domaine du commerce agentique, ainsi que des éléments à considérer pour mettre en œuvre des stratégies d'atténuation efficaces.

Sources de données

Deloitte a mené une étude quantitative et qualitative englobant un vaste éventail de données ainsi que des points de vue d'experts afin de vérifier une hypothèse clé sur les opportunités et l'impact du commerce agentique dans le secteur du commerce de détail. L'étude inclut également des données provenant de fournisseurs de solutions partenaires spécialisés dans la fraude reposant sur l'IA au sein de l'écosystème du commerce de détail. Nous avons réalisé cette étude en septembre et en octobre 2025 en utilisant diverses sources de données, notamment les suivantes :

- ***Sondage 2025 de Deloitte sur la fraude reposant sur l'IA dans le commerce de détail :*** Nous avons recueilli 39 réponses admissibles sur un total de 62 en tenant compte du profil des répondants, y compris la taille de l'organisation et la position du répondant.
- ***Riskified :*** Données exclusives de transactions de commerce électronique et de tentatives de fraudes dans un réseau mondial de commerçants, ainsi que d'un sondage, réalisé en 2025 auprès de plus de 5 000 clients, sur l'utilisation de l'IA à des fins de magasinage et des risques liés au commerce agentique.
- ***HUMAN Security :*** Rapports exclusifs sur les interactions numériques liées à la fréquentation et études liées au parcours numérique des clients, y compris l'affichage des publicités, la consommation, les interactions sur le site avant, pendant et après la connexion, y compris les évaluations des changements de tendances liées à la fréquentation et des attaques numériques à ce jour.

PROFIL DES RÉPONDANTS : SONDAGE 2025 DE DELOITTE SUR LA FRAUDE REPOSANT SUR L'IA DANS LE COMMERCE DE DÉTAIL

Afin de mieux comprendre les points de vue et les défis liés à l'IA agentique et à la fraude reposant sur l'IA dans le secteur du commerce de détail, Deloitte a transmis un sondage à 39 commerçants nord-américains issus de divers secteurs d'activité. Tous les participants avaient une compréhension et des expériences pertinentes en lien avec l'IA agentique et travaillaient pour des entreprises dont le chiffre d'affaires annuel se situait entre 1 M$ et plus de 100 M$.

Lieu du répondant

92 % États-Unis

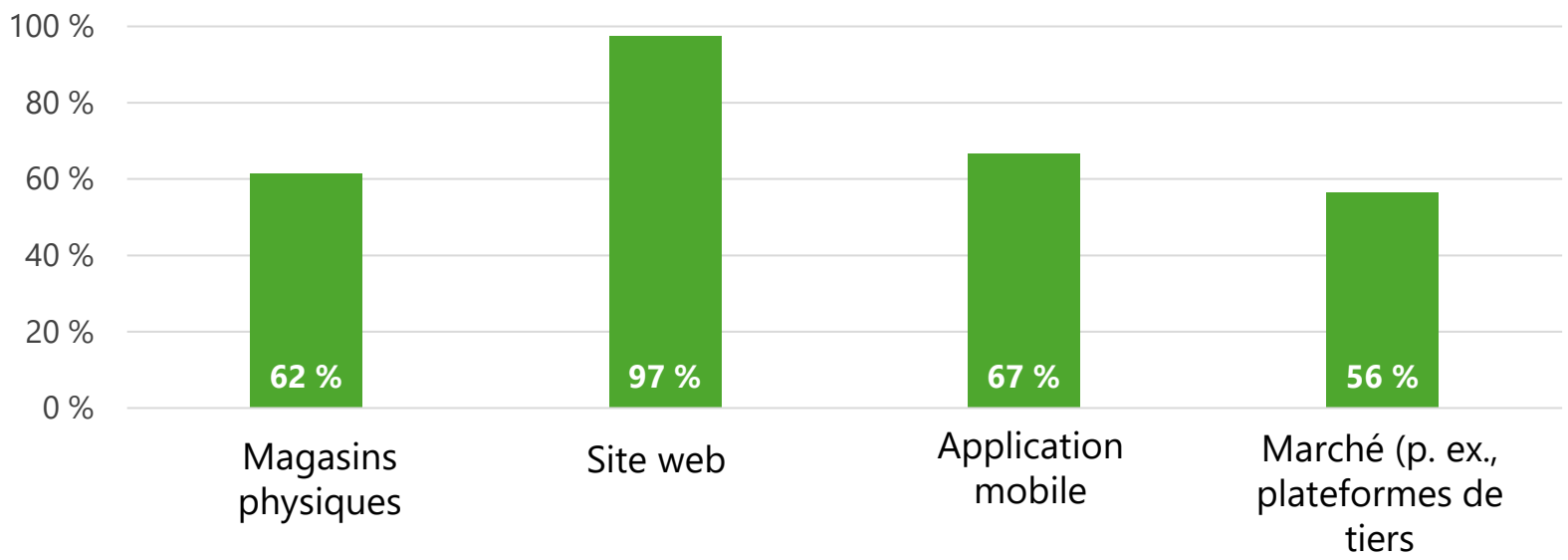
8 % Canada

Chiffre d'affaires annuel du commerçant	Nbre	%
Moins de 1 M$	0	0 %
De 1 M$ à 49,9 M$	2	5 %
De 50 M$ à 99,9 M$	5	13 %
100 M$ ou plus	32	82 %

Marché vertical du commerçant	Nbre	%
Commerce électronique	15	38 %
Accueil	4	10 %
Commerce de détail	16	41 %
Transport aérien	1	3 %
Services aux consommateurs	3	8 %

Niveau du répondant dans l'organisation	Nbre	%
Haute direction ou équivalent	20	51 %
Premier vice-président ou équivalent	3	8 %
Vice-président ou équivalent	7	18 %
Directeur de service ou équivalent	7	18 %
Directeur principal ou équivalent	2	5 %

Canaux utilisés par les commerçants



69 %

des commerçants ont été la cible de fraudes reposant sur l'IA au cours de la dernière année

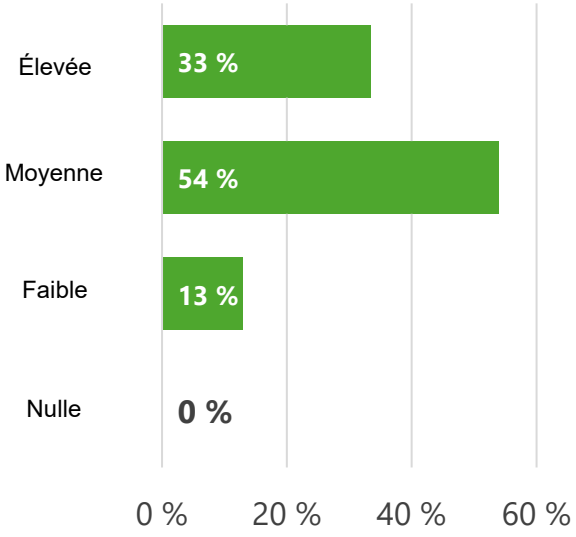
Types de fraudes reposant sur l'IA au cours de la dernière année

- Identités fausses ou synthétiques
- Fabrication de faux documents
- Usurpation d'identité par hypertrucage
- Hameçonnage/harponnage
- Piratage psychologique
- Vol de mots de passe par l'intermédiaire d'une attaque par force brute
- Saisie de comptes
- Attaque par interception
- Faux sites web ou vitrines
- Transactions/cartes de crédit frauduleuses
- Abus liés aux coupons/promotions
- Fraude liée aux retours/dommages

Domaines particulièrement vulnérables à la fraude habilitée par l'IA

Hameçonnage automatisé	82 %
Création d'identités synthétiques	69 %
Piratage psychologique fondé sur des hypertrucages	69 %
Fraudes liées aux paiements/cartes	62 %
Abus liés aux remboursements et à la rétrofacturation	41 %
Programmes/récompenses de fidélisation	36 %
Manipulation de commandes	23 %
Manipulation de prix	15 %
Fraude interne	15 %
Autre	5 %

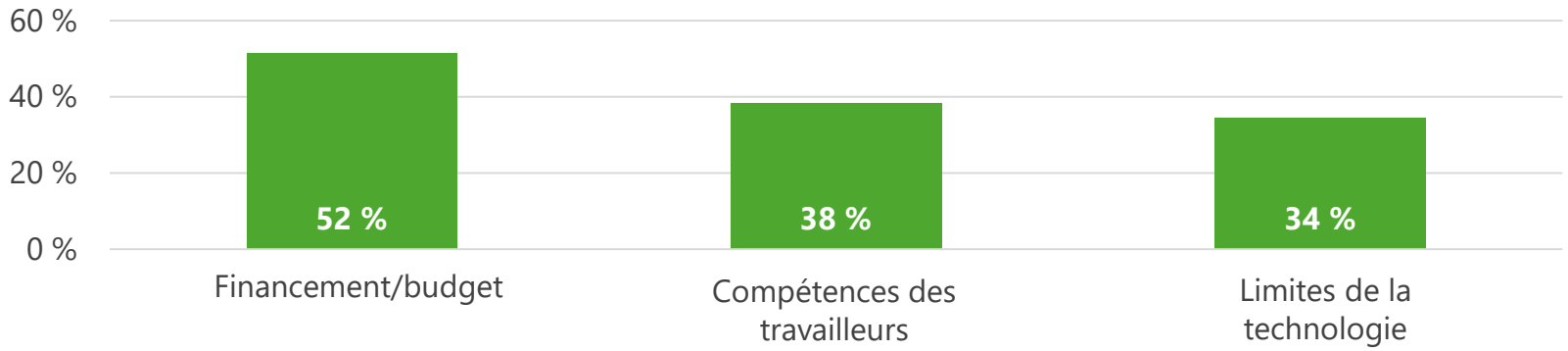
Augmentation prévue du volume d'attaques reposant sur l'IA agentique au cours des 12 prochains mois



95 %

des commerçants prévoient adapter leur stratégie de lutte contre la fraude en fonction de l'IA agentique

Principaux obstacles à la mise en œuvre de stratégies d'atténuation efficaces de la fraude reposant sur l'IA



Les répondants ont été très nombreux à mentionner les termes « IA », « fraude », « automatisation » et « capacités agentiques », ce qui permet de croire que ces sujets définiront le paysage du commerce de détail et de la fraude au cours des deux ou trois prochaines années.

Voici les principaux thèmes émergents :

« Difficulté accrue à faire la différence entre une fraude et une transaction légitime. »

« Les fraudes sont de plus en plus nombreuses et sophistiquées. »

« Augmentation du nombre de stratagèmes de fraude reposant sur l'IA adaptables et à faible coût. »

« Évolution rapide des tactiques de fraude en raison de l'IA agentique et de l'automatisation. »

Pourcentage d'organisations qui ont ou n'ont pas mis à jour leur stratégie ou qui ont ou n'ont pas mis en œuvre de nouveaux contrôles pour lutter contre la fraude reposant sur l'IA

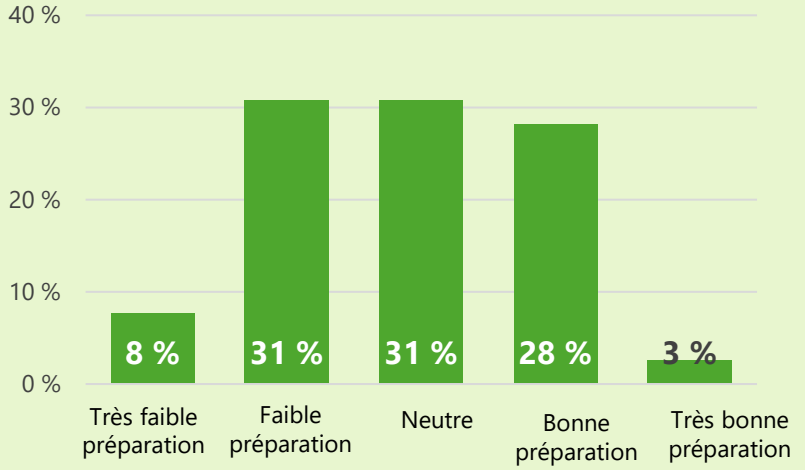
67 % Oui

33 % Non

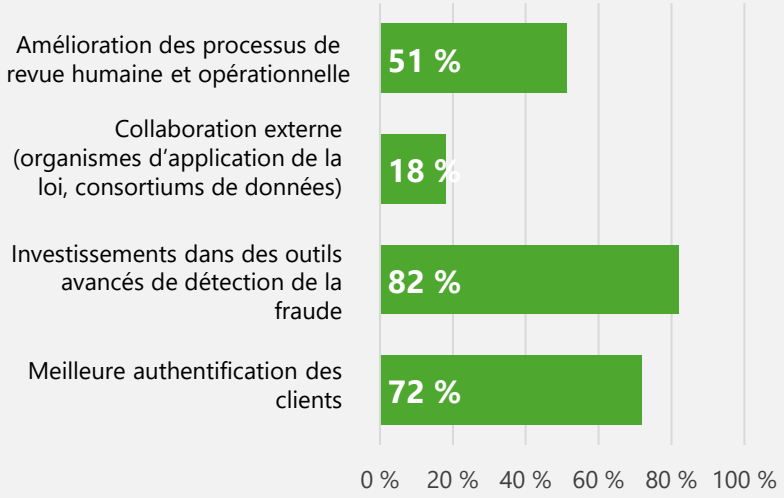
Voici ce sur quoi les organisations qui ont mis à jour leur stratégie et mis en œuvre de nouveaux contrôles pour lutter contre la fraude ont travaillé :

- Connaissance des agents et modèles de gestion des risques
- Tests de pénétration
- Authentification multifactorielle
- Adoption des pratiques exemplaires du secteur
- Création d'outils et de procédures internes
- Contrôles axés sur l'IA pour les programmes d'audit interne
- Outils de détection de l'IA (p. ex., IA adaptative, analytique comportementale, orchestration des menaces en temps réel)
- Inclusion, dans les contrats, d'énoncés sur l'utilisation des données aux fins de l'IA
- Réduction des interventions humaines dans les décisions liées aux fraudes
- Amélioration de la sécurité des courriels et des appareils mobiles

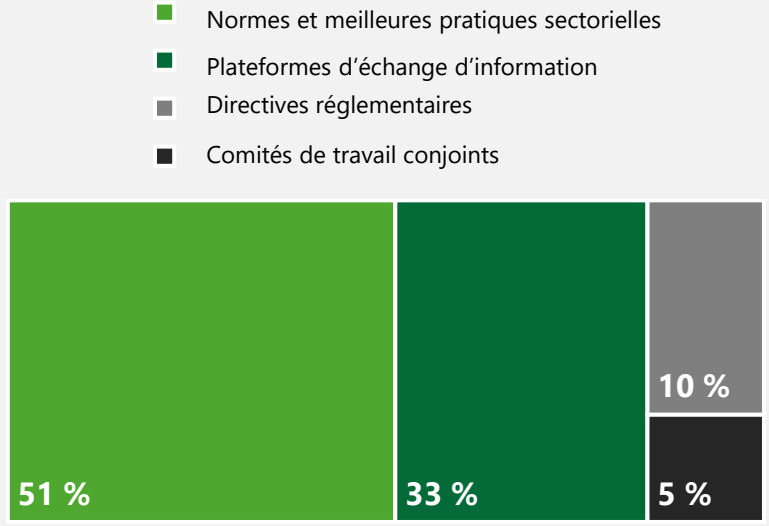
État de préparation des commerçants à faire face aux fraudes reposant sur l'IA



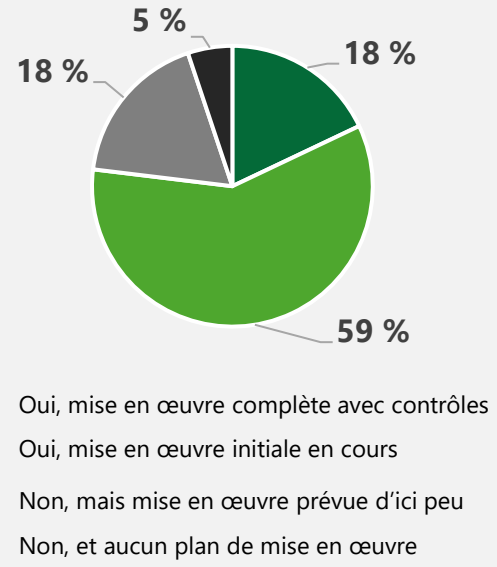
Stratégies d'atténuation qui devraient être les plus efficaces contre les fraudes reposant sur l'IA



Mesures sectorielles considérées comme étant les plus importantes pour faire face aux fraudes reposant sur l'IA



Commerçants qui utilisent ou qui envisagent d'utiliser l'IA agentique dans leurs canaux de service à la clientèle



1. Estimation de Deloitte dans *The future of commerce in an agentic world: How agentic AI will reshape commerce and what payment networks must do next*, 2025.
2. Observation fondée sur des données exclusives de Riskified sur la fréquentation alimentée par les GML, les transactions et les fraudes connexes, 2025.
3. Observation fondée sur des données exclusives de Riskified présentée dans *Global Study : 73% of Shoppers Using AI in Shopping Journey - But Merchants Face New Agentic Commerce Risks*, 2025.
4. Observation fondée sur des données exclusives de Riskified présentée dans *Riskified Champions Fraud Prevention as a Leading Partner of International Fraud Awareness Week 2025*, 2025.
5. Observation fondée sur des données exclusives de HUMAN Security présentée dans *Examining AI Agent Traffic : Powering the Shift to Agentic Commerce*, 2025.

Deloitte.

www.deloitte.ca

À propos de Deloitte

Deloitte offre des services dans les domaines de l'audit et des services-conseils en audit, de l'audit, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.