DIACC CCIAN

BREFFAGE SUR LES MENACES • AVRIL 2026

# Le nouveau paysage de la fraude.

Identités synthétiques, hypertrucages et

l'évolution nécessaire des défenses canadiennes

**RÉSILIENCE À LA FRAUDE ET PRÉPARATION À L'IA** **PILIER STRATÉGIQUE 04**

*Un breffage sur les menaces du CCIAN préparé à l'intention des membres, des décideurs publics et de l'écosystème canadien de la confiance numérique.*

diacc.ca | contact@diacc.ca

# Table des matières

BREFFAGE SUR LES MENACES DU CCIAN

# 01

# Objet, portée et méthodologie

SECTION 09 SUR 10

# 1. Objet, portée et méthodologie

Le présent breffage sur les menaces offre aux organisations canadiennes un portrait clair, fondé sur des données probantes, de la façon dont l'intelligence artificielle transforme la fraude identitaire. Il porte précisément sur deux catégories de menaces qui ont connu une escalade marquée depuis 2023 : la fraude à l'identité synthétique et les attaques utilisant des hypertrucages visant les systèmes de vérification de l'identité, d'authentification et de transaction. Le breffage ne présuppose aucune expertise préalable en techniques de fraude alimentées par l'IA et progresse des concepts fondamentaux aux implications stratégiques.

Les sections 2 à 6 présentent le paysage des menaces : les virages structurels qui propulsent la fraude alimentée par l'IA, les acteurs derrière les attaques et les méthodes qu'ils emploient. La section 7 passe de la description de la menace à l'analyse stratégique, examinant pourquoi les défenses actuelles sont insuffisantes à l'échelle de l'écosystème. La section 8 cartographie l'exposition qui en résulte par secteur, tandis que les sections 9 et 10 portent sur les menaces émergentes et sur la réponse prévue par le CCIAN.

Un document complémentaire, Guide de démarrage rapide : défenses immédiates contre la fraude identitaire par IA, présente des mesures précises et peu coûteuses à l'intention des petites et moyennes entreprises, des cabinets de services professionnels et des autres organisations aux ressources limitées.

Il s'adresse aux responsables du risque, aux dirigeants de la sécurité, aux professionnels des politiques publiques et aux décideurs de haut niveau dans tous les secteurs de l'économie canadienne — particulièrement à ceux qui sont responsables de la posture de risque d'entreprise, de l'évaluation des fournisseurs, de la stratégie de vérification de l'identité et de la mobilisation avec l'écosystème canadien de la confiance numérique.

## Méthodologie et sources

Le présent breffage fait la synthèse du renseignement sur les menaces publié, de données empiriques et d'analyses de normes issues des catégories de sources suivantes :

### Sources gouvernementales canadiennes.

L'Évaluation des cybermenaces nationales 2025-2026 du Centre canadien pour la cybersécurité (CCCS) [8] et Cybermenaces contre le processus démocratique du Canada : mise à jour 2025 [15] fournissent l'évaluation faisant autorité du gouvernement du Canada sur les menaces alimentées par l'IA. Le Rapport statistique annuel 2024 du Centre antifraude du Canada (CAFC) [1] présente les données

principales sur les pertes canadiennes liées à la fraude. Ces sources sont accessibles au public et reflètent les positions officielles du gouvernement du Canada.

### Sources gouvernementales internationales.

L'alerte FIN-2024-Alert004 du Financial Crimes Enforcement Network (FinCEN) des États-Unis [16] propose des typologies réglementaires et des indicateurs de signaux d'alarme pour la fraude identitaire alimentée par l'IA. La publication NIST Special Publication 800-63-4 [18] et la publication NIST AI 100-4 [19] constituent les principales références en matière de normes techniques et de détection de contenus synthétiques. La norme ETSI TS 119 461 v2 [20] de l'European Telecommunications Standards Institute (ETSI) définit la norme de vérification de l'identité pour l'Union européenne. Il s'agit de publications officielles de leurs gouvernements ou organismes normalisateurs respectifs.

### Recherche des membres du CCIAN.

Les données primaires sur les tendances canadiennes de la fraude, l'évolution des vecteurs d'attaque et les profils de fraude biométrique proviennent de rapports publiés par Equifax Canada [2], iProov [5] [6] et Entrust [4] [13]. L'analyse des projections de fraude alimentée par l'IA, de la préparation organisationnelle en cybersécurité et de l'incidence sur le marché est tirée des publications de Deloitte 2024 [3], Ernst & Young 2025 [22] et Accenture 2025 [23]. Ces organisations sont membres du CCIAN. Leurs recherches publiées sont citées parce qu'elles représentent les meilleures données disponibles sur les vecteurs de menace, les lacunes de préparation organisationnelle et les conséquences financières que traite ce breffage; leur adhésion au CCIAN ne constitue pas une approbation de leurs produits ou services. Lorsque les données d'un membre sont la seule source d'une affirmation, cela est indiqué.

### Sources internationales non gouvernementales.

Le Forum économique mondial [7] [10] [12] fournit des analyses transfrontalières des menaces et de la documentation de cas.

### Approche analytique.

Le présent breffage distingue trois catégories d'énoncés :

- Données rapportées : statistiques et constats publiés par les sources ci-dessus, cités directement. Ces éléments sont présentés tels que rapportés, avec attribution de source.
- Constats évalués : jugements analytiques formulés par le CCIAN à partir de la synthèse de plusieurs sources. Ils sont identifiés par des formulations telles que « le CCIAN estime » ou « les données disponibles appuient ». Les constats évalués représentent le jugement professionnel du CCIAN et sont ouverts à la discussion.
- Projections émergentes : énoncés prospectifs tirés de projections publiées par des sources crédibles (p. ex., Deloitte, FEM). Ils sont attribués à leur source et ne devraient pas être considérés comme des prévisions assorties d'intervalles de confiance connus.

Le présent breffage ne s'appuie pas sur du renseignement classifié et ne formule pas d'attributions allant au-delà de celles publiées par les gouvernements canadien et alliés. Les organisations devraient vérifier

les constats sensibles au facteur temps par rapport aux avis courants du CCCS et aux flux de renseignement propres à leur secteur.

# 02

# Évaluation sommaire

SECTION 02 SUR 10

# 2. Évaluation sommaire

**En résumé :** la fraude identitaire alimentée par l'IA est passée du statut de risque émergent à celui de menace active et substantielle pour les organisations canadiennes de tous les secteurs. Les outils sont peu coûteux, les attaques évoluent à l'échelle, et la posture défensive du Canada comporte des lacunes structurelles que les investissements institutionnels individuels ne peuvent combler.

## CINQ CONSTATS ÉVALUÉS QUI DÉFINISSENT LE PAYSAGE ACTUEL

### 1. L'ampleur est saisissante et en croissance.

Le Centre antifraude du Canada (CAFC) a recensé 638 M$ en pertes déclarées liées à la fraude en 2024, en hausse par rapport à 577 M$ en 2023 et à 531 M$ en 2022 [1]. Or, seuls 5 à 10 % des cas de fraude sont déclarés. Le CCIAN estime, en s'appuyant sur les indications du CAFC concernant les taux de déclaration, que les pertes canadiennes réelles liées à la fraude pourraient se situer entre 6,4 G$ et 12,8 G$ par année — un chiffre qui devrait éclairer les évaluations des comités du risque d'entreprise. Les pertes déclarées cumulatives depuis 2021 dépassent désormais 2 G$ [1]. Les données d'Equifax Canada montrent que la fraude à l'identité synthétique dans les demandes de crédit a presque triplé en une seule année, passant de 2,8 % à 8 % entre le T2 2023 et le T2 2024 [2]. Le Center for Financial Services de Deloitte prévoit que l'IA générative pourrait à elle seule faire grimper les pertes américaines liées à la fraude à 40 G$ d'ici 2027 [3]. Les conséquences financières dépassent les pertes directes : l'analyse par EY des entreprises du Russell 3000 a révélé que les sociétés victimes d'un incident cyber voient généralement leur cours boursier reculer de 1,5 % au cours des 90 jours suivants, ce qui témoigne d'une incidence soutenue sur le marché au-delà des coûts immédiats de rétablissement [22].

### 2. Les hypertrucages sont devenus une capacité industrielle.

Le Cybersecurity Institute d'Entrust a documenté une tentative d'hypertrucage toutes les cinq minutes en 2024, les contrefaçons numériques de documents ayant augmenté de 244 % d'une année à l'autre [4]. iProov a recensé une hausse de 2 665 % des attaques par injection par caméra virtuelle et une flambée de 300 % des attaques par substitution de visage, propulsées par un écosystème de crime comme service comptant près de 24 000 utilisateurs qui vendent des technologies d'attaque [5].

### 3. Les données disponibles appuient fortement la conclusion selon laquelle les humains ne peuvent plus servir de couche principale de détection.

Une étude d'iProov a révélé que seulement 0,1 % des participants parvenaient à repérer correctement tous les hypertrucages lorsqu'on leur présentait un mélange de contenu réel et de contenu synthétique [6]. Le Forum économique mondial a noté que la capacité humaine à détecter les hypertrucages oscille entre 55 et 60 % seulement, à peine mieux que le hasard [7]. Cela a des implications directes pour tout processus de vérification de l'identité ou d'autorisation de transaction qui repose sur un contrôle visuel ou auditif humain.

**4. Le Canada fait face à des dynamiques de menace précises et documentées.**

L'Évaluation des cybermenaces nationales 2025-2026 du CCCS désigne l'IA générative et les hypertrucages comme des menaces en accélération visant les infrastructures essentielles, les systèmes financiers et les processus démocratiques du Canada [8]. En juin 2025, les autorités canadiennes ont publié un avis conjoint documentant une campagne d'usurpation d'identité par hypertrucage qui utilisait des messages vocaux générés par IA et des comptes de messagerie imitant des hauts responsables gouvernementaux et des personnalités publiques de premier plan pour escroquer des Canadiens [9].

**5. Le CCIAN estime que la posture défensive actuelle du Canada comporte des lacunes structurelles que les investissements institutionnels individuels ne peuvent combler.**

Les évaluations publiées des menaces, les cadres normatifs et les capacités de détection propres aux fournisseurs ont progressé de façon notable. Toutefois, l'analyse du CCIAN cerne trois faiblesses systémiques — un renseignement sur les menaces fragmenté, des normes sans orientations canadiennes de mise en œuvre, et l'absence d'interopérabilité intersectorielle de l'assurance de l'identité — dont la résolution exige une coordination à l'échelle de l'écosystème. Ces lacunes sont examinées à la section 7.

# 03

# Le virage structurel : l'IA comme accélérateur de fraude

SECTION 03 SUR 10

# 3. Le virage structurel : l'IA comme accélérateur de fraude

La menace de fraude identitaire a subi une transformation structurelle. Trois évolutions convergentes ont fondamentalement modifié l'économie et les capacités dont disposent les acteurs de menace.

## 3.1 L'effondrement du coût de la fraude

L'IA générative a réduit de plusieurs ordres de grandeur le temps, le coût et les compétences requises pour produire du contenu synthétique convaincant. Des documents d'identité qui exigeaient autrefois des compétences spécialisées pour être falsifiés peuvent désormais être générés en quelques secondes. Les données d'Entrust pour 2026 montrent que les méthodes numériques représentent maintenant une part substantielle de la fraude aux documents d'identité : les contrefaçons numériques comptent pour 35 % et les faux numériques pour 9 % supplémentaires de toutes les tentatives de fraude documentaire, tandis que les faux physiques demeurent la plus grande catégorie individuelle à 47 % et que les contrefaçons physiques représentent les 10 % restants [13]. La prévalence soutenue des méthodes numériques reflète l'accessibilité de l'IA générative et des outils d'édition à code source ouvert, qui ont fait s'effondrer le coût et les compétences requis pour produire à grande échelle des faux convaincants. Rob Greig, dirigeant principal de l'information d'Arup, a déclaré au Forum économique mondial qu'il avait créé un hypertrucage en temps réel de lui-même à l'aide de logiciels à code source ouvert en environ 45 minutes [10].

## 3.2 Le passage aux attaques en temps réel

Le virage le plus dangereux est celui de la tromperie statique vers la manipulation en temps réel. Les acteurs de menace peuvent désormais générer des vidéos d'hypertrucage convaincantes pendant des séances de vérification en direct, cloner des voix à partir de quelques secondes d'audio de référence, injecter des contenus synthétiques directement dans les flux de données d'appareils à l'aide de caméras virtuelles, et exploiter simultanément plusieurs identités synthétiques à travers différentes institutions.

La gravité de ce virage a été démontrée au début de 2024 lorsqu'une employée des finances de la multinationale d'ingénierie Arup a été manipulée pour virer 25,6 M$ à des fraudeurs après s'être jointe à un appel vidéo où tous les autres participants, y compris de prétendus cadres supérieurs, étaient des hypertrucages générés par IA. La police de Hong Kong a confirmé que les attaquants avaient utilisé des vidéos et des enregistrements audio accessibles au public pour générer les usurpations synthétiques [10] [11].

## 3.3 L'industrialisation du crime

Le rapport Threat Intelligence Report 2025 d'iProov documente un écosystème de crime comme service en ligne comptant près de 24 000 utilisateurs qui vendent des technologies d'attaque contre l'identité [5]. Ces places de marché offrent des outils de génération d'identités synthétiques, des logiciels d'attaque par substitution de visage et par injection, des tutoriels et du soutien technique sur le Web clandestin, ainsi que des réseaux de passeurs d'argent (mules) pour blanchir les produits du crime. Entrust rapporte avoir identifié 53 réseaux de fraude uniques depuis 2023, dont quatre ont ciblé plusieurs clients dans différents secteurs, avec des rôles définis couvrant recruteurs, organisateurs, exécutants et spécialistes techniques [13].

Le Forum économique mondial rapporte que les agents d'IA frauduleuse, qui combinent IA générative, cadres d'automatisation et apprentissage par renforcement, peuvent maintenant créer des identités synthétiques, interagir avec les systèmes de vérification en temps réel et ajuster leur comportement en fonction des résultats. Selon les projections, ces agents deviendront courants d'ici 18 mois, particulièrement au sein des réseaux de fraude organisés [12].

# 04

# Le Canada sous pression : le portrait des menaces intérieures

SECTION 04 SUR 10

# 4. Le Canada sous pression : le portrait des menaces intérieures

## 4.1 Les chiffres

| INDICATEUR | DONNÉES | SOURCE |
|---|---|---|
| Pertes déclarées liées à la fraude (Canada, 2024) | 638 M$ (taux de déclaration de 5 à 10 %) | CAFC [1] |
| Pertes réelles estimées liées à la fraude (Canada, 2024) | 6,4 à 12,8 G$ (estimation du CCIAN) | Analyse du CCIAN des données du CAFC [1] |
| Pertes déclarées cumulatives depuis 2021 | Plus de 2 G$ | CAFC [1] |
| Rapports de fraude reçus (2024) | 108 878 rapports; au moins 34 621 victimes | CAFC [1] |
| Fraude identitaire en % des demandes de crédit signalées | 48,4 %, en hausse par rapport à 43,2 % d'une année à l'autre | Equifax Canada [2] |
| Fraude à l'identité synthétique dans les demandes de crédit | 2,8 % → 8 % en un an (presque triplé) | Equifax Canada [2] |
| Fréquence des tentatives d'hypertrucage (mondial) | Une fois toutes les cinq minutes | Entrust [4] |
| Croissance des contrefaçons numériques de documents (2024) | 244 % d'une année à l'autre | Entrust [4] |
| Répartition des types de fraude documentaire (sept. 2024 – sept. 2025) | Faux physique 47 %; contrefaçon numérique 35 %; contrefaçon physique 10 %; faux numérique 9 % | Entrust [13] |
| Hypertrucages en % des tentatives de fraude biométrique | 1 sur 5 (2025) | Entrust [13] |
| Croissance des attaques par injection | Hausse de 2 665 % des attaques par caméra virtuelle | iProov [5] |
| Croissance des attaques par injection (corroboration) | ~40 % d'augmentation d'une année à l'autre du taux présumé | Entrust [13] |
| Croissance des attaques par substitution de visage | Hausse de 300 % par rapport à 2023 | iProov [5] |

| INDICATEUR | DONNÉES | SOURCE |
|---|---|---|
| Croissance des attaques par injection sur iOS (2e semestre 2025) | Flambée de 1 151 % | iProov [24] |
| Croissance des attaques par injection sur iOS (annuelle) | Hausse de 741 % | iProov [24] |
| Concentration régionale des attaques (T3 2025) | Asie du Sud-Est : flambée de 720 % | iProov [24] |
| Exactitude de la détection humaine des hypertrucages | 0,1 % repèrent correctement tous les hypertrucages | iProov [6] |
| Pertes projetées dues à la fraude par IA générative (É.-U.) | 40 G$ d'ici 2027 (projection Deloitte) | Deloitte [3] |

## 4.2 Le paysage réglementaire canadien

Les organisations canadiennes évoluent au sein d'un cadre réglementaire en évolution, mais incomplet :

- La LPRPDE / la LPVPC proposée exigent des mesures de sécurité proportionnelles à la sensibilité des renseignements, mais n'offrent aucune orientation précise sur les menaces identitaires générées par l'IA.
- La LIAD proposée imposerait des amendes pouvant atteindre 25 M$ CA ou 5 % des revenus mondiaux pour non-conformité en matière de sécurité de l'IA, mais les modalités de mise en œuvre demeurent en cours d'élaboration.
- La Loi sur la protection des cybersystèmes essentiels traite des obligations de sécurité des infrastructures essentielles, mais ne comporte pas d'orientations propres aux menaces identitaires par IA.
- Les obligations du BSIF et du CANAFE imposent des exigences de conformité au secteur financier que la fraude à l'identité synthétique met directement en péril; or, les orientations de mise en œuvre propres au secteur pour la fraude alimentée par l'IA font défaut.
- Les programmes provinciaux d'identité numérique (BC Services Card avec 4,6 M d'utilisateurs, Ontario, Québec, Alberta) font évoluer à plus grande échelle des écosystèmes de justificatifs numériques qui doivent résister à l'exploitation par identités synthétiques.

Les Objectifs de préparation à la cybersécurité intersectoriels du CCCS énoncent 36 objectifs fondamentaux pour les organisations canadiennes, mais ne traitent pas des vecteurs de menace propres à l'identité synthétique et aux hypertrucages avec la spécificité opérationnelle dont les organisations ont besoin [8].

Le Cadre de confiance pancanadien (CCP) du CCIAN offre un cadre de conformité pour la vérification de l'identité numérique au Canada, dont l'adoption à l'échelle de la production a été démontrée dans le secteur juridique, où les membres ont rapporté plus de 700 000 transactions de vérification de l'identité de clients entre octobre 2023 et octobre 2024 [14] [17].

# 05

# Le paysage des acteurs de menace

SECTION 05 SUR 10

# 5. Qui est derrière les attaques : le paysage des acteurs de menace

## 5.1 Réseaux criminels organisés

***Trajectoire évaluée de la menace : en augmentation.***

Le principal moteur de la fraude à l'identité synthétique au Canada. Ces opérations se déploient à l'échelle industrielle avec des rôles spécialisés : fabricants d'identités, faussaires de documents, ouvreurs de comptes, mules et opérateurs d'encaissement. Ils utilisent de plus en plus des tactiques « dormantes », cultivant des identités synthétiques pendant des mois ou des années afin de bâtir un historique de crédit avant d'exécuter des stratagèmes coordonnés d'éclatement. Les données d'Equifax Canada confirment que les profils de cultivation des identités synthétiques sont détectables, mais nécessitent des capacités d'analytique particulières que de nombreuses organisations canadiennes n'ont pas encore déployées [2].

Le CCIAN estime que la menace issue des réseaux criminels organisés qui déploient des identités synthétiques contre les institutions financières canadiennes s'accroît, propulsée par la disponibilité de l'infrastructure de crime comme service documentée à la section 3.3 et par le délai de cultivation qui retarde la détection jusqu'à la phase de monétisation.

## 5.2 Acteurs commandités par des États

***Trajectoire évaluée de la menace : en augmentation, avec un champ d'action qui s'élargit.***

Le CCCS évalue que la Chine, la Russie, l'Iran et la Corée du Nord ont intégré des hypertrucages générés par IA à leurs cyberopérations ciblant le Canada [8]. L'évaluation du CCCS sur le processus démocratique a documenté le recours aux hypertrucages dans au moins 151 élections évaluées entre 2023 et 2024, y compris l'usage de pornographie hypertruquée pour harceler des femmes politiciennes et des personnes en politique s'identifiant comme 2ELGBTQI+ [15]. En juin 2025, les autorités canadiennes ont documenté une campagne d'usurpation d'identité par hypertrucage qui utilisait des messages vocaux générés par IA et des comptes de messagerie imitant des hauts responsables gouvernementaux et des personnalités publiques de premier plan pour escroquer des Canadiens, à des fins spécifiquement de fraude financière [9].

Ces acteurs utilisent également l'IA pour traiter des ensembles de données massifs recueillis sur les personnalités politiques canadiennes, les personnalités publiques et les communautés issues de la diaspora, produisant du renseignement qui rend l'ingénierie sociale plus ciblée et plus convaincante [8] [15].

Le CCIAN estime que l'utilisation par des États de la manipulation identitaire alimentée par l'IA contre des cibles canadiennes s'étend au-delà de l'espionnage traditionnel et des opérations d'influence,

jusqu'à la fraude financière directe, ce qui représente une convergence des vecteurs de menace étatiques et criminels.

## 5.3 Opérateurs de fraude comme service

***Trajectoire évaluée de la menace : en augmentation, avec des barrières à l'entrée en baisse.***

Une couche intermédiaire grandissante entre les développeurs d'outils et les fraudeurs utilisateurs. Ces opérateurs fournissent l'infrastructure, les dossiers d'identité synthétique, les logiciels d'attaque par injection, les outils de substitution de visage et les réseaux de blanchiment d'argent qui permettent à des acteurs peu qualifiés d'exécuter des fraudes sophistiquées. Le Forum économique mondial décrit ce phénomène comme un passage d'une fraude à grande échelle et à faible qualification à des opérations moins nombreuses, plus coordonnées et plus avancées sur le plan technologique [12].

Le CCIAN estime que cette couche intermédiaire est le facilitateur structurel le plus important de la croissance de la fraude identitaire alimentée par l'IA, car elle découple la sophistication de l'attaque des compétences de l'attaquant. L'implication pour les organisations canadiennes, c'est que la modélisation des menaces fondée sur la capacité présumée de l'attaquant devient de moins en moins fiable — la capacité dont disposent même des acteurs peu sophistiqués dépasse désormais le seuil de détection de nombreux systèmes de vérification de l'identité déployés.

## 5.4 Personnes opportunistes

***Trajectoire évaluée de la menace : en augmentation par le volume, stable par la sophistication.***

La catégorie qui connaît la plus forte croissance en volume. Les outils d'IA générative grand public permettent à des personnes sans expertise technique de créer des documents frauduleux, de cloner des voix et de générer des photographies synthétiques. Les données d'Equifax Canada montrent que la fraude de première partie, dans laquelle des individus falsifient leurs propres renseignements, demeure la forme de fraude la plus répandue dans le financement automobile canadien, et que ces acteurs se tournent de plus en plus vers les outils d'IA pour rendre leur tromperie plus convaincante [2].

# 06

# Vecteurs et méthodes

SECTION 06 SUR 10

# 6. Le fonctionnement des attaques : vecteurs et méthodes

## 6.1 Création d'identités synthétiques

Les identités synthétiques combinent de véritables renseignements personnels volés (numéros d'assurance sociale, dates de naissance, adresses) avec des éléments fabriqués générés par IA (noms, photographies, documents). Il en résulte une identité qui passe les contrôles de vérification classiques parce que certaines de ses composantes sont authentiques.

L'IA a transformé chaque élément de ce processus. Les outils d'IA générative produisent des documents d'identité dotés d'une mise en forme, d'éléments de sécurité et de zones lisibles par machine réalistes. Les photographies de visage générées par des réseaux antagonistes génératifs (GAN) sont indiscernables des images réelles. Des documents financiers (bulletins de paie, relevés bancaires, documents fiscaux) peuvent être créés entièrement à partir de rien, sans source. L'analyse des déclarations d'activités suspectes par FinCEN a révélé que les institutions financières détectent souvent les documents d'identité générés par IA en réexaminant les documents d'ouverture de compte, plutôt que lors de la vérification initiale [16].

## 6.2 Contournement de la validation de l'identité

La validation de l'identité — le processus qui consiste à établir qu'un demandeur est bien la personne qu'il prétend être — constitue désormais la principale surface d'attaque à l'échelle mondiale. Le 2026 Identity Fraud Report d'Entrust confirme que les hypertrucages représentent une tentative de fraude biométrique sur cinq, les égoportraits hypertruqués ayant augmenté de 58 % d'une année à l'autre [13]. Les attaques par hypertrucage sont concentrées dans les secteurs financiers à risque élevé : les plateformes de cryptomonnaies absorbent 60 % de la fraude par hypertrucage, les banques « tout numérique » 22 %, et les services de paiement et aux commerçants 13 % [13].

Le vecteur d'attaque le plus dangereux est l'injection numérique, dans laquelle les attaquants utilisent des caméras virtuelles ou une manipulation logicielle pour insérer des contenus synthétiques directement dans le flux de données de vérification, en contournant entièrement la caméra physique. iProov a documenté une hausse de 2 665 % de ce type d'attaque, propulsée en partie par l'infiltration d'outils d'injection dans les magasins d'applications grand public [5]. Les données de renseignement sur les menaces 2026 d'iProov montrent que la surface d'attaque se déplace également selon la plateforme : les attaques par injection visant les appareils iOS ont flambé de 1 151 % au second semestre 2025, contribuant à une hausse annuelle de 741 % [24]. Ce déplacement de plateforme érode l'hypothèse longtemps tenue selon laquelle iOS offrait une résistance structurelle aux attaques par injection et oblige les organisations canadiennes qui s'appuient sur des signaux de vivacité propres à l'appareil à réviser leurs hypothèses de risque par plateforme.

Les attaques par substitution de visage ont bondi de 300 %, les acteurs de menace adaptant spécifiquement leurs outils pour déjouer les systèmes qui utilisent la détection de vivacité, signe d'une course à l'armement adverse où les attaquants ciblent les défenses précises que les organisations déploient [5].

## 6.3 Usurpation d'identité en temps réel

Les hypertrucages ne sont plus préenregistrés. Les acteurs de menace mènent des usurpations en direct et interactives pendant des appels vidéo, des séances d'authentification vocale et des processus de vérification à distance. Le clonage vocal n'exige que quelques secondes d'audio de référence : facilement accessible à partir de sites Web d'entreprise, d'enregistrements de conférences et des médias sociaux. Le Forum économique mondial a confirmé que les pertes liées à la fraude par hypertrucage ont dépassé 200 M$ au seul T1 2025 [7].

## 6.4 Monétisation

Les identités synthétiques et les hypertrucages permettent un éventail de crimes financiers documentés dans l'alerte de FinCEN de novembre 2024 [16] : ouverture frauduleuse de comptes, stratagèmes d'éclatement de crédit, fraude par paiement autorisé poussé, fraude aux prestations et aux prêts, et recrutement de mules financières au moyen de personnages générés par IA.

BREFFAGE SUR LES MENACES DU CCIAN

# 07

# La brèche défensive : pourquoi les protections actuelles sont insuffisantes

SECTION 07 SUR 10

# 7. La brèche défensive : pourquoi les protections actuelles sont insuffisantes

Les organisations canadiennes, et particulièrement les institutions financières, ne restent pas inactives. Les grandes banques investissent massivement dans la détection de la fraude biométrique, la surveillance des transactions et les technologies de vérification de l'identité. Les bureaux de crédit ont déployé des capacités de signalement des identités synthétiques. Les processeurs de paiement ont renforcé leurs exigences d'authentification. Ces investissements sont bien réels et ont produit des améliorations mesurables des taux de détection pour les typologies de fraude connues.

Toutefois, ces investissements se font sur un arrière-plan mondial de préparation insuffisante marquée : le sondage d'Accenture mené auprès de plus de 2 200 dirigeants en cybersécurité a révélé que 90 % des organisations à l'échelle mondiale ne sont pas adéquatement préparées à sécuriser leurs opérations propulsées par l'IA, et que 77 % ne disposent pas de pratiques essentielles en sécurité des données et de l'IA [23].

La lacune n'est pas dans l'investissement de détection. L'analyse du CCIAN cerne trois domaines structurels où l'investissement institutionnel individuel ne peut se substituer à une coordination à l'échelle de l'écosystème.

## 7.1 Renseignement sur les menaces fragmenté

L'Évaluation des cybermenaces nationales du CCCS, les alertes de FinCEN et les rapports de menaces des fournisseurs contribuent tous au portrait global. Aucune ressource unique n'en fait la synthèse en un modèle de menace unifié et adapté au contexte canadien, assorti d'orientations de mise en œuvre exploitables. L'équipe antifraude d'une institution financière peut s'abonner à plusieurs flux de renseignement, mais traduire ces flux en contrôles calibrés et harmonisés avec les attentes réglementaires canadiennes exige une couche de coordination qui n'existe pas actuellement.

Le présent breffage est lui-même une tentative de combler une partie de cette lacune en synthétisant les sources gouvernementales, fournisseurs et internationales en un portrait cohérent des menaces canadiennes. Toutefois, un breffage ponctuel ne saurait remplacer une fonction de renseignement sur les menaces continue et structurée au service de l'écosystème canadien de la confiance numérique.

## 7.2 Des normes sans orientations canadiennes de mise en œuvre

Les normes ont progressé de façon notable, mais une lacune critique de mise en œuvre persiste — et elle est particulièrement aiguë au Canada.

À l'international, le NIST SP 800-63-4 (juillet 2025) est le premier cadre majeur d'assurance de l'identité à imposer des contrôles contre les hypertrucages et les attaques par injection aux niveaux IAL2 et supérieurs [18]. Il précise aux organisations quels contrôles sont requis, mais non la manière de les déployer, de les configurer et de les rendre opérationnels dans le contexte réglementaire et opérationnel canadien. Le NIST AI 100-4 fournit la référence technique la plus complète sur la détection du contenu synthétique, mais reconnaît explicitement que la plupart des approches sont à plusieurs années du déploiement à grande échelle [19].

La norme européenne émerge, mais n'est pas directement applicable. L'ETSI TS 119 461 v2 (février 2025) définit des exigences rigoureuses en matière de validation de l'identité, y compris des défenses contre les attaques par injection et la détection de vivacité [20]. La norme CEN TS 18099 établit la norme européenne pour les tests de détection des attaques par injection. Ces normes sont techniquement importantes, mais conçues pour le contexte réglementaire de l'UE.

Le Canada ne dispose pas d'une norme nationale d'assurance de l'identité comparable en portée au NIST SP 800-63-4. L'orientation canadienne existante, l'ITSP.30.031 v3 du Centre de la sécurité des télécommunications, s'aligne sur l'ancienne NIST SP 800-63-2 et est entièrement antérieure au paysage des menaces par IA générative. Les organisations canadiennes qui cherchent à déployer des défenses contre les hypertrucages et les attaques par injection doivent donc interpréter les cadres américains ou européens sans cartographie réglementaire canadienne, sans adaptation sectorielle, ni critères de conformité conçus pour l'environnement opérationnel canadien. Le CCIAN évalue cela comme une lacune importante qui accroît à la fois le coût de mise en œuvre et le risque de conformité pour les organisations canadiennes.

## 7.3 Interopérabilité et coordination intersectorielle

La lacune la plus importante ne se trouve pas à l'intérieur des institutions individuelles, mais entre elles. La fraude à l'identité synthétique est intrinsèquement intersectorielle — une identité fabriquée qui ouvre un compte dans une banque, se bâtit un historique de crédit chez une autre et se monétise chez une troisième, en exploitant l'absence d'assurance partagée de l'identité à l'échelle de l'écosystème. L'investissement individuel dans les technologies de détection, si important soit-il, ne peut combler cette lacune sans des normes communes d'assurance de la vérification de l'identité, des indicateurs partagés de compromission par identité synthétique et une interopérabilité intersectorielle permettant qu'une vérification de l'identité menée dans un contexte (p. ex., juridique) puisse être reconnue dans un autre (p. ex., services financiers).

Aucun mécanisme canadien n'existe actuellement pour assurer cette interopérabilité à grande échelle. Le cadre de conformité du CCP démontre que la confiance intersectorielle en matière de vérification de l'identité est techniquement réalisable; son déploiement à l'échelle de la production dans le secteur juridique le confirme [17]. Toutefois, l'extension de ce modèle aux services financiers, aux soins de santé, au gouvernement et aux télécommunications exige une coordination délibérée de l'écosystème qu'aucune institution seule ne peut entreprendre.

# 08

# Ce qui est en jeu : l'exposition par secteur

SECTION 08 SUR 10

# 8. Ce qui est en jeu : l'exposition par secteur

Les lacunes structurelles de défense cernées à la section 7 créent une exposition différenciée dans les secteurs économiques canadiens. L'analyse qui suit cartographie les principaux vecteurs de menace par rapport aux facteurs de risque propres au Canada.

| SECTEUR | PRINCIPAUX VECTEURS DE MENACE | FACTEURS DE RISQUE PROPRES AU CANADA |
|---|---|---|
| Services financiers | Ouverture de comptes par identité synthétique; éclatement de crédit; paiements autorisés par hypertrucage; contournement des mesures anti-blanchiment | Obligations du BSIF et du CANAFE; expansion du secteur bancaire ouvert; intégrité des Paiements Canada; exposition des coopératives de crédit |
| Juridique | Fraude à la vérification d'identité de clients à distance; exploitation des comptes en fidéicommis; usurpation par hypertrucage aux fins de fraude lors de transferts de propriété | Plus de 700 000 transactions de vérification de l'identité à distance rapportées par les membres [17]; pratique à distance en expansion; les passeports comptent pour 44 % des documents frauduleux soumis dans le secteur des services professionnels à l'échelle mondiale [13] |
| Soins de santé | Fraude à l'identité de patients; fraude aux ordonnances; fraude aux prestations; accès aux données de santé | Vérification des cartes d'assurance maladie provinciales; normes d'Inforoute Santé du Canada; législation sur la protection des renseignements personnels en santé |
| Gouvernement | Fraude aux prestations; identité synthétique pour délivrance de justificatifs; ingérence électorale; exploitation des services aux citoyens | Programmes provinciaux d'identité numérique (C.-B. : 4,6 M d'utilisateurs); prestation de services fédéraux; intégrité du processus démocratique |
| Télécommunications | Fraude par échange de carte SIM; fraude à l'identité des abonnés; prise de contrôle de comptes; manipulation du service à la clientèle par hypertrucage | Entreprises de télécommunications comme points d'ancrage de la vérification d'identité pour d'autres secteurs; exigences du CRTC |

| SECTEUR | PRINCIPAUX VECTEURS DE MENACE | FACTEURS DE RISQUE PROPRES AU CANADA |
|---|---|---|
| Énergie / Infrastructures essentielles | Compromission d'identité par des initiés; accès aux systèmes SCADA/TO par exploitation d'identité; fraude identitaire dans la chaîne d'approvisionnement | Désignation des infrastructures essentielles par le CCCS; législation sur la protection des infrastructures essentielles; convergence TO/TI |

Répartition des vecteurs de menace par secteur. Les données du réseau mondial de vérification d'identité d'Entrust montrent que la fraude à l'ouverture de nouveau compte et la fraude par prise de contrôle de compte (PCC) se concentrent différemment selon les secteurs. La fraude au nouveau compte domine dans les contextes où des incitations initiales ou une intégration rapide sont offertes : 67 % des tentatives de fraude en crypto surviennent au moment de l'intégration, et 64 % de la fraude dans les services professionnels est une fraude au nouveau compte. La fraude par prise de contrôle de compte domine là où les comptes ont une valeur à long terme : 82 % de la fraude dans le secteur des paiements et 55 % de la fraude dans les banques « tout numérique » surviennent après l'intégration [13]. Les organisations canadiennes devraient calibrer leurs investissements en contrôles en fonction du vecteur dominant dans leur secteur — contrôles à l'étape de l'intégration pour les activités à fortes incitations, et contrôles de surveillance et d'authentification post-intégration pour les environnements de comptes à forte valeur.

> **Écart de couverture en cyberassurance.** Toutes les organisations, peu importe le secteur, devraient revoir leur couverture en cyberassurance. De nombreuses polices standard excluent les pertes lorsqu'un employé initie « volontairement » un transfert, même lorsqu'une usurpation par hypertrucage a induit cette action. Les organisations devraient vérifier que leurs polices couvrent explicitement l'ingénierie sociale, la fraude par transfert de fonds (FTF) et les scénarios d'usurpation alimentés par l'IA. Cet écart de couverture représente un risque matériel non assuré pour les organisations qui n'ont pas récemment audité leurs polices.

## 8.1 Actions immédiates pour les organisations aux ressources limitées

Le CCIAN a élaboré un document complémentaire autonome, Guide de démarrage rapide : défenses immédiates contre la fraude identitaire par IA, qui présente huit actions précises et peu coûteuses que les petites et moyennes entreprises, les cabinets de services professionnels et les organisations aux ressources limitées peuvent déployer en quelques jours. Le Guide de démarrage rapide traite de la vérification obligatoire par rappel, des périodes de refroidissement, de la double autorisation, des clés d'authentification prépartagées, des capacités d'authentification résistantes à l'hameçonnage, de

l'authentification de domaine de courriel, de l'intégration à composante physique d'abord et des orientations pour l'audit de la cyberassurance.

# 09

# Ce qui s'en vient : les menaces émergentes à l'horizon

SECTION 09 SUR 10

# 9. Ce qui s'en vient : les menaces émergentes à l'horizon

Les organisations devraient se préparer aux développements suivants au cours des 12 à 24 prochains mois :

**Agents autonomes de fraude par IA.** Le Forum économique mondial projette que des agents d'IA combinant IA générative, automatisation et apprentissage par renforcement créeront de manière autonome des identités synthétiques, interagiront avec les systèmes de vérification et s'adapteront en fonction des résultats [12]. Ces agents opéreront à la vitesse machine, risquant de submerger les processus d'examen manuel. Le CCIAN estime qu'il s'agit de l'escalade à court terme la plus importante du paysage des menaces, car elle élimine le goulot d'étranglement humain qui limite actuellement la capacité de traitement des opérations frauduleuses sophistiquées.

**Hypertrucages multimodaux en temps réel.** Les hypertrucages actuels ciblent généralement une seule modalité (visage, voix ou document). La convergence vers un hypertrucage simultané visage-voix-document lors d'interactions en direct mettra à l'épreuve les défenses qui reposent sur des contrôles de cohérence intermodale. Aucune norme canadienne ou internationale publiée n'aborde actuellement les exigences relatives à la détection d'hypertrucages multimodaux.

**Attaques par hypertrucage contre les écosystèmes de justificatifs numériques.** À mesure que le Canada et l'UE déploient à plus grande échelle leur infrastructure de justificatifs vérifiables et de portefeuilles numériques, les acteurs de menace cibleront les processus de délivrance, de présentation et de révocation. Les émetteurs compromis, les portefeuilles clonés et la présentation de justificatifs synthétiques sont des vecteurs de menace émergents pour des systèmes encore en conception. Les organisations participant à la conception d'écosystèmes de justificatifs devraient intégrer dès le départ la modélisation des menaces en contexte adversaire, plutôt que d'ajouter des défenses après coup.

**Menaces internes amplifiées par l'IA.** La technologie des hypertrucages permet l'usurpation d'employés internes pour élever des privilèges, exfiltrer des données et manipuler les systèmes de gouvernance de l'identité. Les organisations dont les effectifs sont en télétravail sont particulièrement exposées.

**Usurpation par hypertrucage dans les flux de travail en entreprise.** Les données de renseignement sur les menaces 2026 d'iProov rapportent que l'usurpation par hypertrucage s'étend au sein des entreprises à travers les flux de travail quotidiens, particulièrement les interactions vidéo [24]. Le cas Arup documenté à la section 3.2 n'est plus une exception; les réunions vidéo de routine, les appels d'approbation et les conversations internes de vérification deviennent des surfaces d'attaque viables. Les organisations canadiennes devraient présumer que tout flux de travail médiatisé par vidéo autorisant un paiement, un accès ou une prise de décision se trouve dans l'enveloppe de menace, et devraient

déployer des contrôles de vérification hors bande pour les transactions matérielles, peu importe l'apparent rang hiérarchique ou la familiarité de la personne à l'écran.

**Fraude au recrutement facilitée par les hypertrucages.** Des identités générées par IA, des curriculum vitæ synthétiques et des entrevues vidéo par hypertrucage en direct sont utilisés pour placer des candidats frauduleux au sein d'organisations cibles, facilitant le vol subséquent de données, l'introduction de maliciels et la fraude financière. Entrust rapporte que le recrutement est désormais parmi les secteurs non financiers les plus ciblés, et Gartner projette qu'un candidat sur quatre à l'échelle mondiale sera un faux d'ici 2028 [13]. Les organisations canadiennes dont les processus d'embauche sont distribués ou à distance — particulièrement celles qui intègrent des entrepreneurs, du personnel technique ou des rôles à accès privilégié sans vérification en personne — devraient considérer l'embauche comme un point de contrôle d'assurance de l'identité, et non uniquement comme un processus des RH.

**Accélération réglementaire.** La mise en œuvre par étapes de la Loi sur l'IA de l'Union européenne (2025-2026), la Loi sur l'intelligence artificielle et les données (LIAD) proposée par le Canada, ainsi que l'évolution de la législation provinciale sur l'identité numérique créeront de nouvelles obligations de conformité. Les organisations qui investissent proactivement dans des défenses contre l'identité synthétique et les hypertrucages seront mieux positionnées à mesure que les exigences se cristalliseront.

# 10

# La réponse prévue par le CCIAN

SECTION 10 SUR 10

# 10. La réponse prévue par le CCIAN

Le présent breffage sur les menaces est le premier d'une série de ressources que le CCIAN élabore dans le cadre du pilier Résilience à la fraude et préparation à l'IA de son Cadre stratégique 2025-2030. Parmi les ressources prévues figurent un Guide de mise en œuvre pour la gestion des vecteurs de menace par IA : identités synthétiques et hypertrucages, qui fournit des contrôles rattachés aux critères de conformité du CCP et au NIST SP 800-63-4; un Addenda aux critères de conformité du CCP pour la vérification de l'identité assistée par l'IA; et des ressources sectorielles, à commencer par les services financiers et le juridique.

> **Participez.** Le CCIAN invite les organisations membres et les partenaires à examiner le présent breffage et à y répondre, à contribuer du renseignement sur les menaces et de l'expérience de mise en œuvre pour renforcer la base de données probantes, et à s'engager auprès du Comité d'experts du cadre de confiance (CECC) dans l'élaboration des critères de conformité. Pour communiquer : contact@diacc.ca

# Références

**[1]** Centre antifraude du Canada, Rapport statistique annuel 2024 et Mois de la prévention de la fraude 2025. 638 M$ en pertes déclarées en 2024 (en hausse par rapport à 577 M$ en 2023 et 531 M$ en 2022); 108 878 rapports reçus; au moins 34 621 victimes; taux de déclaration de 5 à 10 %. Les pertes déclarées cumulatives depuis 2021 dépassent 2 G$. Gouvernement du Canada.
*https://www.canada.ca/en/competition-bureau/news/2025/02/fraud-prevention-month-to-focus-on-impersonation-fraud-one-of-the-fastest-growing-forms-of-fraud.html*

**[2]** Equifax Canada, H1 2024 Market Pulse Fraud Trends, septembre 2024. La fraude à l'identité synthétique est passée de 2,8 % à 8 % des demandes de crédit entre le T2 2023 et le T2 2024. Fraude identitaire : 48,4 % de toutes les demandes frauduleuses signalées, en hausse par rapport à 43,2 %. (Membre du CCIAN)
*https://assets.equifax.com/marketing/canada/assets/reports_white_papers/h1-2024-fraud-trends-en.pdf*

**[3]** Deloitte Center for Financial Services, Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking, 2024. Projette que la fraude alimentée par l'IA atteindra 40 G$ par année d'ici 2027 aux États-Unis. Cité par le Forum économique mondial et l'UNESCO. (Membre du CCIAN)
*https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html*

**[4]** Entrust Cybersecurity Institute, 2025 Identity Fraud Report, novembre 2024. Des tentatives d'hypertrucage se sont produites toutes les 5 minutes en 2024; les contrefaçons numériques de documents ont augmenté de 244 % d'une année à l'autre; les contrefaçons numériques représentent désormais 57 % de toute la fraude documentaire. (Membre du CCIAN)
*https://www.entrust.com/company/newsroom/deepfake-attacks-strike-every-five-minutes-amid-244-surge-in-digital-document-forgeries*

**[5]** iProov, Threat Intelligence Report 2025 : Remote Identity Under Attack, février 2025. Les attaques par caméra virtuelle native ont augmenté de 2 665 %; les attaques par substitution de visage ont bondi de 300 %; écosystème de crime comme service comptant près de 24 000 utilisateurs. (Membre du CCIAN)
*https://www.iproov.com/reports/threat-intelligence-report-2025*

**[6]** iProov, Deepfake Consumer Study, février 2025. Seuls 0,1 % des 2 000 consommateurs du Royaume-Uni et des États-Unis ont repéré correctement tous les stimuli hypertruqués et réels. (Membre du CCIAN)
*https://www.iproov.com/blog/deepfakes-statistics-solutions-biometric-protection*

**[7]** World Economic Forum, « Detecting dangerous AI is essential in the deepfake era », juillet 2025. Exactitude de la détection humaine des hypertrucages à 55-60 %; plus de 200 M$ de pertes confirmées liées à la fraude par hypertrucage au seul T1 2025. (Organisme sans but lucratif)
*https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/*

**[8]** Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2025-2026, octobre 2024. Identifie la désinformation améliorée par l'IA, les hypertrucages et les cybermenaces commanditées par des États comme des risques en accélération. Objectifs de préparation à la cybersécurité intersectoriels : 36 objectifs fondamentaux. (Gouvernement du Canada; membre du CCIAN)
*https://www.canada.ca/en/communications-security/news/2024/10/canadian-centre-for-cyber-security-releases-national-cyber-threat-assessment-2025-2026.html*

**[9]** Centre antifraude du Canada / CCCS, Avis conjoint : campagne d'usurpation par hypertrucage ciblant les Canadiens, juin 2025. Documente des messages vocaux générés par IA et des comptes de messagerie imitant des hauts responsables gouvernementaux et des personnalités publiques de premier plan, utilisés dans des fraudes financières ciblant des Canadiens. (Gouvernement du Canada)
*https://antifraudcentre-centreantifraude.ca/news-nouvelles/2025/2025-06-23-eng.htm*

**[10]** World Economic Forum, « Cybercrime : Lessons learned from a $25m deepfake attack », février 2025. Entrevue avec Rob Greig, DPI d'Arup, sur le cas de fraude par hypertrucage de 25,6 M$. M. Greig a créé un hypertrucage de

lui-même en 45 minutes à l'aide de logiciels à code source ouvert. (Organisme sans but lucratif)
*https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/*

**[11]** Hong Kong Police Force, point de presse, février 2024. A confirmé que des hypertrucages générés par IA avaient été utilisés pour se faire passer pour le chef des finances et les collègues d'une multinationale, entraînant des transferts frauduleux de 25,6 M$ (200 M$ HK). Aucune URL directe disponible; incident rapporté par le Forum économique mondial [10]. (Gouvernement)

**[12]** World Economic Forum, « How identity fraud is changing in the age of AI », décembre 2025. Documente la montée des agents d'IA frauduleuse combinant IA générative, automatisation et apprentissage par renforcement. Projette que ces agents pourraient devenir courants d'ici 18 mois. Les attaques frauduleuses à étapes multiples ont augmenté de 180 % d'une année à l'autre. (Organisme sans but lucratif)
*https://www.weforum.org/stories/2025/12/how-identity-fraud-is-increasing-in-the-age-of-ai/*

**[13]** Entrust Cybersecurity Institute, 2026 Identity Fraud Report, novembre 2025. Les hypertrucages représentent 1 tentative de fraude biométrique sur 5; les égoportraits hypertruqués ont augmenté de 58 %; les attaques par injection ont bondi de 40 % d'une année à l'autre. (Membre du CCIAN)
*https://www.entrust.com/company/newsroom/deepfakes-social-engineering-and-injection-attacks-on-the-rise*

**[14]** CCIAN, Soumission sur la consultation en IA au gouvernement fédéral, octobre 2025. Position politique appelant à la reconnaissance des services d'identité, d'authentification, de vérification et de cadre de confiance comme infrastructures essentielles pour soutenir la mise à l'échelle sécuritaire et digne de confiance de l'écosystème d'IA. Cadre stratégique 2025-2030 du CCIAN : vise une réduction de 50 % des pertes liées à la fraude d'ici 2031. (CCIAN) *https://diacc.ca/2025/11/03/diacc-ai-consultation-submission-to-the-federal-government/*

**[15]** CCCS, Cybermenaces contre le processus démocratique du Canada : mise à jour 2025. A évalué 151 élections (2023-2024); au moins 6 ont connu du harcèlement de politiciens par hypertrucage. Pornographie par hypertrucage ciblant des femmes et des personnes s'identifiant comme 2ELGBTQI+. Acteurs étatiques utilisant l'IA pour traiter des ensembles de données sur les politiciens canadiens et les communautés issues de la diaspora. (Gouvernement du Canada)
*https://www.cse-cst.gc.ca/en/information-resources/news/communications-security-establishment-canada-releases-2025-update-report-cyber-threats-canadas-democratic-process*

**[16]** FinCEN, FIN-2024-Alert004 : Fraud Schemes Involving Deepfake Media, 13 novembre 2024. Indicateurs de signaux d'alarme pour les institutions financières; exigences de déclaration d'activités suspectes; typologies, y compris l'ouverture frauduleuse de comptes et la fraude à l'identité synthétique. (Gouvernement des É.-U.)
*https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial*

**[17]** CCIAN, PCTF Legal Professionals Profile Final Recommendation V1.1, octobre 2025. Les fournisseurs certifiés CCP de vérification de l'identité dans le secteur juridique incluent Chicago Title, FCT, Treefort Technologies et Vaultie (tous au niveau NA2, composante Personne vérifiée). Plus de 700 000 transactions de vérification d'identité de clients ont été déclarées par les membres à travers plusieurs fournisseurs, d'octobre 2023 à octobre 2024. (CCIAN)
*https://diacc.ca/2025/09/22/the-diacc-releases-its-pctf-legal-professionals-profile-final-recommendation-v1-1/*

**[18]** NIST Special Publication 800-63-4, Digital Identity Guidelines, juillet 2025. Premier cadre majeur à imposer des contrôles contre les attaques par injection et les hypertrucages aux niveaux IAL2 et supérieurs. (Gouvernement des É.-U.) *https://pages.nist.gov/800-63-4/*

**[19]** NIST AI 100-4, Reducing Risks Posed by Synthetic Content, novembre 2024. Référence technique pour la détection, le filigranage et le suivi de provenance. Reconnaît que la plupart des approches sont à plusieurs années du déploiement à grande échelle. (Gouvernement des É.-U.)
*https://www.nist.gov/publications/reducing-risks-posed-synthetic-content-overview-technical-approaches-digital-content*

**[20]** ETSI TS 119 461 v2, février 2025. Exigences de validation de l'identité, y compris la détection de vivacité et les défenses contre les attaques par injection. Deux niveaux de validation de l'identité (Baseline et Extended).

(Organisme de normalisation européen)
*https://www.signicat.com/blog/etsi-119-461-v2-1-1-updates-you-need-to-know*

**[21]** iProov, novembre 2025. Premier et seul fournisseur certifié de manière indépendante selon les exigences de vérification biométrique du NIST SP 800-63-4, au moyen des tests de niveau 2 de la norme CEN TS 18099 par Ingenium Biometrics. (Membre du CCIAN)
*https://www.iproov.com/press/nist-digital-identity-requirements-first-biometrics-vendor-demonstrating-deepfake-resilience*

**[22]** Ernst & Young LLP, 2025 EY Cybersecurity Study : Bridging the C-suite Disconnect, avril 2025. Sondage auprès de 800 hauts dirigeants américains. Une analyse distincte d'EY portant sur les entreprises du Russell 3000 a révélé que celles qui subissent un incident cyber voient généralement leur cours boursier diminuer de 1,5 % au cours des 90 jours suivants. (Membre du CCIAN)
*https://www.ey.com/en_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds*

**[23]** Accenture, State of Cybersecurity Resilience 2025, juin 2025. Sondage auprès de 2 286 dirigeants en cybersécurité et en technologies dans 17 pays. 90 % des organisations ne sont pas adéquatement préparées à sécuriser leur avenir propulsé par l'IA; 77 % ne disposent pas de pratiques essentielles en sécurité des données et de l'IA. (Membre du CCIAN)
*https://newsroom.accenture.com/news/2025/only-one-in-10-organizations-globally-are-ready-to-protect-against-ai-augmented-cyber-threats*

**[24]** iProov, Threat Intelligence Report 2026. Les attaques par injection visant les appareils iOS ont flambé de 1 151 % au second semestre 2025, contribuant à une hausse annuelle de 741 %; l'usurpation par hypertrucage s'étend dans les flux de travail en entreprise axés sur la vidéo; l'Asie du Sud-Est a connu une flambée de 720 % des attaques au T3 2025. (Membre du CCIAN) *https://www.iproov.com/reports/threat-intelligence-report-2026*

# Annexe A : Références de l'écosystème du CCIAN

*Le corps du breffage sur les menaces (sections 1 à 10) est neutre à l'égard des fournisseurs. La présente annexe résume les capacités offertes par les organisations membres du CCIAN dont la recherche publiée a contribué au renseignement sur les menaces de ce breffage, ainsi que par les fournisseurs certifiés CCP mentionnés dans l'analyse.*

**Accenture** · **SERVICES PROFESSIONNELS ET CONSEILS**
Cabinet de services professionnels et de conseils en cybersécurité. A contribué une analyse de la préparation organisationnelle mondiale en cybersécurité au moyen de son rapport State of Cybersecurity Resilience 2025 [23].

**Chicago Title** · **FOURNISSEUR CERTIFIÉ CCP**
Fournisseur certifié CCP de vérification de l'identité. Certifié au niveau NA2 selon la composante Personne vérifiée du CCP [17].

**Deloitte** · **SERVICES PROFESSIONNELS ET CONSEILS**
Cabinet mondial de services professionnels offrant des services d'audit, fiscalité, conseil et services-conseils de premier plan. A contribué des projections sur les pertes liées à la fraude par IA générative (40 G$ d'ici 2027 aux É.-U.) par l'intermédiaire de son rapport du Center for Financial Services en 2024 [3]. Deloitte Canada offre des services de gestion des risques, réglementation et juricomptabilité, de cybersécurité, d'IA générative et plus encore.

**Entrust** · **VÉRIFICATION DE L'IDENTITÉ ET CYBERSÉCURITÉ**
Fournisseur de plateforme de vérification de l'identité et de cybersécurité. A contribué des données mondiales sur la contrefaçon de documents, la fréquence des hypertrucages et les tendances sectorielles de la fraude par l'intermédiaire des rapports annuels de son Cybersecurity Institute [4] [13]. Offre des capacités intégrées de vérification de l'identité, d'authentification et de gestion du cycle de vie, y compris la détection des hypertrucages.

**Equifax Canada** · **BUREAU DE CRÉDIT ET ANALYTIQUE DE FRAUDE**
Fournisseur de bureau de crédit et d'analytique de fraude. A contribué au présent breffage des données canadiennes sur les tendances de la fraude, y compris les taux de fraude à l'identité synthétique, l'analyse sectorielle de la fraude et des indicateurs de fraude dans les demandes de crédit [2]. Offre l'analytique FraudIQ pour la détection et la prévention de la fraude durant l'intégration.

**Ernst & Young** · **SERVICES PROFESSIONNELS ET CONSEILS**
Cabinet de services professionnels et de conseils en cybersécurité. A contribué une analyse de l'incidence financière des incidents cyber sur les sociétés cotées en bourse par l'intermédiaire de son Cybersecurity Study 2025 [22].

**FCT** · **FOURNISSEUR CERTIFIÉ CCP**
Fournisseur certifié CCP de vérification de l'identité (technologie en partenariat avec Bluink). Certifié au niveau NA2 selon la composante Personne vérifiée du CCP. Déployé à l'échelle de la production dans le secteur juridique canadien [17].

**iProov** · **VÉRIFICATION BIOMÉTRIQUE**
Fournisseur de vérification biométrique et de détection de vivacité. A contribué des données de tendances sur les attaques par injection et par substitution de visage par l'intermédiaire de son Threat Intelligence Report 2025 [5], de son Threat Intelligence Report 2026 [24] et de ses recherches auprès des consommateurs sur la détection des hypertrucages [6]. Certifié de manière indépendante selon les exigences de vérification biométrique du NIST SP 800-63-4 au moyen des tests de niveau 2 de la norme CEN TS 18099 par Ingenium Biometrics [21]. Exploite le iProov Security Operations Centre (iSOC), qui fournit du renseignement en temps réel sur les vecteurs d'attaque biométriques.

**Treefort Technologies** · **FOURNISSEUR CERTIFIÉ CCP**
Treefort est conforme à SOC 2 Type II selon les cinq critères de confiance et est un fournisseur certifié CCP de vérification de l'identité, certifié au niveau NA2 selon la composante Personne vérifiée du CCP. La plateforme utilise une approche en couches à facteurs multiples, triangulant les données à travers plus de 1 750 points de données d'authentification provenant de sources fiables, plutôt que de s'appuyer sur une méthode de vérification unique [17].

**Vaultie** · **FOURNISSEUR CERTIFIÉ CCP**
Fournisseur certifié CCP de vérification de l'identité. Certifié au niveau NA2 selon la composante Personne vérifiée du CCP et au niveau NA3 selon la composante Portefeuille numérique du CCP [17].

*Note de recherche : Le présent breffage a été élaboré en utilisant l'IA Claude d'Anthropic comme outil de recherche et de rédaction. Claude a été utilisé pour identifier, extraire et synthétiser des données accessibles au public provenant de sources gouvernementales, universitaires et industrielles. Toutes les statistiques ont été vérifiées de manière indépendante par rapport aux sources primaires, et l'analyse finale ainsi que les jugements éditoriaux reflètent l'examen par le personnel du CCIAN. Les URL des sources sont fournies aux fins de vérification indépendante.*

**CCIAN — là où la confiance numérique devient affaire.**