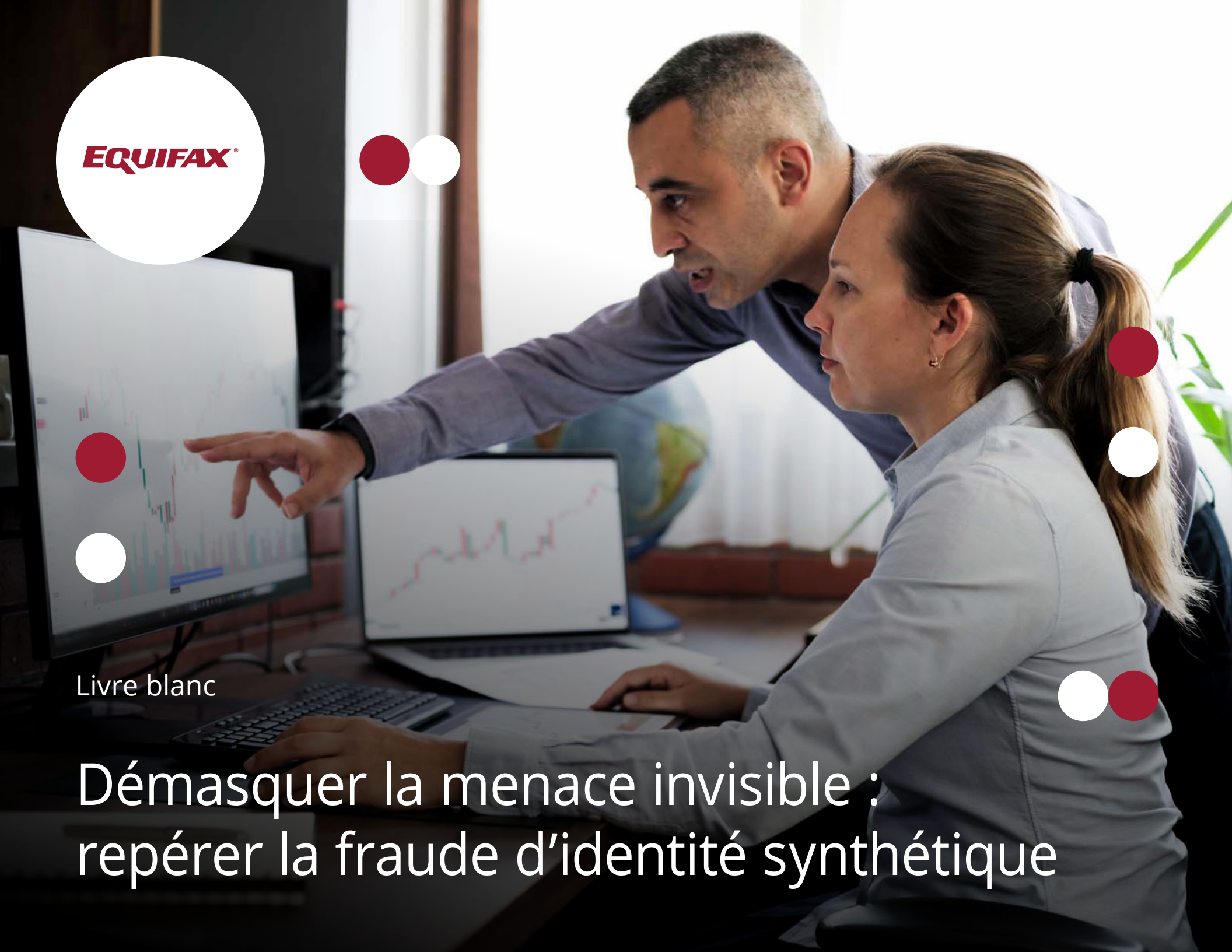




EQUIFAX®

Livre blanc

Démasquer la menace invisible :
repérer la fraude d'identité synthétique



La fraude d'identité synthétique apparaît comme une menace sérieuse au sein de l'écosystème financier canadien. Il s'agit d'un délit financier extrêmement sophistiqué dans le cadre duquel des acteurs malveillants combinent des renseignements personnels réels et fictifs pour créer une nouvelle fausse identité. Les fraudeurs entretiennent ces profils pendant des mois, voire des années, jusqu'à ce qu'ils obtiennent un bon pointage de crédit. Ensuite, ils épuisent leur crédit et disparaissent, en laissant les prêteurs assumer les pertes financières.



L'ampleur de ce problème est considérable. Au Canada, les fraudes d'identité synthétique ont doublé en proportion de toutes les demandes frauduleuses entre 2022 et 2024¹. En outre, les données sur le marché américain montrent que la fraude d'identité synthétique est à l'origine de près de 20 % des pertes de crédit² et qu'elle représente entre 80 et 85 % de toutes les fraudes d'identité³.

Cependant, l'ampleur réelle du problème est masquée, car les pertes liées à la fraude d'identité synthétique sont souvent classées à tort comme des créances irrécouvrables. En l'absence d'une identité réelle associée à la dette, les entreprises gaspillent davantage de ressources à courir après un client inexistant. Cette situation peut pousser les prêteurs à imposer des politiques en matière de crédit plus strictes, sans pour autant s'attaquer à la cause profonde de ces pertes. Pour lutter efficacement contre ce phénomène, les prêteurs doivent s'appuyer sur leurs méthodes de vérification existantes.

« Les acteurs malveillants utilisent des identités et des données personnelles volées pour semer l'anarchie au sein de l'écosystème financier canadien. C'est pourquoi la prévention de la fraude d'identité synthétique nécessite un changement de stratégie. Nous devons cesser de nous demander "ce client est-il solvable?" ou "cette signature est-elle authentique?", et commencer à nous demander "**cette personne existe-t-elle réellement?**" », affirme **Cherolle Prince**, directrice des conseils en matière de fraude à Equifax Canada.

« Les acteurs malveillants utilisent des identités et des données personnelles volées pour semer l'anarchie au sein de l'écosystème financier canadien. C'est pourquoi la prévention de la fraude d'identité synthétique nécessite un changement de stratégie. Nous devons cesser de nous demander "ce client est-il solvable?" ou "cette signature est-elle authentique?", et commencer à nous demander "**cette personne existe-t-elle réellement?**". »

Cherolle Prince,

Directrice des conseils en matière de fraude, Equifax Canada



L'anatomie d'une identité synthétique : comprendre l'arnaque à long terme

Contrairement au vol d'identité traditionnel, qui consiste en la prise de contrôle d'un compte existant et légitime par un criminel, la fraude d'identité synthétique implique une approche plus longue. Le processus se déroule selon un cycle délibéré à plusieurs étapes qui commence par la collecte de données. Les fraudeurs recueillent les renseignements personnels de consommateurs à la suite de violations de données à grande échelle, les achètent sur le Web caché, ou incitent les consommateurs vulnérables à leur communiquer leurs données personnelles par le biais d'escroqueries.

« Une identité synthétique est une identité — une “personne” — qui n'existe pas », affirme **Chris Jepsen, directeur de la gestion des produits liés à l'identité et à la conformité à Equifax Canada**. « Les fraudeurs peuvent créer une identité synthétique à partir d'une combinaison d'éléments réels et faux, comme le nom d'une personne réelle jumelé à un numéro d'assurance sociale illégitime, conçue pour réussir à des vérifications superficielles. »

Cette escroquerie minutieusement orchestrée, qui comporte plusieurs étapes, s'étend sur des mois ou des années :



L'ouverture du compte Le 1^{er} mois

Le fraudeur fait une demande pour un produit de crédit d'entrée de gamme, comme une carte de crédit avec garantie ou à faible limite. L'objectif n'est pas d'obtenir de l'argent tout de suite, mais bien de s'implanter.



L'accumulation des antécédents de crédit Du 2^e au 6^e mois

L'identité se comporte comme un client idéal, en remboursant son solde chaque mois.



Le rehaussement Du 6^e au 12^e mois

À mesure que les modèles d'évaluation des risques commencent à reconnaître le client comme un emprunteur fiable, les restrictions de crédit s'assouplissent : les limites de crédit sont augmentées ou le client passe à une carte sans garantie.



L'ascension du crédit Du 12^e au 24^e mois

Grâce aux antécédents solides de l'identité, son pointage de crédit fait d'elle un client principal. Le fraudeur obtient ainsi des prêts personnels ou du financement automobile d'un montant considérable.



C'est dès qu'il obtient un pointage de crédit « de premier ordre » qu'il commet une **fraude par détournement avec fuite**. Le fraudeur contracte des prêts personnels, utilise ses cartes de crédit jusqu'à leur limite maximale et obtient du financement automobile pour ensuite disparaître avec les actifs. Les créanciers tentent de récupérer leur argent, mais n'y parviennent pas car cette personne n'a jamais existé.

La menace invisible : tomber dans le piège du profil idéal

Pour les institutions financières, le défi consiste à détecter ces faux utilisateurs *avant* que le détournement avec fuite ne se produise. Ces identités ne susciteront pas forcément de soupçons lors du premier contact, et comme il n'y a pas de véritable victime dont la solvabilité serait compromise, personne n'appelle la banque pour signaler une activité frauduleuse.

La solvabilité des profils créés par les fraudeurs est conçue pour paraître irréprochable, mais cela ne reflète qu'une partie de la réalité. Les achats à crédit effectués par les consommateurs réels sont irréguliers : ils sont motivés par des événements de la vie quotidienne et des besoins financiers imprévus. L'établissement d'un bon pointage de crédit se produit sur une plus longue durée. À l'inverse, l'utilisateur d'un profil synthétique se procure successivement des produits de crédit spécifiques, choisis pour l'incidence positive maximale qu'ils peuvent avoir sur le pointage de crédit. Ainsi, ces deux profils peuvent afficher le même pointage de crédit, mais les comportements sous-jacents révèlent des réalités différentes.

Ces indices peuvent échapper aux systèmes d'intégration traditionnels, ce qui fait que 95 % des identités synthétiques ne sont pas détectées au cours du processus d'intégration⁴. « Les identités synthétiques sont généralement entretenues pendant 18 à 24 mois pour imiter le comportement de consommateurs exemplaires, ce qui les rend difficiles à détecter, explique Mme Prince. De plus, les méthodes de détection actuelles peuvent être coûteuses, encombrantes, et appliquées trop tard dans le processus de conversion. »

La technologie, un facteur amplificateur de la menace

La menace que représente la fraude d'identité synthétique est aggravée par les progrès rapides des technologies modernes. En effet, la technologie agit comme un accélérateur et réduit les obstacles à l'accès, ce qui permet même aux criminels financiers inexpérimentés de commettre des fraudes.

La vitesse à laquelle ces attaques peuvent être menées et les données synthétiques testées a augmenté. Les fraudeurs peuvent désormais générer des identités solides et de grande qualité en employant moins d'efforts. Pour contrer ces attaques, les organisations doivent utiliser l'apprentissage automatique avancé et l'IA dans leurs propres stratégies de défense.

Au-delà des lignes d'opérations commerciales : l'importance de la « poussière numérique »

Si les dossiers de crédit traditionnels et les points de données statiques ne suffisent plus à déterminer si une personne est bien réelle, les organisations doivent chercher ailleurs. La clé réside dans le fait de ne plus se limiter à la vérification de données statiques, mais d'évaluer les interactions passées du demandeur et l'empreinte non financière de celui-ci. L'utilisation de signaux supplémentaires de ce genre peut aider à prévoir la probabilité d'un risque de fraude.

Si les fraudeurs peuvent se forger un profil financier, il leur est en revanche extrêmement difficile de créer une vie numérique à plusieurs facettes. En effet, l'écosystème numérique offre une multitude de données différentes susceptibles de mettre au jour les profils synthétiques.

Ces données comprennent des éléments du quotidien tels que les factures de services publics, les loyers, les abonnements récurrents, les données relatives aux appareils, ainsi que les transactions en ligne liées au commerce électronique ou au covoiturage. Une identité synthétique ne dispose pas de cette empreinte numérique riche et chaotique, car elle n'évolue pas dans le monde réel.

L'intégration d'autres sources de données, non financières, offre une image plus précise de la véritable nature d'une identité, mettant en évidence les lacunes que les fraudeurs ne peuvent pas facilement combler. Associée aux données sur le comportement, cette vision d'ensemble devient plus claire. C'est là que l'ensemble de données d'Equifax, particulièrement complet, joue un rôle crucial : grâce aux plus grandes bases de données sur les consommateurs et les entreprises au Canada, cet ensemble de données varié est essentiel pour évaluer la légitimité d'une identité.

« Les plus grands signaux d'alarme sont souvent les éléments manquants. Un véritable consommateur a une histoire qui n'est pas seulement financière... Nous accumulons cette sorte de "poussière numérique" dans la vie de tous les jours. »

Chris Jepsen,

Directeur de la gestion des produits liés à l'identité et à la conformité à Equifax Canada



Lutter contre la menace : le pointage d'identité synthétique

Pour remédier à ce problème, les organisations ont besoin d'un mécanisme de défense à plusieurs niveaux qui comprend des processus de connaissance du client rigoureux et des techniques de modélisation avancées. Le [pointage d'identité synthétique](#) d'Equifax Canada est une solution puissante et ciblée spécialement conçue pour aider à mettre un terme au cycle de la fraude d'identité synthétique avant qu'elle n'ait d'incidence sur les résultats financiers d'une organisation.

Le pointage d'identité synthétique est un modèle en temps réel qui analyse la structure fondamentale et la rapidité de création d'un dossier de crédit, plutôt que d'évaluer la propension à rembourser du client. Il exploite des algorithmes avancés d'apprentissage automatique pour mettre au jour des schémas comportementaux suspects. Le pointage ne nécessite aucune intégration de nouvelles sources de données externes, car il tire parti des données historiques profondes et sur le comportement déjà incluses dans l'ensemble de données solide d'Equifax.

Optimisée par les données sur le comportement lié au crédit d'Equifax et entraînée sur les données du consortium Échange FraudeQ^{IMC}, cette solution d'Equifax axée sur l'IA génère un pointage entre 1 et 999 pour indiquer la probabilité qu'une identité soit synthétique. Un pointage plus élevé indique directement un risque plus élevé que l'identité ait été fabriquée.

Communiqué dans le segment consacré aux pointages du dossier de crédit du consommateur, le pointage d'identité synthétique peut être utilisé lors du processus de création de compte pour cerner les demandes risquées. Les prêteurs peuvent s'appuyer sur leurs propres processus décisionnels pour introduire des obstacles dynamiques dans le processus de demande : ils pourront ainsi accélérer le traitement des demandes hautement fiables, tout en soumettant les demandes suspectes à un examen manuel secondaire.

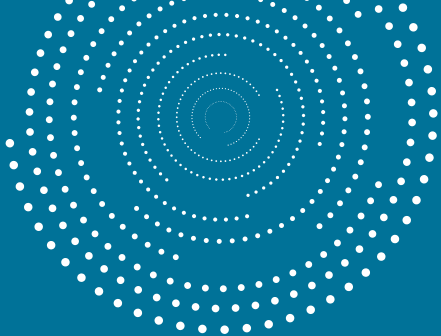
L'un des avantages de cette approche réside dans le recours aux renseignements collectifs du consortium. Le modèle du pointage d'identité synthétique est entraîné à l'aide de cas d'identité synthétique étiquetés provenant de l'[Échange FraudeQ^{IMC}](#), le plus grand consortium dédié aux fraudes confirmées au Canada. Ses données intersectorielles permettent de reconstituer le tableau complet du comportement d'un client dans l'ensemble du secteur financier et, ainsi, de repérer les profils susceptibles d'être synthétiques.

Les aperçus tirés des données montrent que le pointage d'identité synthétique a le potentiel d'avoir une incidence significative. Selon une analyse, les 10 % des pointages les plus risqués regroupaient 30 % des identités qui sont par la suite devenues défaillantes⁵.

Equifax offre également la possibilité d'ajouter ce pointage aux portefeuilles existants, ce qui permettra aux organisations d'analyser leurs bases de données actives afin de détecter toute exposition aux identités synthétiques cachée qui aurait pu passer inaperçue lors du processus d'intégration*.

* L'accessibilité du fonctionnement par lots est prévue plus tard en 2026. La feuille de route peut faire l'objet de modifications.





Avantages du pointage d'identité synthétique

- ✓ **Il s'adapte aux seuils de risque définis par votre organisation** pour permettre une détection et un contrôle précis des taux de vérification, selon votre propension au risque.
- ✓ **Il permet de détecter avec précision** les identités synthétiques en reconnaissant les schémas comportementaux subtils qui présentent un risque élevé.
- ✓ **Il permet la détection précoce des identités présumées synthétiques** afin de prévenir la fraude et de réduire le risque d'exposition à l'avenir.
- ✓ **Il tire parti d'aperçus** pour élaborer des stratégies de lutte contre la fraude fondées sur les données, notamment des flux de travail d'enquête ciblés.

Passer du mode réactif au mode proactif

La fraude d'identité synthétique est un phénomène complexe et dévastateur qui connaît une croissance alarmante. À mesure que les réseaux de fraude organisée continuent d'exploiter des techniques sophistiquées pour créer des profils « idéaux », les processus d'intégration traditionnels risquent de ne plus suffire.

En se concentrant sur les différences de comportement subtiles entre les consommateurs réels et les identités fabriquées, ainsi qu'en exploitant la puissance des renseignements du consortium et les capacités avancées de l'IA, les prêteurs peuvent contribuer à inverser la tendance. Le pointage d'identité synthétique fournit des aperçus prédictifs en temps réel pour vous aider à démasquer ces menaces invisibles. Protéger son entreprise signifie passer d'une approche réactive à une approche proactive, sécuriser les canaux de conversion de clients et, enfin, garantir que les décisions en matière de crédit soient prises avec une plus grande certitude quant à l'authenticité de la personne à l'autre bout.





Communiquez avec un membre de l'équipe de conseil en matière de fraude d'Equifax pour découvrir comment vous pouvez mettre au jour les fraudes d'identité synthétique qui figurent actuellement comme des créances irrécouvrables dans votre portefeuille actif.

Cherolle Prince

Directrice, conseils en matière de fraude
cherolle.prince@equifax.com

Hussein Ezzat

Conseiller principal en matière de fraude (région du Grand Toronto)
hussein.ezzat@equifax.com

Julie Lesco

Conseillère en matière de fraude et en gestion de l'identité
julie.lesco@equifax.com

Sophia Rodopoulos

Conseillère en matière de fraude (région du Grand Toronto)
s.rodopoulos@equifax.com

Patrick Wiltshire

Conseiller en matière de fraude liée aux paiements (Montréal)
patrick.wiltshire@equifax.com



À propos d'Equifax

À Equifax (NYSE : EFX), nous croyons que les connaissances entraînent le progrès. En tant qu'entreprise mondiale de données, d'analyses et de technologies, nous jouons un rôle essentiel dans l'économie mondiale en aidant les institutions financières, les entreprises, les employeurs et les organismes gouvernementaux à prendre des décisions cruciales avec une confiance accrue. Notre combinaison unique de données différenciées, d'analyses et de technologies infonuagiques

alimente des aperçus qui permettent aux gens de prendre des décisions qui les feront aller de l'avant. Ayant son siège social à Atlanta et soutenue par près de 15 000 employés dans le monde entier, Equifax exploite des activités ou possède des investissements dans 24 pays en Amérique du Nord, en Amérique centrale, en Amérique du Sud, en Europe et dans la région de l'Asie-Pacifique. Pour en savoir plus, visitez le site [Equifax.ca](https://www.equifax.ca).

1 Tendances en matière de fraude Poulos du marché d'Equifax Canada du S1 2025. Octobre 2025.

2 Equifax. *The Stark Reality of Synthetic ID Fraud*. https://assets.equifax.com/marketing/US/assets/syntheticID-fraud_wp.pdf

3 *Protect Yourself From Synthetic Identity Theft*. Discover <https://www.discover.com/credit-cards/card-smarts/what-is-synthetic-identity-theft/>. Consulté le 13 mars 2026.

4 Themis. (2025). Tendances en matière de fraude de 2025. Themis.

5 Données d'Equifax de 2026. Les profils défaillants sont ceux qui ont accusé un retard de paiement de 90 jours et plus au cours des 12 mois suivants.