White Paper

Unmasking the Invisible Threat: Spotting Synthetic Identity Fraud

Synthetic identity fraud is emerging as a serious threat in the Canadian financial ecosystem. This is a highly sophisticated financial crime where bad actors blend real and fictitious personal information to construct a new fake identity. Fraudsters nurture these profiles over months or even years until they achieve a good credit score, then max out credit limits and vanish — leaving lenders to absorb the financial losses.

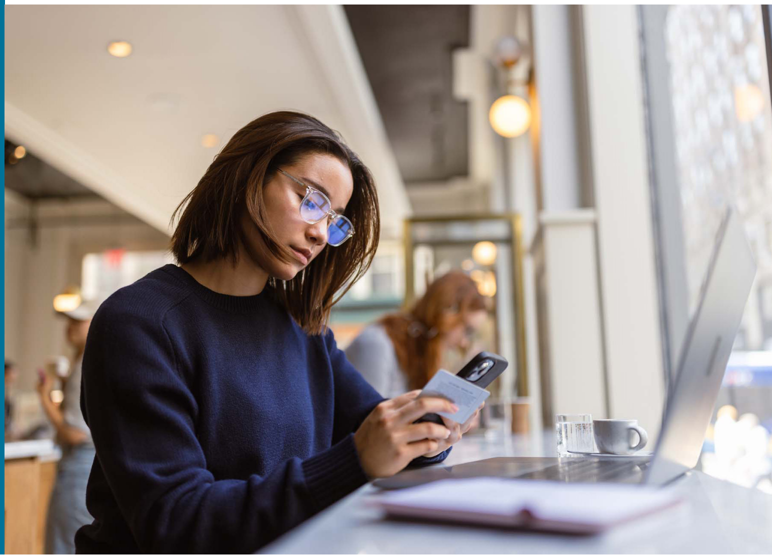
The scale of this problem is significant. In Canada, synthetic identity fraud doubled as a proportion of all fraudulent applications between 2022 and 2024[1]. Market data from the U.S. illustrates that synthetic identity fraud is responsible for up to 20 per cent of credit losses[2] and accounts for 80 to 85 per cent of all identity fraud[3].

The true scope of the problem is obscured because synthetic fraud losses are often miscategorized as bad debt; with no genuine identity behind the debt, businesses waste more resources chasing a non-existent customer. This can lead to lenders mandating tighter credit policies, while failing to address the root cause behind the loss. To effectively fight back, lenders must build on their existing verification methods.

“Bad actors use stolen identities and PII data to create anarchy in the Canadian financial ecosystem. This is why synthetic identity fraud prevention requires a shift in strategy. We must stop asking ‘Is this client creditworthy?’ or ‘Is this signature authentic?’ and start asking ‘**Does this person actually exist?**’”, says **Cherolle Prince, Director of Fraud Consulting, Equifax Canada**.

“Bad actors use stolen identities and PII data to create anarchy in the Canadian financial ecosystem. This is why synthetic identity fraud prevention requires a shift in strategy. We must stop asking ‘Is this client creditworthy?’ or ‘Is this signature authentic?’ and start asking ‘**Does this person actually exist?**’”

Cherolle Prince,
Director of Fraud Consulting, Equifax Canada



The Anatomy of a Synthetic Identity: Understanding the Long Con

Unlike traditional identity theft where a criminal takes over an existing, legitimate account, synthetic fraud takes a longer approach. The process unfolds in a deliberate, multi-stage cycle that begins with data harvesting. Fraudsters collect consumer PII from large-scale data breaches, purchase it on the dark web, or scam vulnerable consumers into handing over their personal data.

"A synthetic identity is an identity — a 'person' — that doesn't exist," says **Chris Jepsen, Director, Product Management - Identity and Compliance at Equifax Canada**. "Fraudsters might create a synthetic identity out of a combination of real and fake elements, such as a real person's name coupled with an illegitimate Social Insurance Number constructed to pass cursory checks."

The highly calculated, multi-stage con unfolds over months or years:

The Opening
Month 1

Fraudster applies for an entry-level credit product, like a secured or low-limit credit card. The goal isn't immediate money; it's establishing a footprint.

The Build-Up
Months 2–6

The identity behaves like an ideal customer, paying off the balance every month.

The Upgrade
Months 6–12

As risk models begin to recognize the identity as a reliable borrower, credit restrictions relax, such as increasing credit limits or upgrading to an unsecured card.

The Credit Climb
Months 12–24

With a solid history, the identity's credit score climbs into prime territory. The fraudster obtains personal loans or auto financing with significant cash value.

Once they reach a prime credit score, that's when the **bust-out fraud** occurs. The fraudster takes out the personal loans, maxes out the credit cards, secures the auto financing, and disappears with the assets. Creditors try to recover their money, but can't because that person never existed.

The Invisible Threat:
Falling into the Perfect Profile Trap

The challenge for financial institutions is detecting these fabricated users *before* the bust-out occurs. These identities won't necessarily trigger traditional alarm bells during the first interaction. And because there is no real victim whose existing credit is being ruined, no one is calling the bank to report fraudulent activity.

The creditworthiness of profiles crafted by fraudsters are designed to look flawless, but that only tells one part of the story. A genuine consumer's credit acquisitions are inconsistent, driven by real-life events and unexpected financial needs. Building a good credit score happens over a longer duration. Conversely, a synthetic profile takes on specific credit products in quick succession, chosen for their maximum positive impact on a credit score. Both profiles may have the same credit score, but the underlying behaviours tell different stories.

Traditional onboarding systems may miss these clues, leaving 95 per cent of synthetic identities undetected during the onboarding process[4]. "Synthetic identities are typically nurtured over 18–24 months to mimic ideal consumer behaviour, making them difficult to detect," explains Prince. "Current identification methods can be costly, cumbersome, and applied too late in the acquisition journey."

Technology as a Threat Multiplier

The threat of synthetic identity fraud is compounded by the rapid advancement of modern technology. Technology acts as a speed multiplier, lowering the barrier to entry so even inexperienced financial criminals can perpetrate fraud.

The velocity at which these attacks can be executed and synthetic data can be tested has increased. Fraudsters can generate robust, high-quality identities with less effort. Countering these attacks requires organizations to use advanced machine learning and AI in their own defence strategies.

Looking Beyond Tradelines:
The Importance of "Digital Dust"

If traditional credit files and static data points are no longer sufficient to determine if a person is real, organizations must look elsewhere. The key lies in shifting away from verifying static data, and moving toward assessing an applicant's past interactions and non-financial footprint. Using additional signals like these can help predict the likelihood of fraud risk.

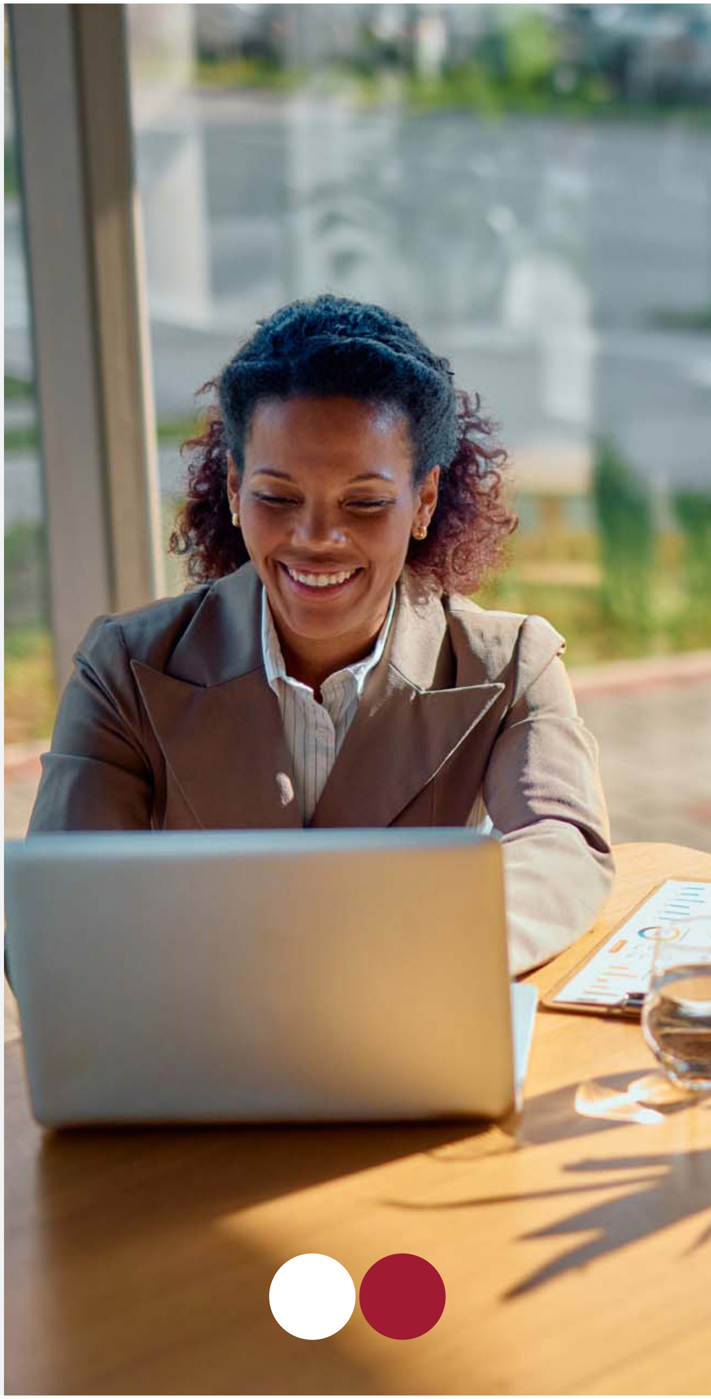
While fraudsters can nurture a financial profile, it is exceptionally difficult to fabricate a multi-layered digital life. The digital ecosystem provides a wealth of alternative data that can expose synthetic profiles.

This data includes everyday elements like utility bills, rent payments, recurring subscriptions, device data, and online e-commerce or ride sharing transactions. A synthetic identity lacks this rich, chaotic digital footprint because it is not operating in the real world.

Incorporating alternative, non-financial data sources provides a more accurate picture of an identity's true nature, exposing the gaps that fraudsters can't easily fill. Paired with behavioural data, the complete picture becomes clearer. This is where the robust Equifax data set plays a crucial role; with the largest consumer and commercial databases in Canada, this diverse data set is key when it comes to assessing the legitimacy of an identity.

> "The biggest red flag is often what isn't there.
> A genuine consumer has a history that isn't just financial…
> We accumulate that sort of 'digital dust' in the course of everyday life."

Chris Jepsen,
Director, Product Management - Identity and Compliance,
Equifax Canada



Combating the Threat:
Synthetic Identity Score

To tackle this problem, organizations require a layered defence mechanism that includes solid KYC processes and advanced modelling. Synthetic Identity Score from Equifax Canada is a powerful, targeted solution designed specifically to help halt the synthetic fraud lifecycle before it can impact an organization's bottom line.

Synthetic Identity Score is a real-time model that analyzes the fundamental structure and velocity of a credit file's creation, rather than evaluating its repayment propensity. It leverages advanced machine-learning algorithms to discover suspicious behaviour patterns. The score requires no integration of new external data sources, as it leverages the deep historical and behavioural data already present in the robust Equifax data set.

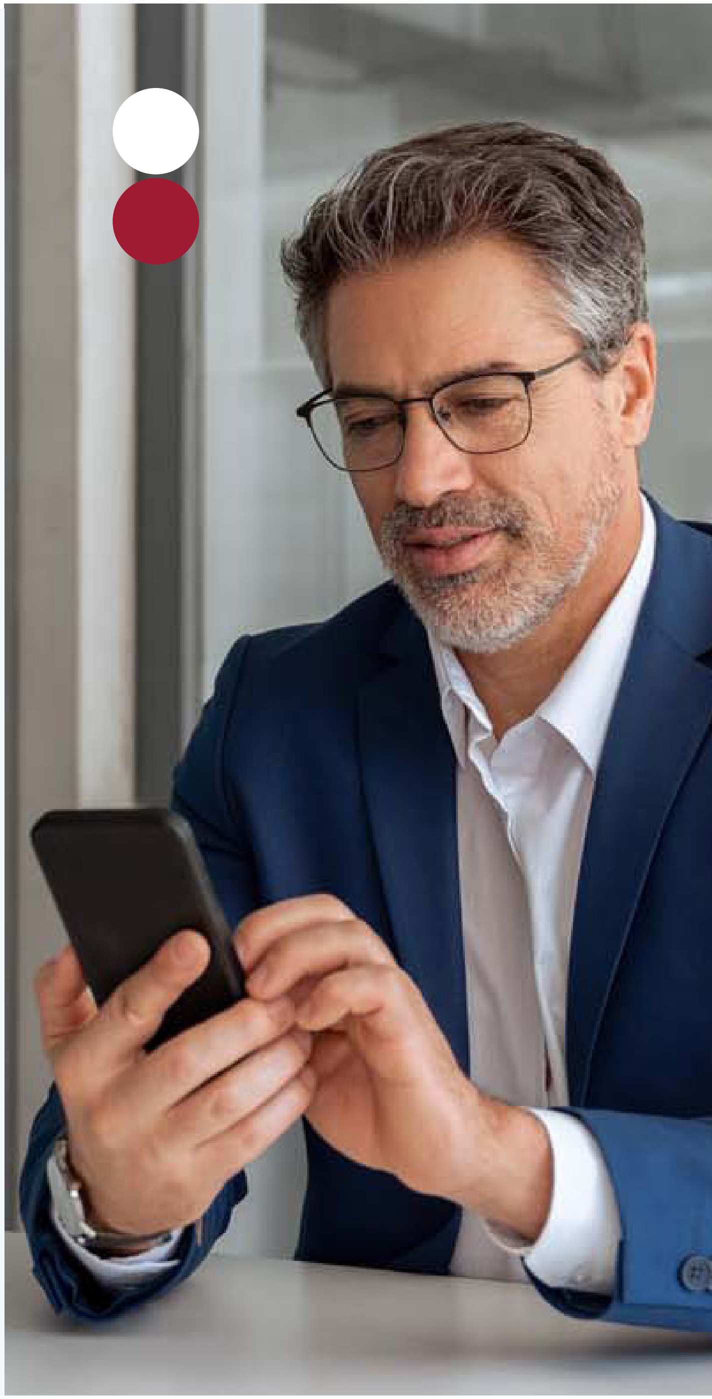
Powered by Equifax credit behavioural data and trained on FraudIQ™ Exchange consortium data, this AI-powered solution from Equifax provides a score ranging from 1 to 999 indicating the likelihood that an identity is synthetic. A higher score directly indicates a higher risk that the identity has been fabricated.

Delivered on the scores segment of the consumer credit file, Synthetic Identity Score can be used during account origination to identify risky applications. Lenders can use their own decision-making processes to add dynamic friction to the application process — fast-tracking high-confidence identities while sending suspicious applications for a secondary manual review.

One of the advantages of this approach is its use of shared consortium intelligence. The Synthetic Identity Score model is trained using labelled synthetic cases from the FraudIQ™ Exchange, the largest known fraud consortium in Canada. Its cross-industry data helps piece together the full puzzle of a customer's behaviour across the financial sector, helping to identify profiles that might be synthetic.

Data insights show the Synthetic Identity Score has the potential to make a meaningful impact. In one analysis, the riskiest 10 per cent of scores contained 30 per cent of identities that later became delinquent[5].

Equifax also offers the capability to append the score to existing portfolios, allowing organizations to scrub their active databases to uncover hidden synthetic exposure that may have slipped through during onboarding*.



* Batch functionality scheduled to be available later in 2026. Roadmap subject to change.

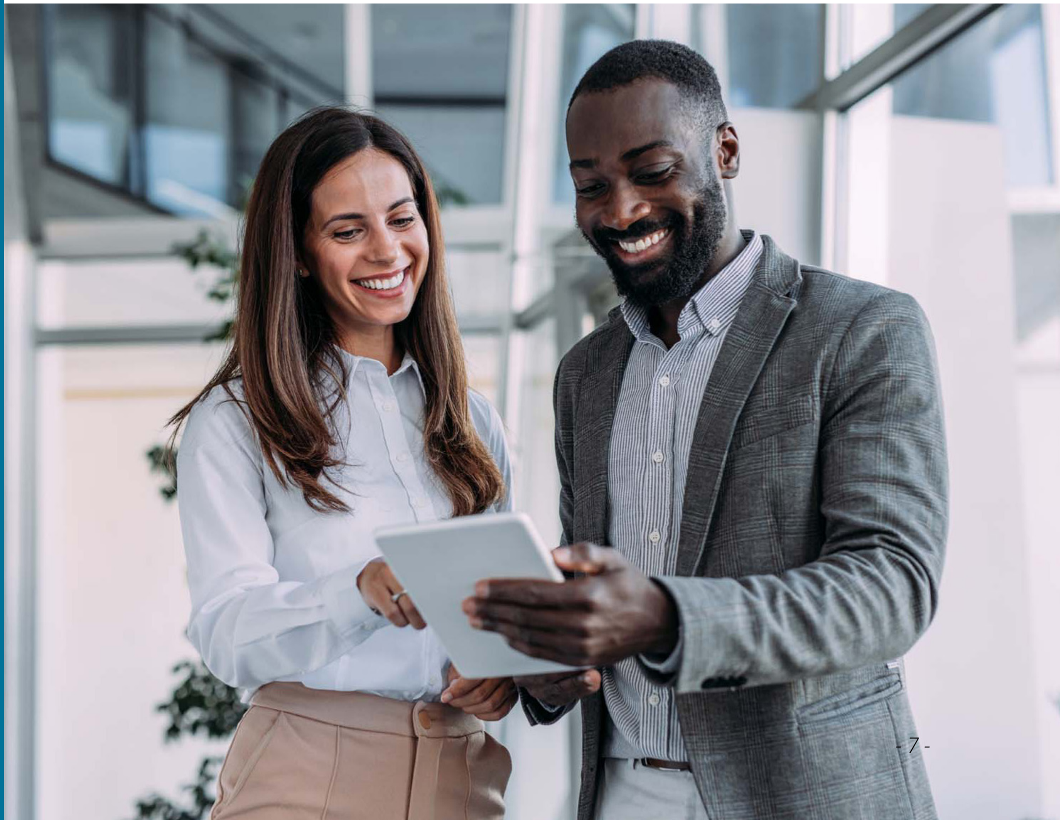
Benefits of Synthetic Identity Score

- **Works with your organization's own defined risk thresholds** to enable precise detection and control of review rates to align with your risk appetite
- **Helps accurately detect** synthetic identities by recognizing subtle, high-risk behavioural patterns
- **Enables early detection of suspected synthetic identities** to prevent fraud and reduce future exposure
- **Leverages insights** to develop data-driven fraud strategies, including targeted investigative workflows

Moving from Reactive to Proactive

Synthetic identity fraud is complex, devastating, and growing at an alarming rate. As organized fraud rings continue to harness sophisticated techniques to nurture "perfect" profiles, traditional onboarding processes may not be sufficient.

By focusing on the subtle behavioural differences between genuine consumers and fabricated personas — and by leveraging the power of consortium intelligence and advanced AI capabilities — lenders can help turn the tide. Synthetic Identity Score provides real-time, predictive insights to help unmask these invisible threats. Protecting your organization means shifting from reactive to proactive, safeguarding acquisition channels, and ultimately ensuring that credit decisions are made with greater confidence that the person on the other end is real.



Contact an Equifax Fraud Consulting Team member to learn how you can uncover synthetic identity fraud currently sitting as bad debt in your active book.

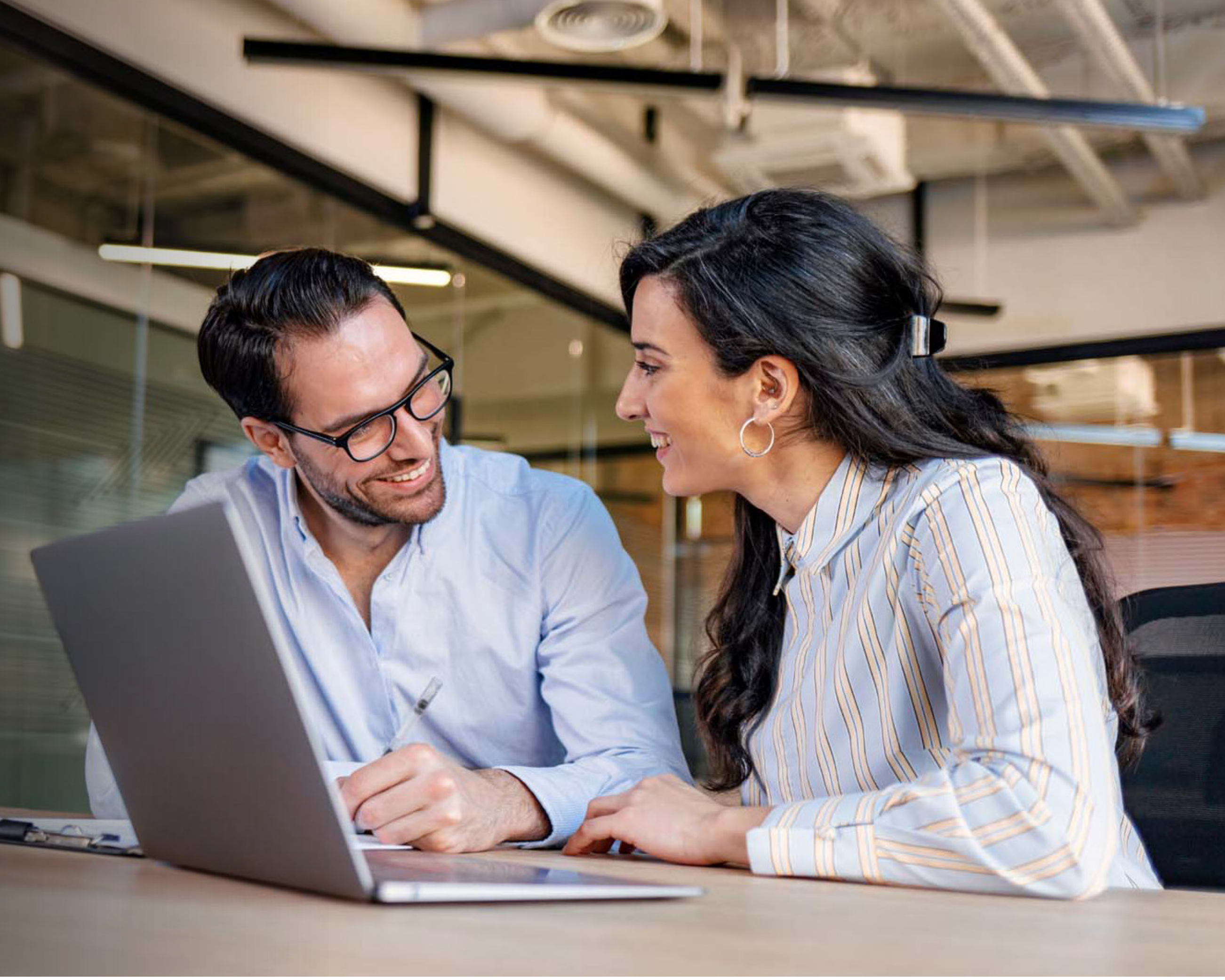
Cherolle Prince
Director, Fraud Consulting
cherolle.prince@equifax.com

Hussein Ezzat
Senior Fraud Consultant (Greater Toronto Area)
hussein.ezzat@equifax.com

Julie Lesco
Fraud and Identity Management Consultant
julie.lesco@equifax.com

Sophia Rodopoulos
Fraud Consultant (Greater Toronto Area)
s.rodopoulos@equifax.com

Patrick Wiltshire
Fraud Consultant – Payments (Montreal)
patrick.wiltshire@equifax.com



About Equifax

At Equifax (NYSE: EFX), we believe knowledge drives progress. As a global data, analytics, and technology company, we play an essential role in the global economy by helping financial institutions, companies, employers, and government agencies make critical decisions with greater confidence. Our unique blend of differentiated data, analytics, and cloud technology drives insights to power decisions to move people forward.

Headquartered in Atlanta and supported by nearly 15,000 employees worldwide, Equifax operates or has investments in 24 countries in North America, Central and South America, Europe, and the Asia Pacific region. For more information, visit Equifax.ca.

1 H1 2025 Equifax Canada Market Pulse Fraud Trends. October 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/. Accessed March 13, 2026.
4 Themis. (2025). 2025 Fraud Trends. Themis.
5 Equifax data 2026. Delinquency defined by profiles which became 90+ days past due in the following 12 month period.