2025 FCT Fraud Insights Report

Table of contents

3

Introduction

- The purpose of this report
- Meet the experts

5

Key Trends

- The top fraud trends in 2025
- How market pressures and technology can enable fraud
- Industries are pushing back on fraud

8

Preventing Fraud

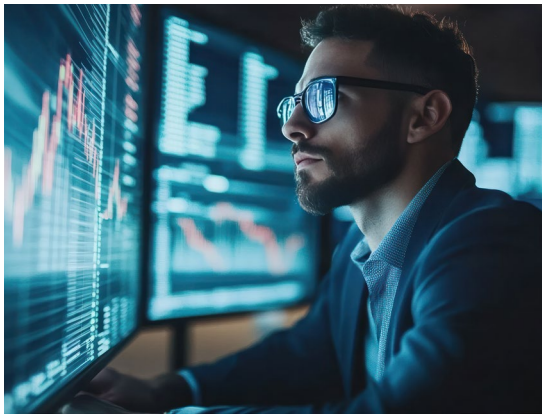
- Be on the lookout for fraud flags
- Collaboration and industry leadership

10

Looking Ahead

- Potential future fraud and prevention trends

Introduction



Understanding the evolving landscape of fraud

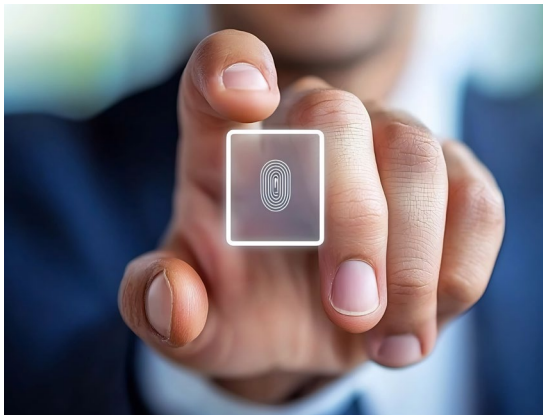
Fraud continues to be a growing concern in the real estate and financial services industry, with new schemes emerging as technology advances.

As fraudsters become more sophisticated, businesses and other organizations must stay ahead by leveraging data-driven insights, innovative prevention strategies and collaborative industry efforts.

The purpose of this report

The Fraud Insights Report provides a deeper look into current fraud trends, emerging threats and actionable mitigation strategies. New fraud data, industry research and insights from fraud prevention experts will help equip professionals with the knowledge needed to help protect their organizations and customers.

It's designed for professionals in financial services, risk management, compliance and fraud prevention, as well as business leaders seeking to enhance their fraud detection capabilities. Whether you're an industry veteran or new to fraud prevention, the insights in this report will help you stay up-to-date on the latest trends, tools and techniques in fraud, as well as where future threats may be headed.



Key areas of focus

- **Emerging fraud trends** –Analysis of new and evolving fraud tactics, and the technologies behind them.
- **Industry response** – How organizations are developing innovative strategies to prevent sophisticated fraud attempts.
- **Mitigation strategies** – Best practices and advanced solutions for fraud prevention and risk management.

Introduction
Meet the experts

"We often observe a direct correlation between a **declining market and increased financial desperation**, leading some individuals to take drastic measures."

Daniela DeTommaso

President

Daniela DeTommaso is the president of FCT, the leading title insurance company in Canada.

She's responsible for overseeing all lines of business, with a network of over 1,000 employees.

Daniela has been with FCT for over 25 years, and is focused on building long-term partnerships with her customers by ensuring that they are at the center of every FCT transaction.

"The more layers you can get into your fraud detection, the **harder it is for fraudsters to make it through all** of them."

Marie Taylor

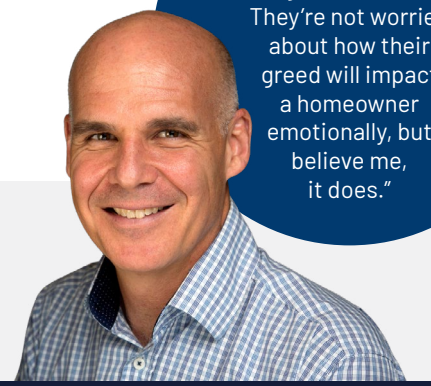
Director, National Underwriting

Marie Taylor has been a valued member of FCT's legal team for over twenty years.

She is a sought-after subject matter expert specializing in residential title insurance and the effects of fraud on the title insurance industry in Canada.

She has travelled across the country as a keynote speaker on title fraud educating real estate professionals so that they can more readily spot red flags and suspicious indicators on real estate transactions.

Marie is a member of the Association of Certified Fraud Examiners which is the largest anti-fraud organization in the world and is a past member of FRSA's Technical Advisory Committee for Mortgage Brokering.



"**Fraudsters are organized and they're innovative.** They're not worried about how their greed will impact a homeowner emotionally, but believe me, it does."

John Tracy

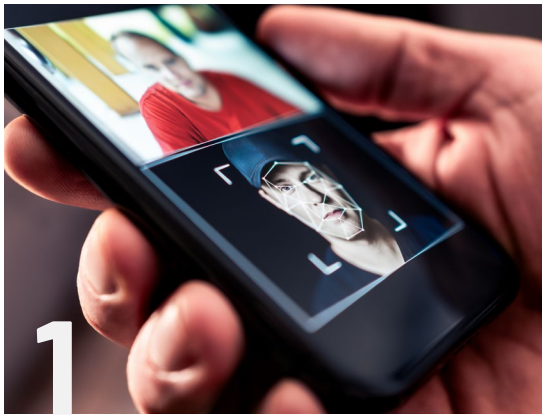
Senior Legal Counsel, Claims

John Tracy is the senior legal counsel for FCT, where he's responsible for handling title insurance claims, with a keen focus on fraud.

John was called to the Ontario Bar in 1993 after attending McGill and Queen's Universities, and has been with FCT since 2004.

He's a leader of FCT's fraud prevention efforts, and a sought-after seminar speaker on the topic.

The top fraud trends in 2025



AI is transforming impersonation and fraud

Remote transactions have always posed risk for fraud, but the threat has completely transformed thanks to new AI-powered tools that fraudsters can use to effectively impersonate their target.

Professionals need to be wary, even in these communications:

- Phone calls: AI text-to-speech tools and real-time voice modulation let fraudsters change their apparent age, gender and accent to better match their story, and spoofing tools can make the call appear to come from the phone number of a fraudster's choosing.
- Virtual meetings: deepfake technology was previously limited to pre-rendered impersonation of people who appear in large amounts of video footage, such as politicians and celebrities. It has improved to the point where it can replace a fraudster's face with a homeowner's, on camera, in real time.

In-person fraud is on the rise

Before AI, the reason remote transactions were seen as risky was distance—a fraudster on a video call could hold up a stolen piece of ID where they bore a resemblance to the real owner, or even stick their own photo to the card.

If a transaction could be completed in office with physical ID documents, then the deception would be more likely to fall apart.

But with fraudsters' access to more advanced editing software and printing hardware, professionals are face-to-face with a new reality: the person sitting across the desk with an intact and legitimate-looking ID showing their photo can be an imposter.

Fake ID documents have gotten sophisticated enough that in-person no longer means fraud free.

ID theft is just the start

Fraudsters can use small pieces of compromised information about their target to leverage more of that person's information from financial institutions, businesses or government services, until they have enough to impersonate them.

Fraudsters can also make themselves harder to detect by generating synthetic IDs: using a single piece of compromised ID, like a target's Social Insurance Number (SIN), and adding fabricated personal information.

They can then use this false persona to apply for small loans and other instruments that, over time, make that identity take on legitimacy, and even a credit history.

Emerging fraud risks in the real estate market

Economic conditions in 2025 carry a higher risk generally because of the effects of economic uncertainty and downturn: more people feel pressure or even desperation, and look to secure money any way they can, with fraud seen as a safer alternative to violent crime.

Those same pressures can benefit criminal organizations, who use so-called "straw buyers" with clean records in order to better insulate themselves.

Email hacking to carry out wire transfer fraud

One particular way fraudsters are leveraging compromised information is gaining access to organizations' internal systems, especially email accounts.

This lets them monitor activity and wait for the right opportunity.

When the hacked account sends payment instructions to their client, the fraudster is able to send a faked version of that email instead and redirect the funds.

Key trends

Industries are pushing back on fraud

Evolving practices and education

More organizations are adopting best practices in identity verification, including stringent ID verification, and Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures. Multi-factor authentication (MFA) adds an important layer of security to digital transactions. Biometric verification factors like fingerprint and face recognition are gaining traction in the financial sector, where they're helping make banking apps more secure, for instance.

Industry leaders are also investing in the human factor through education on how to better spot phishing (as well as smshing, spear phishing and other related attempts), social engineering tactics as well as the flags on transactions that can indicate fraud. FCT is a leader in educating professionals as well as the public on the dangers and signs of fraud, and how to avoid falling prey.

Increased risk in refinance transactions

2025 is set to be the start of a significant surge in refinances as high mortgage volumes from 2021 come up for renewal.

Even if the percentage of fraudulent transactions stays the same, the volume will increase along with legitimate transactions.

Professionals and organizations involved in refinancing should be on the lookout even during these routine-seeming transactions: a fraudster can make an equity withdrawal as part of the refinance and walk away with the proceeds.

Preventing fraud

Be on the lookout for fraud flags

Each instance of fraud is different, but there are recurring common factors. Any one of them on their own doesn't mean that a transaction is fraudulent, but professionals seeing several of these "fraud flags" should take extra caution:

- Credit history that isn't consistent with the person's age
- The person currently resides at the property they're purchasing
- The person can't meet in person and/or isn't willing to verify their ID documents
- Requests to direct funds to an unrelated third party
- Work addresses that are difficult to verify, or go to a post office box
- There are significant variations in handwriting between documents
- Funds are being transferred outside Canada
- The transaction is being put through as a rush, especially at end-of-month
- The property in a mortgage transaction already has a mostly-paid mortgage on title
- A real estate transaction that is an equity withdrawal from a recently purchased, mortgage-free property

Preventing fraud

Collaboration and industry leadership

Partnership will play a key role in preventing fraud

Fraudsters continue to develop more diverse and sophisticated methods of deception. In response, industry leaders are building partnerships that drive the search for new and innovative ways to prevent fraud.

Sharing expertise and different approaches to protecting transactions through technology has led to the development of robust, sophisticated ID verification systems. These solutions combine tools like face-matching technology, AI-powered risk analysis and biometric security to provide professionals and consumers a broader, more sophisticated defense against ID theft and fraud.

Ensuring safer, smoother transactions through industry collaboration

Industry partnerships can create an ecosystem of connected solutions that all work together to ensure legal and real estate professionals can have confidence that their clients are who they say they are, and that each transaction meets stringent FINTRAC, KYC and AML client identification standards.

Looking ahead

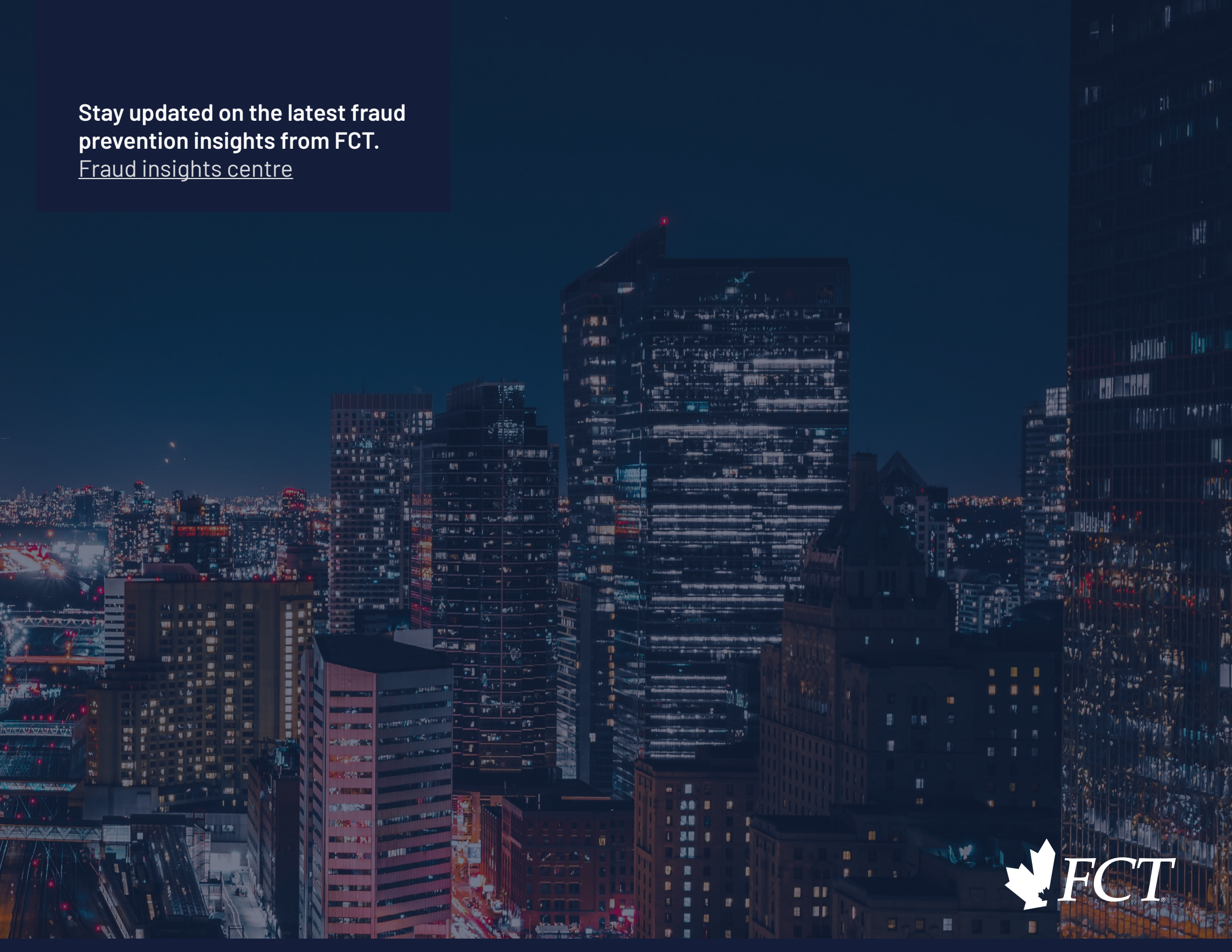
Potential future fraud and prevention trends

As awareness of new fraud threats spreads, more provincial regulators and law societies may introduce KYC and ID verification requirements, even for in-person transactions.

We may see the first instance of mortgage title fraud carried out by a non-human actor: the AI tools used by fraudsters can be combined and managed by a single algorithm with its directive shaped by the fraudster, and then deployed for "hands-off" execution.

Financial institutions will likely invest in developing AI-powered defenses against AI-powered fraud and cyberattacks, as the threat grows. As the tactics and counter-tactics of fraud start to leave human hands, the direction they take would become increasingly difficult to predict.

Fraudsters have found success with email account hacking and phishing, but as they ramp up their efforts, we may see a greater number of small-scale attacks intended to avoid media attention and industry scrutiny.


Stay updated on the latest fraud prevention insights from FCT.
Fraud insights centre
FCT