

2026

FCT Cybersecurity
Resource Guide



Contents

Introduction

1

Decoding Cybersecurity:
Key Terms and Concepts
to Know

4

A Conversation with Cory
Woods on Cybersecurity

7

Fraudsters Vocabulary:
The Essential Cyberfraud
Terms and Tactics

10



A Conversation with
John Tracy on
Cyberfraud

13

The Big Claim:
\$Multi Million Learnings

17

Other Fraud
Claim stories

19

Preparing for Tomorrow:
Understanding Future
Risks and Evolving Threats

22

A Conversation with
our expert from the field
Matt Cunningham

24



How FCT Can Be Your
Partner for Secure Real
Estate Transactions

30

Conclusion

32

Introduction

Cybersecurity has become a defining challenge of our digital age—one that demands not only technical solutions, but industry-wide awareness, accountability, and action. At FCT, we recognize that every transaction represents more than data; it represents people, trust, and life-changing decisions. Protecting that trust is not just our responsibility – it's our commitment.

This guide offers a comprehensive view of the evolving landscape of cybersecurity threats within our industry. It begins by identifying and understanding the language of these risks—clarifying key cybersecurity and cyber-fraud terminology to empower informed vigilance. It then moves into real-world examples of claims and incidents, illustrating how threats manifest and how they can be intercepted moving forward. Finally, we look to the future, exploring emerging trends and showcasing how FCT is helping clients secure their transactions through proactive tools like Client ID Verification.

Cybersecurity is a shared responsibility. Through awareness, insight, and innovation, we can build a more resilient ecosystem—one where trust is not only earned, but actively protected.



Message From Our President

At FCT, protecting people is at the heart of everything we do. Behind every transaction are people like a family purchasing their first home, a trusted legal professional guiding a client, or a lending professional helping facilitate an important step in someone's financial journey. In today's digital world, this trust faces new challenges from increasingly sophisticated fraud tactics.

Cybersecurity is no longer just a technical issue—it's a human one. The emotional and financial impact of fraud is real, that's why awareness and vigilance is essential. By coming together as an industry, we can better recognize emerging threats, strengthen our defenses, and protect what truly matters: the people behind every deal. This guide brings forward insights, strategies and stories to help us do just that, ensuring that FCT continues to be a trusted partner in every transaction.



Cybersecurity doesn't just live in IT systems—it lives in culture. When people feel safe, trusted, and connected, they're more likely to speak up, spot risks, and stop threats before they spread.

Daniela DeTommaso, LL.B.
President

Spot It



Decoding Cybersecurity: Key Terms and Concepts to Know

FCT believes understanding the fundamentals of cybersecurity is key to protecting both people and transactions. In this section, we will explore essential terms like social engineering, phishing, multi-factor authentication, and cloud vulnerabilities. These concepts are all interconnected and are at the core of the cyber-threats which we face on a daily basis. For example, phishing is a social engineering tactic designed to trick people into giving up sensitive information, and cloud vulnerabilities can increase exposure if proper protections, such as multi-factor authentication, are not in place. By learning how these threats work together and how to defend against them, we can strengthen the digital safety of every professional and client we serve.

Cybersecurity 101

What is Social Engineering?

A form of cyber manipulation where attackers exploit human behaviour to gain access to sensitive information or systems. Rather than breaking through technical defenses, these schemes rely on psychological tactics to deceive individuals into taking harmful actions.

- Common techniques include phishing, impersonation, and urgent requests that bypass normal security protocols.
- Targets often include professionals handling financial transactions or confidential data.
- These attacks can lead to significant financial losses and are often excluded or limited under certain insurance parameters.



What is Phishing?

A deceptive tactic where cybercriminals impersonate trusted sources to trick individuals into sharing sensitive information or clicking malicious links, generally through email or SMS communications. These messages are designed to appear legitimate and are crafted to provoke quick responses before the recipient has time to analyze the contents more closely.

- May appear as emails from banks, clients, or colleagues requesting urgent action.
- Clicking links or downloading attachments can lead to credential theft or malware installation.
- Often used as an entry point for broader fraud schemes or system breaches.



What is Multi-Factor Authentication?

A security measure that requires users to verify their identity using more than one method of authentication. This generally means using something they know (personal information questions), something they have (another device or communication channel) or something they are (biometric information). This added layer makes it significantly harder for attackers to gain unauthorized access—even if a password is compromised.

- Typically combines something you know (password) with something you have (e.g., a mobile device or authentication app).
- Common forms include one-time codes sent via text, push notifications, or biometric verification.
- Strongly recommended for email, banking, and any system handling sensitive data.



What is Cloud Vulnerability?

A weakness or misconfiguration in cloud-based systems that can be exploited by cybercriminals to gain unauthorized access to data or services. These vulnerabilities often arise from poor access controls, unpatched software, or insecure third-party integrations.

- Can expose sensitive client information, including financial and personal data.
- Often targeted through credential theft, misconfigured storage, or insecure application programming integrations (APIs).
- Requires proactive monitoring, encryption, and strong identity management to mitigate risk.



A Conversation with Cory Woods on Cybersecurity



As cyber threats continue to evolve in complexity and scale, organizations across the real estate and financial services sectors face growing challenges in protecting sensitive information, maintaining trust, and securing high-value transactions.

To shed light on these issues, we spoke with **Cory Woods, Chief Information Security Officer (CISO) at FCT**. Drawing on years of experience in cybersecurity and risk management, Cory shares his perspective on the evolving threat landscape, emerging technologies, and the importance of maintaining trust in an increasingly digital world.

This conversation provides valuable insights for legal professionals, realtors, lenders, and anyone interested in understanding how cybersecurity continues to shape modern business.

■ From your perspective, what are the most pressing cybersecurity risks facing the real estate and title insurance industries today?

One of the most significant risks continues to be identity-based fraud.

Cyber criminals are becoming increasingly effective at impersonating trusted parties, whether through compromised accounts, fraudulent communications, or sophisticated social engineering techniques. In industries that rely heavily on trust, communication, and financial transactions, the ability to convincingly impersonate legitimate individuals creates significant risk.

The challenge is no longer simply protecting systems and information. Organizations must also consider how they validate the identity of those with whom they are conducting business.

■ Phishing and social engineering attacks are often the most common entry points for cyber criminals. What tactics are you seeing used most frequently in these areas and how are they evolving over time?

Phishing and social engineering remain highly effective because they target people rather than technology.

What is changing is the sophistication and scale of these attacks. Advances in artificial intelligence have made it easier for attackers to create highly convincing communications that appear authentic and relevant to the recipient. Cyber criminals are increasingly investing time in understanding their targets and personalizing their attacks. As technology continues to evolve, organizations and individuals must remain vigilant and treat unexpected requests, particularly those involving sensitive information or financial transactions, with appropriate caution.

■ How do the cyber threats faced by FCT differ from those faced in other industries, such as traditional financial institutions or other service providers?

At a high level, many organizations face similar cybersecurity challenges. The need to protect information, maintain operational resilience, and safeguard customer trust is universal.

Where industries differ is often in how criminal activity manifests itself. Attackers tend to focus on areas where significant value can be extracted and where trust-based interactions create opportunities for fraud. While the underlying threats may be similar, the specific business processes being targeted often vary between industries.

■ What do you identify as the most likely next wave of cyberattacks in this industry?

I believe we will continue to see rapid advancements in identity-based attacks, particularly those enabled by artificial intelligence.

The ability to generate convincing text, images, audio, and video content creates new opportunities for fraud and impersonation. Technologies that were once considered highly reliable for establishing trust may become increasingly difficult to rely upon in isolation. As a result, organizations will need to place greater emphasis on identity verification, trust frameworks, and layered security approaches designed to address emerging threats.

■ How do organizations equip employees and partners to recognize and resist these potential threats?

Technology alone cannot solve cybersecurity challenges.

Organizations must foster a culture in which cybersecurity awareness is viewed as a shared responsibility. Education, communication, and ongoing reinforcement remain critical components of any successful security program. The objective is not to make everyone a cybersecurity expert, but rather to help individuals recognize potential risks, ask the right questions, and know when to seek assistance.

■ You've spoken before about the importance of multi-factor authentication (MFA). How critical is it in protecting sensitive data?

Strong authentication remains one of the most effective measures available for reducing the risk of unauthorized access.

As cyber threats continue to evolve, organizations should adopt authentication approaches that provide an appropriate balance between security, usability, and the needs of their business. While no single control is foolproof, layered approaches to identity and access management remain essential components of modern cybersecurity programs.

■ What are some challenges organizations face when broadly adopting MFA?

One of the biggest challenges is balancing security with user experience.

Any security control must ultimately be accepted and used by the people it is intended to protect. Organizations that focus exclusively on security without considering usability often struggle with adoption.

The most successful implementations are those that combine strong security practices with clear communication, education, and a practical understanding of how people work.

■ As organizations continue to adopt cloud-based technologies, what cloud-related risks concern you most?

The pace of technological change continues to be one of the greatest challenges.

Cloud technologies provide organizations with significant benefits, but they also require continuous attention, governance, and risk management. As technology evolves, organizations must ensure they understand the implications of new capabilities, changing business requirements, and an increasingly interconnected digital ecosystem.

Maintaining visibility and understanding how information moves through an organization remain important considerations regardless of the technology platform involved.

■ Looking ahead, do you see authentication evolving into more advanced forms of identity verification?

Absolutely.

Authentication technologies will continue to evolve as both technology and threat actors advance. The future will likely involve a combination of techniques that improve both security and user experience while reducing reliance on traditional passwords.

More broadly, the conversation is already shifting from authentication toward identity assurance. Organizations increasingly need confidence not only that someone has authenticated successfully, but that they are genuinely who they claim to be.

■ If you could give one key piece of advice to legal professionals, realtors, and lenders about the current and future state of cybersecurity, what would it be?

The nature of trust is changing.

Historically, people relied on familiar signals to establish trust, whether that was an email address, a phone call, or even a face-to-face conversation. As technology continues to advance, many of those signals will become easier to imitate.

Organizations and individuals should place increasing focus on verification, validation, and healthy skepticism when dealing with sensitive information or financial transactions.

Cybersecurity is ultimately about trust. Those who adapt their processes and practices to maintain trust in a rapidly evolving digital environment will be best positioned for the future.

Fraudsters Vocabulary: The Essential Cyberfraud Terms and Tactics

Cyber-fraud is the next step in the chain of risk when cybersecurity measures fall short. Here, we will introduce terms like data breach, deepfakes, synthetic identity theft, digital title fraud, and wire fraud. These threats often build on one another: a compromised system with exposed data can be used to create deepfakes and synthetic identities, which fraudsters exploit to commit crimes such as digital title fraud and wire fraud. Understanding these risks and how they arise helps FCT and our partners stay vigilant and protect the people at the center of every transaction.

Cyber-Fraud 101

What is a Data Breach?

An incident where unauthorized individuals gain access to sensitive or confidential data, often resulting in exposure, theft, or misuse of personal or financial information. These breaches can occur through hacking, phishing, or system vulnerabilities.

- May involve client records, financial details, or login credentials.
- Can lead to reputational damage, legal consequences, and financial loss.
- Often preventable through strong access controls, encryption, and regular system audits.



What is Deepfake?

AI-generated media—such as video, audio, or images—that convincingly mimics real people, often used to deceive, impersonate, or manipulate victims. These synthetic creations can be weaponized in fraud schemes, especially when used to impersonate trusted individuals in high-stakes transactions.

- Can clone voices, facial expressions, and mannerisms with alarming accuracy.
- Often used in social engineering or impersonation scams to gain trust or authorize fraudulent actions.
- Presents growing risks in legal, financial, and real estate sectors where identity verification is critical.



What is Synthetic Identity Theft?

A sophisticated form of fraud where criminals create a new identity using a combination of real and fabricated personal information. These identities are often used to open accounts, apply for loans, or conduct fraudulent real estate transactions.

- May include real Social Insurance Numbers paired with fake names, addresses, or employment details.
- Difficult to detect because the identity doesn't belong to a single real person.
- Can result in long-term financial damage and legal complications for victims and institutions.



What is Digital Title Fraud?

A form of real estate fraud where criminals use stolen or synthetic identities to illegally transfer property ownership or access home equity—often facilitated through digital tools and communication channels. These schemes exploit gaps in identity verification and remote transaction processes.

- May involve forged documents, impersonated homeowners, or fraudulent mortgage applications.
- Increasingly executed through email scams, online platforms, and falsified digital credentials.
- Can result in significant financial loss and legal complications for property owners and professionals.



What is Wire Fraud?

A type of financial fraud where criminals impersonate legitimate parties—such as clients, lawyers, or lenders—to redirect closing funds into their own accounts. These schemes often rely on email spoofing and social engineering to manipulate trusted professionals during high-value transactions.

- Frequently targets real estate closings and trust fund transfers.
- Attackers may use fake email addresses or hacked accounts to send convincing payment instructions.
- Can result in substantial financial loss and reputational damage.



A Conversation with John Tracy on Cyberfraud



In today's increasingly digital real estate environment, fraudsters are becoming more sophisticated – leveraging everything from synthetic identities to email hacking to exploit vulnerabilities in property transactions. To better understand these emerging threats and how the industry can respond, we spoke with John Tracy, Senior Legal Counsel at FCT and a leading voice in fraud prevention. Drawing on his extensive experience investigating title insurance claims, John shares insights into the evolving cyber threat landscape, the role of technology, and the critical importance of human vigilance. This interview offers practical guidance for legal professionals, realtors, and clients alike as they navigate the complex realities of digital fraud in real estate.

■ How does the rise of deepfakes and synthetic identity theft affect the client ID verification process and what is being done to combat it?

Synthetic identity theft is a growing concern, though it's still relatively rare in our claims. I recall one case from years ago where a fabricated identity – someone who didn't exist – was used to successfully obtain a mortgage from a major bank. These schemes are long-term plays; fraudsters build up a credit profile over time to make the fake identity appear legitimate. Though, to be successful, a synthetic identity needs to include some connection to a real person, it's never entirely fictional. As for deepfakes, we haven't seen them surface in our claims yet, but they're on our radar. Phone calls and video meetings still play a key role in client identity verifications, and while tools like Zoom could potentially be exploited, we haven't encountered that scenario so far.

■ How have you seen the cyber threat landscape evolve over your time at FCT? Particularly in the last few years, what advancements have you seen that have led to the biggest impact on real estate and title fraud?

Over the years, the cyber threat landscape has become significantly more sophisticated, especially with the rise of near-pristine fake IDs and advanced email hacking techniques. One of the most impactful shifts has been the targeting of legal professionals – if a lawyer's email is compromised, fraudsters can redirect funds with alarming ease. These breaches often stem from simple vulnerabilities like reused passwords or the absence of multi-factor authentication. That said, gaining access to an email account doesn't guarantee success for fraudsters; the sheer volume of daily messages can sometimes work in our favor, burying malicious attempts in the noise. Still, the risks are real, and the consequences can be severe.

■ **Have more traditional fraud tactics been effectively replaced by new developments such as deepfakes and synthetic identity theft, or is there a balance between new and traditional techniques currently used by fraudsters?**

There's definitely still a balance.

The traditional fraud tactics – like forged documents or impersonation – continue to be effective, and we see them regularly. What's changed is that newer technologies like synthetic identities and deepfakes are now being used to enhance those older methods. Fraudsters aren't abandoning the basics; they're building on them, making schemes more convincing and harder to detect. It's a layered approach, and that's what makes it so challenging.

■ **Title fraud has been a known risk for many years, but how do you see digital title fraud emerging in the era of electronic records and online property systems?**

Digital systems have certainly changed the landscape, but they haven't necessarily made title fraud easier – just different. One emerging concern is the manipulation of corporate records online. Fraudsters can change the listed officers and directors of a corporation that owns property, then exploit that false authority to transfer or mortgage the land. While the move to electronic records brings efficiency, it also introduces new vulnerabilities. That said, committing fraud digitally isn't inherently simpler than doing it in person – it still requires a high level of planning and precision.

■ **Wire fraud has become one of the most damaging risks in real estate transactions. Where do you see the biggest vulnerabilities for lawyers, realtors and clients?**

In any real estate transaction, you're only as strong as the weakest link. Lawyers, in particular, face significant pressure – especially on busy closing days – where the sheer volume of tasks can lead to lapses in information security. If cybersecurity isn't built into every step of the process, that “busyness” can become a serious vulnerability. Fraudsters know how to exploit these moments, and even a small oversight can open the door to wire fraud with devastating consequences.

■ **What safeguards can be put in place to protect against fraudsters exploiting digital registries, resulting in a potential data breach?**

It really comes down to keeping information security front and center. While it may sound repetitive, the fundamentals still matter – using strong, unique passwords, changing them regularly, enabling multi-factor authentication, and being cautious about what personal information is shared online. Social media, in particular, can be a goldmine for fraudsters if people overshare. These basic practices are often overlooked, but they're critical in protecting access to digital registries and preventing breaches that could lead to serious fraud.

■ Could you walk us through an example of how synthetic identity theft and use of a deepfake might play out in a property transfer or mortgage application?

Synthetic identity fraud is a long-term scheme where fraudsters build a persona using real and fake details, gradually establishing credit to make it seem legitimate. In real estate, this often involves forging a homeowner's signature to transfer property ownership to the synthetic identity. Once "owned," the fraudster secures a mortgage and collects most of the funds. While more common in credit card fraud due to easier access, it does occur in real estate, though it's more complex and resource heavy. Notably, deepfakes aren't usually needed—just a convincing fake ID can bypass verification. A more prevalent tactic is identity theft, where the fraudster impersonates a real mortgage holder and drains equity through a mortgage.

■ What role can title insurers like FCT play in helping professionals mitigate these wire fraud risks?

Title insurers like FCT play a critical role in both prevention and protection. First and foremost, we focus on education – helping professionals understand how a cybersecurity breach can directly impact a real estate transaction. Our underwriters are trained to spot red flags and actively look for signs of wire fraud or identity theft during the process. And when something does go wrong, title insurance is there to help protect against financial loss, offering a safety net when the unexpected happens.

■ If a data breach occurs at a law firm or brokerage, what steps can be taken by FCT to help mitigate the impact and protect future transactions?

While FCT isn't in a position to provide IT services directly to a law firm or brokerage that's experienced a breach, we can still play a meaningful role. If the breach results in a covered claim, the affected clients will have the protection of their title insurance policies to help recover insured losses. Beyond that, FCT brings deep experience in handling these situations and can offer guidance on immediate steps to reduce or avoid further loss. Our goal is to support professionals through the aftermath and help safeguard future transactions.

■ What technologies currently show the most promise and benefit at being able to protect against instances of digital fraud?

There are some promising tools out there – products like Blulnk help prevent identity theft by verifying identities securely, and advanced email programs can flag suspicious domains or spoofed addresses before they cause harm. But no technology is foolproof. As we're reminded often, we all have to be human firewalls. That means staying vigilant, practicing good cybersecurity habits, and not relying solely on tech to protect us. The best defense is a combination of smart tools and smart people.

Stop It



The Big Claim: How a Fraudster Hijacked a \$Multi Million Mortgage Payout

It began as a high-value refinance transaction – routine in structure, but it quickly escalated into one of the most significant cases of fraud that FCT has ever covered. FCT had issued a title insurance policy to a major Canadian financial institution, insuring a ten-digit first mortgage. The transaction was expected to proceed smoothly, but instead, it became the target of a sophisticated case of identity and wire fraud.

The fraudster's first move was gaining access to the legitimate lawyer's email account – an act of phishing that opened the door to a layered deception. By exploiting the law firm and creating fake email addresses and impersonating the lawyer, the fraudster inserted themselves into the transaction, intercepting and manipulating communications between parties. Again, they didn't just impersonate, they filtered, intercepted, and doctored legitimate emails, and may have even successfully negotiated legitimate documents maintaining the illusion of authenticity throughout the communication process.

As the transaction progressed, the fraudster intercepted the real mortgage payout statement and wiring instructions, altered them, and sent the manipulated documents to the lender. Trusting the source, the lender forwarded the fraudulent payout instructions to FCT.



The result: A very significant multi-million mortgage payout was diverted to a financial account controlled by the fraudster. The mortgage remained undischarged. The insured was exposed. The fraud had succeeded.

This case underscores the evolving nature of cybercrime in real estate transactions. It wasn't just a breach – it was a full-fledged hack and impersonation, executed with precision and patience. The fraudster didn't rely on a single point of failure; they exploited multiple layers of trust, communication, and process – all hallmarks of sophisticated social engineering tactics.

This case serves as a powerful reminder that email verification alone is no longer enough. In high-value transactions, especially those involving mortgage payouts, multi-factor authentication and heightened scrutiny are essential. Questioning the source, the timing, and the context of every instruction isn't just cautious – it's critical.

This wasn't just another claim, it was a big claim and big learning – a defining example of how fraud can infiltrate even the most secure systems, and why vigilance must evolve alongside the threats we face.

What makes this case so striking is the sheer sophistication of the deception. The fraudster didn't just break into a system – they assumed an identity, controlled communications, and manipulated trust at every stage of the transaction. It's a wake-up call for the entire industry that cybercrime in real estate has reached a new level of precision and patience.

Robert Antenore, LL.B.
Vice President, Commercial Solutions



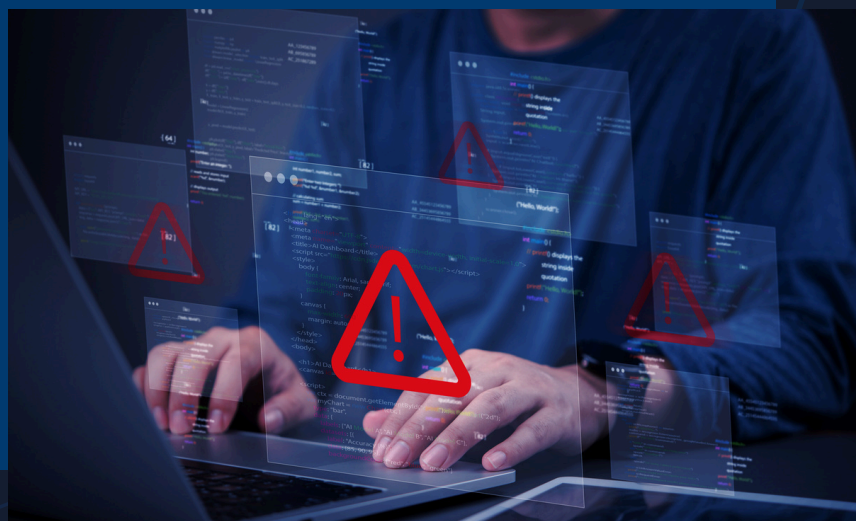
Claim: When a confirmation wasn't enough: A mortgage payout intercepted by fraud

What began as a seemingly ordinary transaction quickly took a turn that no one anticipated. A lender's lawyer sent updated wire instructions to the insured's lawyer, who, following best practices, confirmed the change by replying to the same email thread. But something was off. The lender never received the funds.

What unfolded next revealed a sophisticated cyberattack. The lender's email account had been compromised, and a fraudster had inserted themselves into the conversation. The wire instructions were fake, and the mortgage payout—meant to discharge the loan—was redirected to a fraudulent account. The mortgage remained undischarged, leaving the insured in a vulnerable position.

The investigation revealed not only the financial impact but also the limitations of traditional verification methods in the face of evolving cyber threats.

Had the email compromise been spotted earlier—or if a secondary channel had been used to confirm the change, this fraud might have been stopped before funds were lost. It's a powerful reminder that securing a transaction means more than just confirming details; it means questioning the context, the timing, and the source.



Claim: An email exposed. A commission lost.

A real estate transaction was nearing completion when the lawyer received a seemingly straightforward request: the agent wanted their commission sent via electronic funds transfer instead of a cheque. The request came from the agent's email address, and nothing appeared suspicious—until the funds disappeared.

The agent's email account had been compromised. A fraudster, posing as the agent, intercepted the communication and redirected the commission to a fraudulent account. The lawyer, unaware of the breach, followed the instructions in good faith.

The investigation confirmed coverage after a thorough review. This case served as a stark reminder that cybercriminals don't just target large sums—they exploit trust and familiarity in everyday transactions.

In this instance, the fraud wasn't spotted until it was too late. But it highlighted how a simple step—like verifying a change in payment method through a separate channel—could have stopped the fraud in its tracks. It's a lesson in securing not just systems, but the habits and assumptions we rely on every day.



Secure It



Preparing for Tomorrow: Understanding Future Risks and Evolving Threats

Top Fraud trends:

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



A "hands-off" future

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.



A Conversation with our expert from the field Matt Cunningham, Halton Regional Police Service



Detective Constable Matt Cunningham has over 23 years of law enforcement experience and currently serves in the Financial Crimes Unit at the Halton Regional Police Service, where he investigates complex financial crime and fraud. He holds specialized certifications as a Certified Fraud Examiner (CFE), Certified Financial Crimes Investigator (CFCI), and TRM Crypto Fundamentals Certification (TRM-CFC), supporting his work in protecting the public and maintaining trust within the community. His career also includes experience in major crime, child abuse and sexual assault, intimate partner violence, and homicide investigations, bringing a disciplined, detail-driven approach to complex and sensitive cases.

■ What early warning signs of fraud are commonly overlooked in everyday situations?

One of the earliest and most common warning signs of fraud is the use of urgency and pressure. Once a fraudster has a victim engaged—often on the phone—they work deliberately to keep them from pausing, hanging up, or thinking critically. Victims are frequently told things like, “This offer expires today,” “Your account will be locked,” or “Don’t tell anyone or you’ll make it worse.” The goal is to create panic and force immediate action, leaving little room for reflection or verification. Another red flag is being asked to make unusual or unconventional payments. Requests for gift cards, wire transfers, or cryptocurrency are especially telling, even when they are framed as a “temporary workaround” or “a faster option.” In many cases, these requests start with smaller amounts to avoid raising suspicion early on, gradually escalating once trust has been established.

Unexpected contact followed by requests for personal information is also a common pattern. Fraudsters may reach out without warning and, after building rapport, begin asking for sensitive details under the guise of verification. Phrases such as “We just need to confirm a few details” can sound routine, but they are often used to extract information that can later be exploited. Finally, fraud often relies heavily on emotional manipulation. This can take the form of fear, such as threats of legal trouble or account compromise; excitement, including promises of prizes or investment opportunities; or trust, as seen in romance scams or impersonation of authority figures like police or the CRA. When emotions take over, logical thinking can slip into the background, and small warning signs are more easily dismissed or rationalized.

■ In impersonation cases, how do fraudsters appear legitimate, and what should people verify to confirm someone's identity?

What we typically see in the Financial Crime Unit is the frequent use of fraudulent identification, most often in the form of an Ontario driver's licence. Fraudsters have become increasingly sophisticated in how they duplicate these documents. In many cases, the person reviewing the identification can sense that something is not quite right, even if they cannot immediately articulate what the issue is. Fraudsters are skilled at recognizing this hesitation and will often exploit it by applying pressure to move the interaction forward.

A common example of this can be seen in account takeover scenarios. A fraudster may approach a bank teller while presenting fraudulent identification. The teller might notice something feels off and instinctively pause, but without a clear reason to stop the transaction. At that point, the fraudster may escalate the situation by creating a sense of urgency, becoming visibly frustrated, or appearing angry. The teller, feeling the pressure of the situation and possibly concerned about a customer complaint or causing a delay, may rush the transaction and override their initial instincts.

The most effective way to confirm whether identification is fraudulent is through the use of a verification scanner. This type of tool represents a relatively small investment but can prevent significant financial losses. A scanner can quickly validate or disprove the concerns an employee may already have when examining an identification card, providing confidence to pause or stop a transaction when something does not appear legitimate.

■ What contact methods do fraudsters most often use, and how do those channels shape how the fraud unfolds?

Most of the cases I've investigated with my team involve fraudsters cold-calling victims. As noted earlier, these individuals often pose as bank representatives, government officials, or technical support staff. Phone calls are particularly effective because of their personal and direct nature, which allows fraudsters to apply psychological pressure in real time. They can create a sense of urgency, steer the conversation, and manipulate victims into sharing personal information or making payments. When this is combined with caller ID spoofing, the call can appear legitimate, making it more likely that the victim will comply.

Fraudsters are also highly skilled at adjusting their script on the fly based on how a victim responds, which helps the interaction feel more authentic and convincing. These scams tend to be especially effective when the fraudster exploits unfamiliar technology, such as cryptocurrency, and positions themselves as a helpful guide through the process. In many cases, trust is gradually built as the fraudster walks the victim step by step through a transaction, reinforcing the illusion of legitimacy and making it harder for the victim to recognize the situation as fraudulent.

■ What vulnerabilities do fraudsters look for, and do they tailor their tactics to specific age groups or situations?

Based on my experience, fraudsters most often target individuals aged 60 and over, particularly through investment scams, phishing attempts, and romance scams. This group is frequently targeted because they may have accumulated more financial assets over time and, in some cases, may be less familiar with evolving online threats. Fraudsters deliberately tailor their approaches to appear credible and trustworthy, increasing the likelihood that these scams will succeed.

Emotional vulnerability is another factor that fraudsters commonly exploit. Situations involving widowhood, loneliness, grief, fear, or heightened excitement can impair judgment and make individuals more susceptible to manipulation. Scams such as romance fraud, banking scams, cryptocurrency schemes, lottery scams, and inheritance fraud are often designed to tap into these emotional states, encouraging victims to act quickly or maintain secrecy.

Limited digital literacy and gaps in cybersecurity knowledge can also increase exposure to fraud, particularly when it comes to technical scams. Phishing attempts, tech support scams, and identity theft frequently rely on unfamiliarity with digital tools or processes. When victims are unsure how certain technologies work, fraudsters are able to position themselves as helpers or authorities, further reducing the likelihood that the scam will be questioned.

■ Have you seen fraud cases that break common assumptions, and what could have prevented them?

Within the past year, a newer scam commonly referred to as “banker’s fraud” has emerged. In this scheme, fraudsters cold-call victims while posing as bank representatives. Using persuasive language and pressure tactics, they convince victims that their debit and credit cards have been compromised. Victims are told that a bank representative will come to collect the cards and are instructed to cut them up and place them in an envelope for pickup. During the call, the fraudsters also obtain the victim’s PIN, which gives them full access to the associated accounts.

In reality, the person collecting the envelope is often an Uber driver who is unaware they are participating in a scam. The driver delivers the envelope to an accomplice, frequently meeting at a public location such as a street corner. Once the cards are in their possession, the fraudsters begin using them almost immediately. In these cases, the financial impact is significant, with average losses per victim ranging between \$35,000 and \$40,000. The most effective way to prevent this type of fraud starts with understanding that a bank will never ask for a PIN over the phone. Under no circumstances should a PIN be shared. If someone claims to be calling from your bank, the safest step is to hang up and independently contact the bank using the official phone number listed on the back of your card or on a bank statement. Any phone number provided by the caller should be treated with caution, as it may be part of the scam.

■ Beyond financial loss, what broader impacts does fraud have on victims?

Victims of fraud often experience significant emotional and practical impacts, including stress, anxiety, and feelings of shame or embarrassment, even though the crime is never their fault. Access to funds may be disrupted, which can make it difficult to pay bills or manage day-to-day expenses. In some cases, fraud can also damage a person's credit score, affecting their ability to secure loans, mortgages, or certain types of employment.

The effects of fraud can also extend to personal relationships, as victims navigate both the emotional strain and the financial consequences of the crime. Recovery is rarely immediate and often requires considerable time and effort, including contacting financial institutions, working with law enforcement, and closely monitoring accounts for any further suspicious activity. While some victims become more cautious following an incident, others may remain vulnerable and risk being targeted again.

Investigators with the Halton Regional Police Service frequently work alongside the Victim Services Unit to help support individuals affected by fraud. This collaboration helps ensure that victims have access to appropriate resources and guidance as they move through the recovery process.

■ What actions by victims can make investigations more difficult, and why do some people delay reporting fraud?

One of the biggest concerns we see from an investigative standpoint is when victims continue communicating with the fraudster after the matter has already been reported to police. Victims may feel embarrassed, anxious, or desperate to recover their money and believe they can persuade the fraudster to return the funds. In some cases, they may also attempt to conduct their own "investigation" in an effort to help police. Unfortunately, continued contact often leads to further victimization and can significantly complicate the investigation by alerting the fraudster, altering evidence, or undermining investigative strategies.

Another challenge arises when victims are unfamiliar with the Canadian court process. If charges are laid, a lack of understanding about how the legal system works can lead to confusion, unrealistic expectations, or missteps that may affect the case. Having a clear understanding of the process is important so victims know what to expect and how their actions may impact proceedings.

Finally, embarrassment or fear of judgment can lead some victims to withhold or minimize key details when reporting the fraud. Omitting information—intentionally or unintentionally—can create integrity and credibility issues later in the investigation. If additional details come to light after the fact, it can weaken the overall case and, in some situations, result in charges being withdrawn. Full honesty and transparency are critical when reporting fraud, as complete and accurate information gives investigators the best chance to pursue the matter effectively.

■ If fraud is suspected, what immediate steps should someone take to reduce harm?

Once fraud is suspected, the most important initial step is to immediately cease all contact with the fraudster and preserve any potential evidence. This includes keeping emails, text messages, phone numbers, names or aliases provided, bank and credit card records, transaction receipts, and any other relevant information. Victims should avoid deleting, editing, or altering files in any way, as doing so can compromise the integrity of the evidence. Maintaining a clear chain of custody is critical to ensure that the information remains reliable and, if necessary, admissible in court. At the same time, the appropriate authorities should be notified as quickly as possible. This includes contacting local police, financial institutions, credit card companies, and reporting the incident to the Canadian Anti-Fraud Centre. Early notification allows these organizations to take immediate steps to limit further losses, flag suspicious activity, and support any subsequent investigation. Where possible, victims or witnesses should also be encouraged to provide written or video-recorded statements to police or the relevant investigative body. Detailed statements captured early help preserve accurate recollections of events, timelines, and interactions, which can be crucial as investigations progress. Providing clear, timely, and complete information gives investigators the strongest foundation to assess the incident and pursue appropriate next steps.

■ What long-term habits or practices meaningfully reduce the risk of fraud?

Proactive awareness is one of the most effective tools for reducing the impact of fraud. Members of the Halton Regional Police Service actively work to educate citizens, community groups, financial institutions, and businesses about fraud prevention. These efforts focus on helping people recognize common tactics, understand emerging risks, and know how to respond if something does not seem right.

When new fraud trends begin to affect the community—particularly those involving multiple victims—the Financial Crimes Unit also issues media releases to raise awareness. These communications are intended to alert the public quickly, share practical prevention advice, and reduce the likelihood of further victimization by ensuring timely and accurate information reaches the community.

■ How do you expect fraud tactics to evolve, and what should people be more alert to in the future?

One of the most significant trends in recent years has been the increasing use of cryptocurrency in fraud-related activity. As digital currencies become more widely adopted, they are also being used more frequently by fraudsters to move and conceal illicit funds. Cryptocurrency transactions can be difficult to trace and recover, which makes them particularly attractive for criminal activity and places investigators at a disadvantage.

As a result, organizations involved in fraud prevention and investigation should prioritize education and training for their employees on how cryptocurrency works. At present, criminals are often far ahead of prevention efforts in their understanding and use of these tools. Improving awareness of how cryptocurrency is acquired, transferred, and misused can help close this gap and better equip organizations to recognize, prevent, and respond to fraud as these tactics continue to evolve.

This Q&A is provided for general informational purposes only. The views and opinions expressed by [Detective Cunnington] are their own and do not necessarily reflect the views, policies, or positions of any law enforcement agency or government body. Participation in this Q&A does not constitute an endorsement of First Canadian Title Company Limited, its products, or its services.



How FCT Can Be Your Partner for Secure Real Estate Transactions

The Role of Client ID Verification in Cybersecurity

In today's digital-first real estate market, verifying client identities is no longer just a regulatory requirement – it's a critical line of defense against cyber threats and fraud. Cybercriminals continue to exploit weaknesses through tactics like phishing, social engineering, and synthetic identity theft, putting sensitive client data and property transactions at risk. A robust client ID verification solution helps safeguard all parties by ensuring that individuals are who they claim to be. By using advanced tools like biometric checks, multi-factor authentication and encrypted data handling, these systems create an additional layer of security, preventing fraudsters from exploiting vulnerabilities. For professionals across the industry – from legal professionals to REALTORS® – identity verification provides peace of mind, regulatory compliance, and protection against the growing risks of cyber-fraud.

Fintracker: A Compliance Partner for REALTORS®

Fintracker is designed with REALTORS® and brokerages in mind. More than just an ID verification tool, Fintracker offers a full digital compliance platform that integrates seamlessly into real estate workflows. It scans and authenticates government-issued IDs, auto-populating some of the required information on FINTRAC forms, and performs comprehensive checks against AML watchlists, sanctions and adverse media sources. By maintaining encrypted, audit-ready records, Fintracker reduces paperwork and ensures brokers and REALTORS® are always prepared for regulatory reviews. What makes Fintracker unique is its ability to simplify compliance in a fast-paced market – helping REALTORS® confidence. With Fintracker, identity verification isn't just a security step, it's a powerful enabler of efficiency, trust and professional accountability.

Bluink: A Trusted Tool for Legal Professionals

FCT's Client ID Verification solution, powered by Bluink, helps legal professionals verify clients with confidence through authenticated identity document verification, passport-chip scanning, and a secure mobile experience that clients can complete in minutes. At its core, the solution goes beyond a visual review by authenticating identity documents and checking client information against multiple trusted data sources, helping legal professionals strengthen their client verification process.

What sets FCT Client ID Verification powered by Bluink apart is its ability to fit seamlessly into modern legal real estate workflows. Verification requests can be submitted through the FCT online ordering portal or integrated conveyancing platforms, making client verification a simple addition to existing processes.

Whether a transaction is completed in person or remotely, FCT Client ID Verification powered by Bluink helps legal professionals apply a consistent approach to client verification while supporting Know Your Client (KYC) obligations and helping strengthen fraud prevention efforts.

Together, solutions like Bluink and Fintracker strengthen the real estate industry's defenses against cyber-fraud. By tailoring identity verification to the unique needs of both legal professionals and REALTORS®, FCT is helping to ensure that every transaction is secure, compliant and built on a foundation of trust.



Final Words From Our CEO

As we have seen, cyberthreats are a continually evolving risk, but our best defense is staying informed and proactive. When we know how to **spot** the red flags, take action to **stop** suspicious activity and implement safeguards to **secure** sensitive information, we can create a more secure real estate transaction.



Every solution we bring to market is designed with both innovation and security in mind, because progress without protection should never be an option. Our clients trust us to deliver tools that are forward looking and reliable. That trust is earned by ensuring every innovation reflects the same standard of security that defines FCT.

Michael LeBlanc, LL.B.
Chief Executive Officer, FCT

Continue Learning:

To continue building your knowledge and resilience against cyberthreats, we invite you to explore our blog articles below, where you'll find practical insights and resources to help you stay ahead of emerging risks:

How to spot a phishing attack

What you and your clients should know about ID verification

Your top cybersecurity questions answered

How technology transformed title fraud

What's next? The future of fraud prevention

Digital ID Verification: do you know your customer?

Stay updated on the latest fraud prevention insights from FCT:

Fraud insights centre



Insurance by **FCT Insurance Company Ltd.** Services by **First Canadian Title Company Limited.** The services company does not provide insurance products. This material is intended to provide general information only. For specific coverage and exclusions, refer to the applicable policy. Copies are available upon request. Some products/services may vary by province. Prices and products/services offered are subject to change without notice.

®Registered Trademark of **First American Financial Corporation.**