2025

FCT Cybersecurity Resource Guide

FCT

Contents

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 Twane Boettinger on Cybersecurity

As cyber threats continue to evolve in complexity and scale, the real estate and title insurance industries face unique challenges in protecting sensitive data and high-value transactions. To shed light on these issues, we spoke with Twane Boettinger, Director of Information Security and IT Risk at FCT. With a background in law enforcement and a deep expertise in cybersecurity, Twane offers a comprehensive look at the current threat landscape—from phishing and identity impersonation to the future of multi-factor authentication and cloud vulnerabilities. This conversation provides valuable insights for legal professionals, realtors, and lenders looking to strengthen their defenses and stay ahead of emerging risks.

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

One of the biggest risks we currently encounter is regarding compromised business email accounts. Fraudsters are able to impersonate authorized participants in a transaction with increasing accuracy, by hijacking legitimate email accounts or creating lookalike domains. These tactics allow them to divert funds or isolate real participants from communication threads. Also, as identity impersonation becomes more sophisticated with virtual avatars and deepfake technology, even video calls may no longer be a reliable means of verifying someone's identity.

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 the most common entry points. Fraudsters are now able to bypass multi-factor authentication MFA (MFA) by stealing credentials, most frequently from users who recycle passwords across multiple platforms. MFA itself is under attack — with criminals investing time and resources to intercept or hijack authentication tokens. The rise of generative AI has also made phishing more convincing and scalable, allowing attackers to craft highly personalized and believable messages.

How do the cyber threats faced by FCT differ from those faced in other industries, such as traditional financial institutions or other service providers? Is there a significant overlap or are we dealing with a unique set of challenges?

The fundamentals are the same for us as in other industries — you're protecting data and processes. What differs is how fraudsters exploit those processes. In our industry, they're not skimming pennies off ATM transactions; they're targeting high-value real estate deals worth millions. So, while the threats are similar, the scale and method of exploitation are unique in our case.

What do you identify as the most likely next wave of cyberattacks in this industry – will it be more sophisticated phishing and social engineering, exploitation of cloud systems, or something new entirely?

The next wave will likely involve more sophisticated forms of phishing, greater ease of bypassing current MFA tools, and greater accuracy of impersonation through the use of AI. Criminals are already using generative AI to craft more convincing phishing messages and build attack code. The advances in quantum computing also poses a significant future threat — encrypted data that is stolen today may be secure for now, but could be decrypted at a later time, as quantum computing is predicted to be available in a mainstream context within a 4–8 year timeframe. This can lead to sensitive information like biometric data or financial records, which are currently secured, eventually being exposed.

How does FCT train or equip employees and partners to recognize and resist these potential threats?

At FCT, we run monthly security training updates for all employees, with completion tracked and escalated if missed. For the past 2+ years, we've utilized a dramatic video series that embeds security lessons into a storyline, followed by quizzes to reinforce learning.
We also ramp up our efforts during Cybersecurity Awareness Month with corporate events like cybersecurity themed escape rooms and internal awareness campaigns.
The goal is to build a culture of cybersecurity consciousness across the organization.

You've spoken before about the importance of multi-factor authentication (MFA). How critical is it in protecting sensitive client and transaction data and how is it currently used by FCT to accomplish this?

Multi-factor authentication is absolutely essential in protecting sensitive data, particularly in industries like ours where the financial stakes are high. At FCT, we've made MFA a core part of our security strategy.
We rely on tools like authenticator apps and hardware tokens for our internal MFA practices, while we actively discourage the use of SMS and email as MFA tools in our organization due to their known vulnerabilities. These methods ensure that even if a password is compromised, unauthorized access will still be blocked.
MFA adds a critical layer of additional defense and is enforced across all internal systems that handle sensitive client and transaction data.

What are some challenges faced by organizations when broadly rolling out MFA, and what are some ways to help mitigate these challenges?

User resistance is one of the biggest challenges, especially with mobile authenticators—not everyone is comfortable using their phone, so we offer hardware alternatives like FIDO keys. Another hurdle is helping users understand the differences in strength between MFA methods: biometrics like facial recognition and fingerprints are strongest, followed by authenticator apps; SMS is weaker and vulnerable to SIM swapping, and email should never be used due to its exposure risk. We address these issues through ongoing education, clear communication, and flexible options that balance security with usability—making MFA effective without being burdensome.

As there is a continued push to leverage cloud-based platforms, what are some of the key cloud vulnerabilities that concern you most?

The biggest concern is the rapid pace of change in cloud environments. Features and security controls are constantly updated or deprecated, often without clear notice. This requires continuous monitoring to avoid gaps in security posture. What used to change over months or years now shifts in days or weeks, and staying on top of these changes is essential.

Looking ahead, do you see MFA evolving into more advanced identity verification tools over time, such as the regular use of biometrics?

Absolutely. Biometrics like Face ID and fingerprints are currently the strongest MFA methods. But even biometric data could be at risk in the future, especially with advances in fields such as quantum computing and deepfake technology. The MFA practices we know today will need to evolve to stay effective, especially as virtual interactions become more commonplace and ultimately harder to verify if it is actually a real person on the other end.

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

The nature of identity is under threat. With the developments in deepfake technology, even video calls can be spoofed with alarming accuracy. Organizations must find reliable ways to validate identity and ensure that they are interacting with the authorized individuals that they claim to be. That's going to be a major challenge in the near term — and one we need to get ahead of. Cybersecurity measures often operate in a reactionary state, where we need to adapt to the way new technologies are used by criminal entities. Looking ahead we need to remain proactive rather than reactive to stop these potential crimes before they begin.

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 BluInk 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

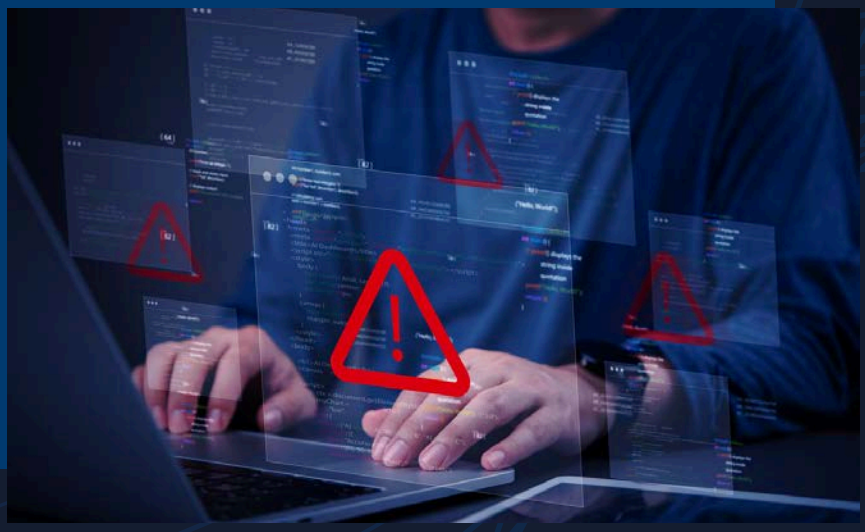
Claim: When a confirmation wasn't enough: A mortgage payout intercepted by fraud

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 AIpowered 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 Marie Taylor on Future Risks and Evolving Threats

As the real estate industry continues to adapt to an increasingly digital world, so too do the threats that challenge its integrity. To help us look ahead and prepare for the future of cybersecurity in property transactions, we spoke with Marie Taylor, Director, National Underwriter Legal, Risk and Compliance at FCT. With over two decades of experience on FCT's legal team, Marie is a nationally recognized expert in residential title insurance and fraud prevention. As a Certified Fraud Examiner and former member of FSRA's Technical Advisory Committee for Mortgage Brokering, Marie brings a wealth of insight into the emerging risks and technologies shaping the future of title fraud. In the following Q&A, she shares her perspective on how AI, synthetic identities, and digital platforms are transforming the fraud landscape—and what the industry must do to stay one step ahead.

What emerging cyber fraud techniques do you believe will pose the greatest threat to real estate transactions in the next 3–5 years?

The increasing sophistication of fraudsters, paired with the emergence of AI, poses the biggest threat. Only a couple of years ago it was easy to detect phishing and smishing scams given the grammatical and typographical errors. Now, with the implementation of AI, fraudsters are composing very authentic emails. Deep fakes are also evolving, and it is no longer as easy to detect if the person across the computer screen is in fact the individual you believe you are speaking with. Voice cloning has also become very convincing. The evolution of AI has made a fraudster's job so much easier than it was prior to Covid.

With the increasing digitization of land registries and legal records, what vulnerabilities do you identify that the industry should start preparing for now?

With the digitization of land registries and legal records, one of the most significant vulnerabilities is the risk of cyberattacks, especially ransomware. As these systems store highly sensitive data, it's critical to implement strong security measures, including resilient authentication protocols, reliable data backups, and proactive threat monitoring, to ensure the integrity and availability of records in the face of evolving digital threats.

How do you see AI-driven tools like deepfakes and voice cloning evolving in their ability to bypass identity verification systems used in property transfers?

Fraudsters are increasingly using AI to create convincing synthetic audio and video, allowing them to impersonate executives or authorized users to access secure systems or approve transactions. Deepfakes can mimic facial features, while voice cloning replicates voices to fool biometric authentication. A recent scam that received significant media coverage saw a Hong Kong financial worker tricked into sending $25 million during a web meeting with false participants using deepfakes to impersonate real individuals. Criminals can now forge documents, selfies, and voices to build fake digital identities and commit fraud. With this technology, it's easy to imagine a fraudster creating a realistic ID and using deepfakes to impersonate a lawyer advising a client to send funds to close a real estate deal.

What role do you think blockchain or decentralized technologies could play in either preventing or enabling future title fraud?

Personally, I think the use of blockchain technology could help prevent future title fraud. While I am not particularly well versed in blockchain technology, from what I have read it's an interesting concept. Imagine having a database for a real estate transaction where all the data from the point of finalizing an agreement of purchase and sale, to obtaining a mortgage, to the preparation of the legal documents and sending of funds is all stored in one secure place that cannot be altered.

Do you foresee synthetic identity fraud becoming more prevalent in real estate, and how might fraudsters try to adapt current tactics to exploit mortgage systems more effectively?

Synthetic identity fraud is already widespread in real estate transactions. Equifax Canada reported in 2024 that cases tripled in just one year. With new techniques and technologies, fraudsters have more ways to exploit system vulnerabilities. We've moved from in-person mortgage applications and cheque handoffs at Land Registry Offices to fully digital processes—online applications, electronic signatures, and wire transfers—without ever meeting face-to-face. This shift creates the perfect environment for fraudsters to hide behind technology and impersonate professionals, making it easier than ever to carry out real estate fraud.

How can title insurers like FCT better support legal professionals and realtors in preparing for the next wave of cyber threats?

I think education and the use of IDV software like Bluink and Fintracker goes a long way in supporting our customers. The systems we use are highly secure and monitored in real time for potential threats. FCT was the very first title insurer to employ fraud underwriting over 20 years ago, and we work diligently on keeping up with the current fraud trends in order to mitigate the risk for lawyers, lending professionals and of course ourselves.

What are the biggest risks associated with third-party platforms (e.g., e-signature tools, virtual meeting software) in the context of secure property transactions? Is there anything we can do to mitigate the risks associated with using these tools?

The biggest risks that we see associated with the use of these platforms are cyber security threats, data breaches, and fraud.
Some poorly designed systems may lack comprehensive audit trails or sufficient data logging. Mitigating this risk requires the use of platforms that have strong encryption, multi-factor authentication, and comprehensive audit trails. You should perform your due diligence on the vendor - find out how information is being stored, understand and learn their security policies and data handling practices.

Are there any emerging technologies or innovations that you believe could revolutionize fraud prevention in the title insurance space?

I believe that fraud prevention requires a combination of technology, vigilance, and proactiveness. I think blockchain and robust biometric verification will go a long way in fraud prevention, but so does good old know your customer and instinct. It's important to remember that while technology enhances our ability to prevent fraud, it also provides fraudsters with more tools to commit fraud. As an industry, we must all work together to ensure we are doing what we can to prevent it and to try to stay one step ahead.

As technological advancements are helping to facilitate cybercriminals in becoming more organized and collaborative, how should FCT evolve its internal fraud detection and prevention strategies to stay ahead?

I think FCT has already taken significant steps to evolve its internal fraud detection strategies. We have a dedicated team of experienced individuals who receive ongoing training on how to detect new types of potential fraud. We work closely with our claims department to dissect our fraud claims and see if there are patterns emerging that require us to alter our underwriting. We also leverage IDV software that hits on many different attributes to flush out fraudulent identification.

Looking ahead, what cultural or behavioral shifts within the industry do you think are necessary to build stronger cyber resilience across all stakeholders?

I think the industry must accept the fact that fraud is here to stay and it is only going to get easier for the fraudsters. We need to educate ourselves on how it happens and how we can stop it. We must increase our personal security practices, with strong passwords, multi-factor authentication, fire walls and employing secure IDV software. Verify, verify, verify – and never become complacent, because fraud can happen to anyone.

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** focuses on creating a secure and compliant experience for legal professionals. At its core, Bluink leverages biometric verification and advanced document authentication to confirm client identities against government issued IDs. What sets Bluink apart is its emphasis on privacy-first design. Verified IDs are stored securely on the client's mobile device in their digital wallet, not on central servers, reducing the risk of data breaches. For lawyers and notaries, this means streamlined compliance with FINTRAC KYC and Law Society requirements, while ensuring sensitive information remains protected. Bluink blends ease of use with industry-leading security standards, allowing legal professionals to focus on serving their clients with confidence, knowing their transactions are backed by trusted, verified identities.

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