2025 DATARISK RESEARCH REPORT

2025 Sector Report on Cyber Security

Executive Summary

Cyber Security Awareness Series

Cyber threats to the real estate industry are escalating in complexity and frequency. Fraudsters are targeting residential and commercial real estate transactions with business email compromise, seller impersonation, synthetic identities, and even AI-generated voice scams. As the financial and reputational risks grow, legal professionals must be prepared to recognize patterns, respond swiftly, and strengthen controls.

This guide equips legal professionals involved in real estate transactions with a current threat overview, a catalog of real-world red flags, and practical tools to meet Canada's evolving Know Your Client (KYC) obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Whether you're processing payouts, onboarding clients, or closing transactions, the message is the same: Spot It. Stop It. Secure It.

PREPARED BY
Claudiu Popa
Datarisk Canada

Sector Research Report

Current Threat Landscape

1. Wire fraud is the leading risk in title transactions.

The U.S. Internet Crime Complaint Center (IC3) reported over $2.9 billion in business email compromise (BEC) losses in 2023, with a significant share impacting real estate. Criminals intercept transaction emails and redirect wire transfers, often targeting closings.

2. Seller impersonation is surging.

A 2024 industry survey by the American Land Title Association found that 28% of title companies experienced at least one seller impersonation attempt in the past year. Fraudsters pose as property owners—often of vacant land—and push for fast closings.

3. Synthetic identity fraud is entering title workflows.

Synthetic IDs combine real and fake information to create a new, convincing identity. Fraudsters use them to pose as borrowers, attorneys or payees. These identities can pass soft KYC but break under document scrutiny.

4. Mailbox rule hijacking is on the rise.

Cybercriminals set forwarding rules on compromised email accounts, silently diverting replies and documents. This technique avoids spam filters and is rarely noticed until after wire transfers are sent.

5. Deepfake-enabled impersonation is emerging.

AI tools are being used to create convincing voice and video recordings. Criminals use deepfake voices on callback verifications to impersonate executives or clients and approve large fund transfers.

6. Weak identity verification and over-retention increase exposure.

Collecting and storing too much personal data—especially unverified or unnecessary ID images—creates risk if breached. Improperly handled KYC data is a rising liability under new compliance frameworks.

Risk Summary

The table below connects key threat intelligence gathered from national reporting agencies, law enforcement alerts, and industry surveys, to real operational risks in title insurance. It distills how large-scale fraud patterns surface inside files and workflows, helping professionals anticipate vulnerabilities before they become incidents. Each risk type includes its most likely entry point and the internal role typically targeted, allowing firms to map safeguards to the right process and people.

Risk Type	Description	Common Entry	Most Vulnerable
Wire Fraud	Diverted funds via fake instructions	Email	Closing officer
Seller Impersonation	Fake owners selling legitimate property	Email, e-signature	Title agent
Synthetic Identity	Fraud using mixed real/fake identity	Onboarding, payouts	Intake and payout teams
Mailbox Rule Hijacking	Forwarding rules that hide email trails	Compromised email	Attorneys, staff
Deepfake Voice/Video	Realistic fake audio used to confirm wire changes	Phone calls	Finance, partners
KYC Data Over-retention	Storing raw ID images beyond necessity	Shared folders	Compliance and intake

Catalog of Red Flags

This listing outlines the most common warning signs observed in fraudulent transactions, and provides recommended Prevent, Detect, and Correct actions.

1. Last-Minute Change in Wire Instructions

- Prevent: Prohibit email-based payment approvals. Require dual authorization and verified callback using a trusted number.
- Detect: Look for time-sensitive language, high-pressure tactics, or changes made after business hours.
- Correct: Immediately contact the receiving bank's fraud department. Notify your underwriter and begin recovery protocols.

2. Seller Requests Quick Cash Closing

- Prevent: Flag and delay closings where ownership cannot be verified through land registry and independent documents.
- Detect: Watch for vacant land, non-owner-occupied properties, and new email domains.
- Correct: Pause transaction and re-verify identity via phone, video and address-linked documentation.

3. Unusual Email Forwarding Behavior

- Prevent: Disable automatic forwarding rules in corporate accounts. Use MFA and anti-spoofing records (SPF, DKIM, DMARC).
- Detect: Monitor logs for new mailbox rules or unfamiliar access locations.
- Correct: Reset credentials, audit correspondence history, and alert clients to use trusted portals.

4. Inconsistent ID Documents or Thin Credit Files

- Prevent: Use identity verification that cross-checks name, DOB and address via credit bureaus or document authentication tools.
- Detect: Spot low file depth, mismatched phone numbers, and perfect documents with no history.
- Correct: Request secondary proof (e.g., government ID + utility bill) and escalate to compliance.

5. Voice Approval that Doesn't Feel Right

- Prevent: Use pre-assigned callback phrases or verbal PINs. Avoid approving transactions on the first inbound call.
- Detect: Note odd pacing, refusal to repeat back account details, or robotic-sounding responses.
- Correct: End call and initiate outbound verification using a trusted directory.

Red Flags Summary for Front Liners

5 Red Flags Everyone Should Know

- “Please update account details before close of business”
- “Client unavailable for call; just email”
- Property owned by someone not on the call
- Account number off by one digit
- ID image perfect but no credit history

3 Things to Do Every Time

- Use a callback to a verified number
- Store verification results, not images
- Require dual approval for fund release

What to Do if Something Feels Wrong

- Stop the transaction
- Call your manager
- Notify FCT and the client immediately

638
$M REPORTED LOSSES

12.8
ACTUAL LOSSES (EST $B)

28%
OF TITLE FIRMS WITH SELLER IMPERSONATION

+14%
INCREASE IN SELLER IMPERSONATION ATTEMPTS

48%
2024 US MORTGAGES FLAGGED FOR 1+ WIRE/FRAUD RISK

Sources: Canadian Anti-Fraud Centre, ALTA 2024 Fraud Alert Survey, FundingShield Q1 2024 Wire Fraud Risk Report

Controls & Safeguards Checklist

Understanding the application of effective countermeasures to cyberfraud and risk scenarios in operational situations.

Control Area	**Best Practice**
Client Verification	Use third-party identity tools (Equifax, TransUnion) or trusted ID verification portals
Data Minimization	Store only the verification result and reference ID, not the ID image itself
Callback Controls	Use a printed or digital directory, not numbers from the email thread
Dual Authorization	Require two authorized signers for all payment changes
Portal Use	Move fund approvals and communications into a secure portal with audit logs
Incident Response	Create a 15-minute checklist: notify bank, insurer, client, preserve logs
Training	Refresh staff quarterly on fraud tactics, suspicious activity signs, and KYC steps

Red Flag Quick Table

Red Flag	How to Respond
Change in wire instructions	Call using verified number, require dual sign-off
Seller refuses video call	SDelay closing, verify ownership with land registry
Mailbox rule appears or triggers	Lock account, notify IT, switch to portal messaging
ID too perfect, no file depth	Use document scanning + credit bureau validation
Weird-sounding voice approval	Stop, re-initiate callback with secure code

Three-Year Forecast (2025–2027)

- BEC and seller impersonation will continue to grow unless verified communication channels become standard.
- Synthetic ID fraud will increase, particularly targeting remote transactions.
- FINTRAC examinations will begin by late 2026, requiring defensible KYC and transaction recordkeeping.
- Deepfakes will be used more frequently to hijack trust, especially over phone and video.
- Regulatory penalties and class-action litigation will increase for over-retention or mishandling of ID data.