

LAWPRO®

Toronto Lawyers ASSOCIATION TLA

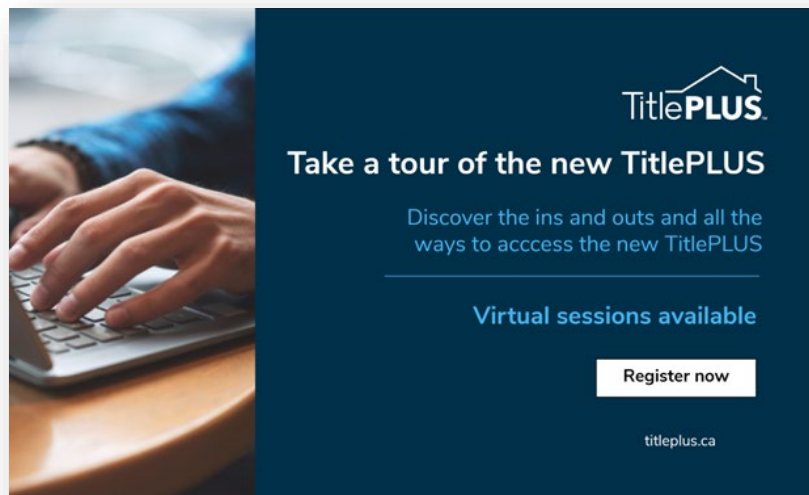
TitlePLUS™

Thursday Tips with LAWPRO and TLA:
Protecting your firm against fraud

April 13, 2023

Program materials

| | |
|--------------------------------------------------------------------------------|-----------|
| Funds transfers verification checklist..... | 1 |
| Fraud watch fact sheets..... | 2 |
| Update about funds transfers..... | 14 |
| You transferred funds to the wrong account. What now?..... | 17 |
| Wire fraud scams on the rise: 5 tips to reduce your risk..... | 19 |
| Watch for real estate frauds involving private mortgages..... | 21 |
| What’s wrong with this picture? Be on alert for fake IDs..... | 23 |
| Title insurance matters: One of these things is not like the other..... | 24 |
| Additional resources and CPD..... | 25 |
| Speaker bios..... | 26 |



This resource is provided by Lawyers’ Professional Indemnity Company (LAWPRO®). The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.



lawpro.ca
Tel: 416-598-5800 or 1-800-410-1013
Fax: 416-599-8341 or 1-800-286-7639
Email: practicepro@lawpro.ca

Funds Transfer Instructions Verification Checklist

| | |
|--------------|----------------|
| Date: | Verifier Name: |
| File Number: | File Name: |

1. Attach a copy of the funds transfer instructions to this page.

2. Check that the name of the sender of the instructions matches the name of the person you were expecting to send instructions in your file. If not, involve a lawyer and have the lawyer complete the verification process.

3. **Verification method DO NOT use the phone number in the instructions.**

Always use a trusted number such as the one from the file opening sheet or from a reliable directory.

*On file opening, obtain a password from the client and record it in the physical file

Phone call

OR

In person

Phone # called _____

Name on ID: _____

4. **Verify sender identity and payment details:**

Person contacted (name and date): _____

Does the sender confirm they sent the funds transfer instructions?

YES – continue on

OR

NO – immediately involve a partner and proceed to Step 6

Verify the payee and bank account details:

Payee: _____ Bank: _____

Institution number

Transit number

Account number

Are the bank account details correct? If yes, continue on. If not, immediately proceed to Step 6.

Are there any red flags? Any typos in the instructions or email address? Any issues or concerns that came up? If something is amiss, trust your instincts. Make a note and raise it with a partner.

5. If the sender and payment instructions are correct, continue with normal processes and request cheque or wire.

6. If any part of the verification fails, **STOP**. Immediately involve a partner at your firm.

7. **If payment instructions change, STOP**. Involve a partner at your firm and complete the verification process again.

7. **If funds were mistakenly sent before the process was completed:**

a) IMMEDIATELY contact the bank and request a freeze and reversal.

b) IMMEDIATELY report the matter to LAWPRO: www.lawpro.ca/claims.

c) Consider reporting to any crime or cyber insurer you may have.


d) Review our article [You transferred funds to the wrong account – what now?](#) For further guidance.

BAD CHEQUE SCAMS

Fraudsters retain the firm on a contrived legal matter so they can run a counterfeit cheque or bank draft through the firm trust account and walk away with real money. The fraudster will provide real looking ID and documents. When the bad cheque or draft bounces, there will be a shortfall in the trust account.



FRAUD WATCH



! If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS

- Initial contact email is generically addressed (e.g., “Dear attorney”) and/or BCC’d to many people.
- Client uses one or more email addresses from a free email service (e.g., Gmail, Yahoo!), even when the matter is on behalf of a business entity.
- Domain name used in email address or website was recently registered (check at Whois.com or a similar service provider).
- Email header indicates sender is not where they claim to be.
- Client is new to the firm.
- Client says they prefer email communication due to time zone differences.
- Client may sign retainer but never actually makes the payment.
- Client is in a rush and pressures you to “do the deal” quickly, before the cheque clears.
- Client is willing to pay higher-than-usual fees on a contingent basis from (bogus) funds you are to receive.
- Despite the client stating a lawyer is needed to help push for payment, the debtor pays without any hassle.
- Cheque is drawn from the account of an entity that appears to be unrelated (e.g., a spousal arrears payment from a business entity).
- Payment amounts are different than expected or change without explanation.
- Client instructs you to quickly wire the funds to another bank account based on changed or urgent circumstances.

TIPS

Cross-check and verify information provided to you by the client:

- Google names, addresses, and phone numbers of the client and other people/entities involved in the matter.
- Look up addresses using Street View in Google Maps.
- Search AvoidAClaim.com’s database of bad cheque fraud names.
- Ask your bank or the issuing bank to confirm the branch transit number and cheque are legitimate.
- Call the entity making the payment or loan and ask if they are aware of the transaction.
- Hold the funds until all banks confirm funds are clear and can be withdrawn.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 2023 Lawyers’ Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers’ Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.

CORPORATE ID FRAUD

Changing or stealing the identity of corporate property owners is commonly accomplished by filing a notice naming imposter directors and officers, using fake ID for the real directors and officers or changing the address of the registered office. The fraudsters then retain a lawyer to help sell or mortgage the corporation's property.



FRAUD WATCH

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS

- Notice of Change is filed after a long period without a change in control of the corporation – even where real owners or their agents regularly make corporate filings
- Corporation has owned vacant land, disused or run-down property for a long time, without activity on title or visible use of land
- Property may be in highly marketable or developing areas but subject to restrictive zoning, is environmentally sensitive, or lacking road access
- Real directors/officers/shareholders are elderly, remote or otherwise vulnerable
- Current officers and directors were appointed very recently (see “Date Began” in Corporate Profile Report). This may not be a concern by itself, but merits a query about the circumstances of the recent changes and any notes taken (especially if there are other red flags)
- Corporation’s head office changed to non-existent or problematic address (such as a hotel – Street View on Google Maps may help determine this)
- Corporate resolutions or minute book with obvious errors or typos, or simply not available
- One lawyer retained to discharge an existing mortgage or file a Change Notice, but a different lawyer retained for borrower in the new mortgage transaction, or for corporation as vendor in a sale
- Mortgage statement for discharge purposes shows much less than registered amount of mortgage

- Small encumbrance, such as a construction lien, recently registered and discharged from title (to give credibility to the fraudster’s claim to be legitimate owner of the corporation)
- Client is new to you and documents show a different lawyer has acted for a corporation for years
- Clients say that title insurance for new mortgage is not required
- Client pushes for fast closing

TIPS

Check the Document Last Filed in the Corporate Profile Report. It will likely be an Annual Return, but could be a Form 1 – a possible red flag. A Corporate Document List search will disclose a history of the documents filed for the corporation. Ask for details of the change in control of the corporation, or permission to contact the corporation’s previous lawyer, agent, directors or officers.

Share this information with clerks and other law firm staff as they may be involved in parts of the transaction that you may not see.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAclaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 2023 Lawyers’ Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers’ Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.


INTERNAL OFFICE FRAUD

Is the fraudster in your office?

Not all fraudsters are strangers. Even partners, associates, law clerks or other employees can be fraudsters.



FRAUD WATCH

A futuristic digital background featuring a laptop with glowing blue and red data streams, binary code, and various icons like a magnifying glass, a document, and a target. The overall aesthetic is high-tech and data-driven.

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS

- Someone never takes vacation or sick leave, works overly long hours, or refuses to delegate work.
- A firm member undergoes a sudden change in lifestyle or temperament.
- The firm receives mail for a corporation for which no client file is opened or billed, or minute books are kept in the lawyer's office instead of with the corporate law clerk.
- Unusual patterns such as a sudden increase in payments to a person or entity, or complaints about slow payment from suppliers or clients, or an increase in written-off work in progress.
- Handwritten amendments on cheques returned from the bank.
- Double endorsed cheques which pay the fraudster personally. Look for names that are similar but not quite the same as existing clients and parties.

For more information see "Fraud on the Inside: What to do when partners, associates or staff commit fraud" at lawpro.ca/magazine

TIPS

- Conduct regular and random spot audits of lawyers and staff with access to law firm trust accounts.
- Keep an eye on lawyers and staff morale.
- Create a law firm culture which encourages mentorship and collegiality.
- Use unique passwords for anyone with access to law firm trust accounts.
- Create accounting systems where one person does not have full control or access to the money.
- Conduct a proper investigation, including gathering evidence and obtaining legal advice before proceeding on any suspicions of internal fraud.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 2023 Lawyers' Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers' Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.

REAL ESTATE SCAMS


Real estate frauds often occur in situations where the true owner's identity is stolen (ID theft) for sale or mortgage purposes, or the value of a property is exaggerated (flips).

Identity theft

When a client uses fake ID to assume the identity of existing property owners or uses a Notice of Change to become a director or officer or corporate owner for the purpose of committing fraud, this is identity theft. Once identity has been stolen, the fraudster sells or mortgages the property, or discharges a mortgage from title, then gets a new mortgage from another lender.



FRAUD WATCH



The background of the lower half of the page is a complex digital visualization. It features several vertical columns of glowing blue numbers, resembling a data stream or a server rack. In the foreground, there are various glowing elements: a large, semi-transparent exclamation mark on the left, a glowing blue circle with a red vertical line through its center, a glowing pink and purple area that looks like a stylized map or a data plot, and several glowing green and blue circles and lines. The overall aesthetic is futuristic and high-tech, with a color palette dominated by blues, greens, and pinks.

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

SIGNS that your client may be a fraudster

- Property owned by same person or family for several years
- Property may be mortgage free or may be subject to an institutional first mortgage and may have lots of equity, one or more recently discharged mortgages, or recent transfers. (Always request a PIN printout with full history of deleted instruments)
- Client is in a hurry and may discourage house inspection or appraisal
- Transaction closes, funds are withdrawn quickly and client disappears
- New client for you and/or new referral source if any, or no referral source
- Funds directed to parties with no apparent connection to borrower, property or transaction
- Client changes instructions regarding amounts or payees just before closing, or fails to bring in funds as promised
- Client does not care about property, price, mortgage interest rate, legal and/or brokerage fees
- Client does not appear familiar with property
- Client won't permit contact with prior lawyer or have a valid explanation why they are not using them
- Other party appears to control the client
- Client advises funds were paid privately. No funds pass through a lawyer's trust account
- One spouse or business partner mortgaging equity in property owned by both
- Client contact is only by email or text
- Client says title insurance for new mortgage is not required
- Client pushes for fast closing

SIGNS that the transaction is fraudulent

- Repeat, recent transfers, mortgages, or discharges on a single property or for a single client
- New referral source sending lots of business
- Use of Power of Attorney and/or funds directed to the Attorney instead of borrower
- Power of Attorney is not executed correctly
- Rental, Airbnb, and vacant properties are especially vulnerable
- Property listing expired without sale (i.e., sale may be unregistered)

- Recent registrations and discharges of private mortgages
- Property has been mortgage free, or subject only to an institutional first mortgage, but owner now registering a large mortgage in favour of private lender
- Property area and/or client residence is distant from your office
- Deposit not held by agent or lawyer
- Deposit is higher than normal and is paid directly to the vendor
- Small deposit relative to price
- May target long time owners or deceased, ill, or elderly who may be less alert to signs their identity is being stolen
- Rush deals, sometimes with promise of more
- Amendment to Agreement of Purchase and Sale reducing price, deposit, or adding creditors
- Sale is presented as a "private agreement" – no agent involved, or named agent has no knowledge of transaction
- Municipality or utility companies have no knowledge of client's ownership
- Client paying little or nothing from own funds
- Unusual adjustments in favour of vendor, or large vendor take-back mortgage
- Use of counter cheques

TIPS to help verify ID

- Is the person smiling in their ID photo? Smiling isn't allowed in government ID.
- Compare the images on the different pieces of ID – they shouldn't be the exact same image.
- Verify the date on the IDs. Does the person look like they've aged if the ID was from some time ago? If two pieces of ID are many years apart but the image doesn't reflect whether the person has aged, ask questions.
- Does the minister on the ID match who was in office at the time the ID was issued?
- Does the same picture appear on two different types of ID issued years apart?
- Is the signature similar to your client's?
- Is the client's name spelled differently in different types of documents/ID?

TIP

Advise lenders of recent activity on title, amendments to purchase price and significant changes in value in advance of closing.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAclaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 2023 Lawyers' Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers' Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.

WIRE FRAUD

Fraudsters are actively trying to direct lawyers and law firms to wire money to them – often through spoofed emails of people you know or hacking into emails.

Fraudsters have pretended to be:

- A lawyer in the firm directing staff to wire funds to a client or to complete a transaction
- A lawyer or staff acting for a seller in a transaction directing the other side to wire funds
- A financial institution directing wire payment to itself
- A client seeking payment of funds by wire



FRAUD WATCH

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

It starts with a hacked email system or impersonation using a lookalike fake email address. In the hacked email situation, the fraudster hacks into a lawyer or law firm email system, the client's email, or the email of others related to the transaction (or those copied in the email thread) and monitors the emails. The fraudster then sends wire transfer instructions from legitimate email addresses directing the wiring of funds to a particular account that the fraudster has set up or can access. When using a lookalike fake email address, the fraudster sends instructions that appear to be legitimate. In some cases, corporate records may be altered to add credibility to the scheme.

In recent cases reported to LAWPRO, a fraudster infiltrated a law firm email system, intercepted correspondence regarding a transaction, and then sent wiring instructions from a law clerk's email address. Since the wire instructions were being sent from a legitimate law firm email address, there was nothing to suggest anything suspicious from the email itself. Given that the fraudster could see incoming emails, only a separate means of verifying the instructions could stop the fraud.

TIPS

Verify instructions independently: Anytime you receive instructions to wire money to a bank account, contact the payee directly by an independent method (not replying to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information.

Double check email addresses to see if they are fake: Fraudsters will spoof an email address by creating a very similar looking address by adding an extra letter/number or changing a character(s). Having hacked into one account, they may spoof other email addresses that were in the email thread to increase your confidence that it is a proper message. It is important to carefully look at all the email addresses in the message. And remember, if the client's email account is compromised, it could be the fraudster sending you emails that look like they are coming from your client.

Implement two-factor authorization on your email systems: Two-factor authentication is an extra layer of security to make sure that people trying to gain access to your email are who they say they are. First, a user will enter their username and password. Then, instead of immediately gaining access, they will be required to provide another piece of information such as a code. Outlook and Gmail both offer two-factor authentication.

Regular training: Train staff in what to look out for and have regular discussions to reinforce the cyber security message. Someone from the office may see information or indications of fraud that others may not.

Educate your clients: Advise your clients of wire transfer risks. If you do not accept wire payments from them, tell them so that if they are approached to send funds by wire, they know it will be a fraud. If you do accept wire payments, explain your process and insist that they call you before they send you payments.

Examples of independent verification in action

Internal verification: The law firm partner purportedly emails from the firm address or a personal email address instructing you to wire money out of trust. Walk down the hall to the partner's office to ask if the partner sent the instructions. If the partner is out of the office, rather than replying to the email to confirm the direction (which will not help if the lawyer's email account has been compromised), call or text the lawyer.

Before wiring funds to another firm: If a lawyer at one firm emails wire instructions to a lawyer at another firm, that lawyer should call them to confirm the wire instructions. The same process can apply on receiving wire instructions from a financial institution or any other request for payment by wire transfer.

Before wiring funds to a client: A client may email you to instruct you to wire payments to an account. You can call the client to verify that the client's instructions are valid and that the client's account has not been hacked.

Firms that have implemented independent verification protocols have successfully blocked fraud attempts. A quick call to verify written wire payments might save you from being a victim of fraud.

Use this wire checklist: Funds Transfer Instructions Verification Checklist.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.

© 2023 Lawyers' Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers' Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.

PHISHING

Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Phishing is an email, text message or phone call that appears to come from a trusted source, institution, vendor or company, but is actually from a third-party impostor. Phishing emails, texts or phone messages are intended to trick you into giving fraudsters your information by asking you to update or confirm personal or online account information.



FRAUD WATCH

If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

A “spear” phishing attempt is a phishing message that is personally addressed to you, will appear to be from someone you already know (such as a senior partner at the same firm), and may include other detailed personalized information.

Fraudsters do their best to make phishing messages look official and legitimate. They will mimic real communications from the company or entity they are supposedly from by using the same layout, fonts, wording, message footers and copyright notices. They will often include corporate logos and even one or more links to the alleged sender’s real website.

Many phishing messages will include a link or attachment that you are asked to click so you can update your information. After doing so, the webpage or attachment you will see (which will also have text and logos to make it look official) will prompt you to enter your name, account number, password and other personal information – thereby giving it to fraudsters.

SIGNS

- The link you are asked to visit is different from the company’s usual website URL (place your mouse over the link and look at the taskbar in your window to see if the link matches. It should take you to the proper website)
- The main part of the sender’s email address is not the same as the company’s usual email address
- Spelling and grammar mistakes
- A sense of urgency – money has to be transferred quickly without the usual checks and balances
- The caller purports to be from the fraud prevention department of your bank, credit card company or other institution and needs you to provide them with key personal information over the phone
- Anyone asking for money – even if you know them
- The promise of receiving money or another big prize

Examples of phishing

- An irregular salutation from someone you are familiar with, such as “Hello Mr. Smith,” instead of “Hi Johnny.”
- An alert to reset your password or login to your account to review invoice or payment.
- “...your account has been hacked”: A request to update your information and go to a website or attachment, then prompting you to enter your account number, password and personal information.

- “...won a big prize,” “...refund to you”: A request to go to a website or open an attachment to claim monies.
- “...document I promised”: Posing as someone you know who may send you documents, a request to open an attachment.
- A call from a fraudster claiming to be from a legitimate corporate or government entity saying that you owe money or face civil/criminal charges.
- Requesting payment in Bitcoin, other cryptocurrencies or with gift cards.

TIPS

Never respond to requests for personal information in the mail, over the phone or online – just delete them. Never reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother’s birth name or birthday), even if they appear to be from a known or trusted person or business since this is probably the most common way that personal information is stolen.

Legitimate businesses should never send you an email asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don’t use the number in the email – it could be fake too!

Share this information with the lawyers and staff at your firm to make sure they will not fall for a spear phishing scam.

Follow firm processes and procedures for the review and approval of financial transactions – and don’t bypass them due to urgent circumstances. Never share confidential client or firm information without being sure it is appropriate to do so by getting confirmation from someone familiar with the file. Be on the lookout for and question any last-minute changes on fund transfers or payments.



If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca. Visit AvoidAClaim.com and click on “All Fraud Warnings” for a list of confirmed fraudsters.

© 2023 Lawyers’ Professional Indemnity Company.

LAWPRO is a registered trademark of Lawyers’ Professional Indemnity Company. All rights reserved. The material presented does not establish, report or create the standard of care for lawyers. The material is not a complete analysis of the topics covered, and readers are encouraged to conduct their own appropriate legal research.

Update about fund transfers



Raymond G. Leclair, Vice President, Public Affairs

There has been much written about how lawyers receive and deliver money from their trust accounts on behalf of their clients as part of a transaction. The issue comes down to ensuring good funds are being dealt with in order that value is exchanged. In Canada, our banking system works on the basis of trust, providing you with a provisional credit. Financial institutions (FIs) trust that the money destined for an account is good and thereby provide an immediate credit to the recipient for the designated amount, subject to the funds being settled or the credit reversed. Lawyers should be leery of exposing themselves to a situation where money they are dealing with is removed from their account by the FIs.

Existing Payment Channels

Payments Canada, which sets the rules for all fund transfers in Canada has, until recently, had two channels for the transfer of money – Automated Clearing Settlement System (ACSS) or the Large Value Transfer System (LVTS). Under the rules, only LVTS funds were irrevocable, so that once deposited into a lawyer's trust account, they could not be reversed. The problem is, our existing channels have very limited data transfer ability so, although we see a dollar in our account online, we do not know if it was funded via ACSS or LVTS.

Modernization of Payment Channels

Payments Canada has undertaken a modernization of its banking channels for three channels to better respond to modern transfer needs. In August 2021 it launched LVTS's replacement, Lynx. You noticed no difference in banking process due to the extensive planning undertaken. Lynx now has updated coding to allow more features to be added. One of the significant features will be the addition, this fall, of the ISO 20022 international data rich capability. Systems will be able to exchange much information and automatically update accounting systems without the need for manual entry for the transfer or receipt of funds. It is hoped that users will be able identify the channel used to confirm that the funds are irrevocable. The good news is that all three new channels will be dealing with irrevocable funds, but until all three are launched, we will continue to have various sources that may or may not be good irrevocable funds.

The second channel to be launched will be Real Time Rail (RTR), which is promoted to be for small dollars transactions, possibly up to \$50,000 initially and more later as FIs know more about possible fraud and other risks. In the USA and UK, where they have had these systems for some time, they are presently transacting much greater amounts. The third channel will replace ACSS with Retail Batch Payments. This, as presently, will process all online utility payments, cheques, payroll payments, debit and other similar transactions. The RTR is expected in June 2023 and the third some time after.

Lender-Lawyer Working Group

Lawyers should consider recent important developments that could improve their practices.

The Canadian Bar Association Real Property Section has been in discussions with the Canadian Bankers Association and its members to address issues of concern to both lawyers and lenders. The discussions have led to the creation of four important documents that can be found on the CBA Mortgage Instructions Toolkit ([MIT](#)) [webpage](#).

1. [Information Required from Lawyers for Wire Transfer of Mortgage Payout/Discharge](#), indicates which FIs (six at present) will accept a wire payment to discharge their mortgage and the details of where to send the payments and any relevant information required.
2. [Portal Providers for Mortgage Instructions and Discharge Statements at Lenders](#), provides lawyers with information on where and how to order a discharge of mortgage statement to receive it in a timely fashion for the closing (12 FIs presently).
3. [Phone Numbers and Web Page Addresses for Mortgage Prepayment Information for Borrowers](#), has information for clients who wish to exercise a prepayment prior to discharging their mortgage to benefit from a reduced penalty on the payout of their mortgage. It is important to note that this cannot be done in conjunction with the payout of the mortgage. (9 FIs presently)
4. [Best Practices Guide for Wires](#) is a document for lawyers to ensure the most efficient and timely processing of wires from their account and into the FIs or others account. FIs are promoting the use of wires and reducing or eliminating the use of certified cheques and bank drafts, but lawyers and clients are frustrated by the time delays in funds being credited to the recipient's account. These best practices seek to ensure the smooth and timely processing of wire instructions by the sending and receiving FI.

How to Identify Good Funds - The PRCN

How does one identify good irrevocable funds in your account for funds wired to you? Upon settlement of a Lynx Payment Obligation, Lynx will generate a unique confirmation number for that payment, the *Payment Confirmation Reference Number* (PCRN) and make it available to the Sending and Receiving Participants via the Lynx Web Client. Any Lynx Payment Obligation that Settles and has a PCRN assigned is final and irrevocable in Lynx.

The PCRN is available to the sender of the wire from their desktop after the wire has been sent. The sender has access to the FI's wire report and can send it to the other side to prove a wire has been sent. The PCRN is composed of 4-letters and 9-numbers, starting with "LVTS" followed by 9-digits. Any recipient of wired funds should be asking the sender to provide them with their sending receipt showing the PCRN. Lawyers receiving a wire should insist that their FI provide them with the PCRN they received with the wired funds. Matching the PCRN will confirm that the funds were transferred via Lynx, a secure channel which delivers irrevocable funds. A receiving FI participant must provide a payee with the PCRN if the receiving participant has the number, and it is requested by the payee¹. Lawyers should ask their FI to add the PCRN to the transaction so that it is visible from an online view of their trust account.

¹ Section 39, Canadian Payments Association By-law No. 9 – Lynx SOR/2021-182.

Caution – Fraud

One caution with wires is where they are destined to be deposited. A major source of fraud is seen all across the world by way of email fund redirection scams. This consists of fraudsters infiltrating email accounts, anyone's account in the email thread for that transaction, and monitoring for a payment event. The fraudsters then direct or redirect the payment of the funds from the legitimate account to their own. This might be in the body of an email or in an attachment, such as a direction to pay or a discharge statement from an FI. Fraudsters are very talented at reproducing very credible looking documents with their banking details instead of the ones you intended to benefit. To avoid being a victim of these email diversion scams, **call to verify the account information before you click to send the wire**, even for existing clients for which you transferred funds before. Also, warn your clients to be on guard and to call you before they send any wire after receiving an email or other request. LAWPRO has an article on how to [avoid being a victim](#) and what to do if you realize the money was sent to the [wrong account](#). In addition, we have a [CPD program](#) for you and your staff to watch and get CPD credits. **Be vigilant and educate everyone in the office. CALL BEFORE YOU CLICK!**

This resource is provided by Lawyers' Professional Indemnity Company (LAWPRO®). The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.

© 2022 Lawyers' Professional Indemnity Company (LAWPRO). All rights reserved.
* Registered trademark of Lawyers' Professional Indemnity Company



lawpro.ca
Tel: 416-598-5800 or 1-800-410-1013
Fax: 416-599-8341 or 1-800-286-7639
Email: practicepro@lawpro.ca

You transferred funds to the wrong account what now?



Fraudsters try to trick lawyers into wiring funds to an account that the fraudster controls. Sometimes, they succeed, and the funds get into the hands of criminals. What do you do then?

Below are some examples that have been reported to us:

1. A lawyer's office received a last-minute redirection of monies payable on the sale of a property, which was a spoofed email from fraudsters.

Without verifying the legitimacy of the redirection (other than by email with the fraudsters through the firm's law clerk), the funds were wired to the account of the fraudsters.

It was later determined that the email account of the law clerk had been compromised (likely by guessing an easy password or the clerk responded to a phishing email.) It was by hacking into the law clerk's email account that the fraudsters learned about the transaction and were able to

read and send genuine emails in furtherance of the fraud. The rules of the email account were re-written so that these emails were sent to folders other than the Inbox and Sent folders so the clerk wouldn't catch on.

2. A lawyer acted for the seller on a non-real estate transaction. The purchaser's lawyer attempted to cc them in an email, but sent the correspondence to an address that was one letter off from the real email address. In response, the purchaser's lawyer received instructions from this fraudulent email address with new trust account information and payment instructions.

The purchaser's lawyer thought this was suspicious, and called the seller's lawyer, who was able to confirm that the instructions were fraudulent. Independent verification saved the day.

It is unclear how the email hack occurred in the first place.

Three simple things you can do



1) Call before you click

If you receive instructions from a client, colleague, or other lawyer that involves a change in wire transfer account numbers or relates to a transfer of funds, always pick up the phone and call the individual to verbally confirm those instructions.



2) Train your lawyers and staff

Make sure all the lawyers and support staff in your firm are aware of the likelihood of spear-phishing attacks and the need to verbally confirm any changes to wire-transfer instructions received by email.



3) Warn your clients

Alert your clients of the dangers associated with wire fraud and advise them to verbally confirm with your firm any bank account details received by email.

What should you do if this happens to you?

What to do immediately



Contact the bank

The person who initiated the wiring of funds should immediately report the diversion to the bank from where the wire was initiated, requesting that they stop the wire. This is not always possible as wires are usually instantaneously dispatched and irrevocable, however, they may get caught in the financial institution's suspicious transaction filters and be pending.

Also, request that they contact the bank they sent the wire to and so on until the trail disappears or the money is found and frozen.



Report to LAWPRO

File a claim (lawpro.ca/claim) with LAWPRO as soon as possible. Provide all the relevant documents in your possession.



Alert your client

Notify your client of the diversion fraud immediately and request that they consider whether their systems have been compromised and they should seek the assistance of IT professionals.

The systems of third parties with knowledge of the transaction (e.g., in the email thread) may have also been compromised. Speak with your client about similarly alerting such third parties to the fraud, with your client's permission. If no system was hacked, consider if this was an inside job.

What to do next



Notify the authorities

Report the matter to your local police as a fraud, and the Canadian Anti-Fraud Centre.



Review your other insurance policies

Consider filing a claim under other policies you may have intended to respond to this type of risk, including but not limited to professional liability excess coverage, cyber insurance, commercial general liability, crime, computer fraud, and fidelity insurance. It is important that you obtain complete copies of all your insurance policies, including the declarations, policy wordings, and endorsements, for purposes of analyzing the potential coverages available to you. Your insurance broker may be of great assistance to you in this regard.



Seek IT help

Obtain the assistance of an IT specialist if it appears that your systems were hacked. Even if you received a spoofed email from a fraudster, the fraudster may have hacked into your systems to determine when to make the request for the wire transfer and which client representative to impersonate.

Be prepared to act quickly and work closely with your insurer(s) and other professionals retained. Cooperation between the parties is vitally important in these types of situations. ■



Tips to avoid being a victim:

Review our article [Wire Fraud Scams on the Rise](#): 5 Tips to Reduce Your Risk

Verify instructions independently: Anytime you receive instructions to wire money to a bank account and especially if the instructions are changing previous instructions, contact the payee directly by an independent method (not replying to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information.

Confirm instructions before a transfer: Advise your clients, or anyone you expect funds from, of the potential for a diversion attempt and to confirm the instructions before initiating the wire transfer.

Double check email addresses to see if they are fake: Fraudsters will spoof an email address by creating a very similar looking address by adding an extra letter/number or changing a character(s). Having hacked into one account, they may spoof other email addresses that were in the email thread to increase your confidence that it is a proper message. It is important to carefully look at all the email addresses in the message. And remember, if the client's email account is compromised, it could be the fraudster sending you emails that look like they are coming from your client.

Regular training: Train staff in what to look out for and have regular discussions and to reinforce the cyber security message. Someone from the office may see information or indications of fraud that others may not.

Stay up to date: For general cyber prevention tips, review our Cybersecurity and Fraud Prevention Tips, and subscribe to AvoidAClaim.com for fraud alerts.

Wire fraud scams on the rise:

5 tips to reduce your risk



LAWPRO is seeing an increase in phishing attacks against lawyers trying to trick them into wiring funds out of their trust accounts to the fraudster.

There are different ways that fraudsters are trying to direct lawyers and law firms to wire money to them. Fraudsters have pretended to be:

- A lawyer in the firm, to direct staff to wire funds to a client or to complete a transaction
- A lawyer or staff at a firm acting for a seller in a transaction, to direct the other side to wire funds
- A financial institution, to direct wire payment to it
- A client, to seek payment of funds by wire

It starts with a hacked email system or impersonation using lookalike fake email address. We have seen cases where the fraudster has hacked into a lawyer or law firm email system, the client's email, or the email system of others related to the transaction. In these situations, fraudsters monitor the emails and send wire transfer instructions from legitimate email addresses to send out wire payment instructions.

Follow the tips below to reduce your risk of falling victim to these increasingly sophisticated fraud scams.

Tip 1: Don't be spoofed: check the email address

Lawyers should use spam filters and check email addresses to reduce the risks posed by fraudsters impersonating lawyers, law firm staff, clients, financial institutions and others. For more tips to avoid spoof email addresses, see our article "Paying attention to the fraud behind the curtain."

Tip 2: Check documents to make sure they haven't been manipulated

When sending documents electronically, on receipt back, double check to make sure that key information, such as wire direction instructions, have not been manipulated. If you send out a document with wire instructions or other key financial information, you can check the document on receipt back that this information has not been changed.

Tip 3: Implement independent verification on all wire payments

Verify all directions to wire funds out of trust by confirming the instructions using a different medium than they were first received. This step can help reduce the risks posed by email hacks and cases where documents have been intercepted and manipulated.

Here are a few examples of independent verification in action:

- **Internal verification:** The law firm partner purportedly emails from the firm address or a personal email address instructing you to wire money out of trust. Walk down the hall to the partner's office to ask if the partner sent the instructions. If the partner is out of the office, rather than replying to the email to confirm the direction (which will not help if the lawyer's email account has been compromised), call or text the lawyer.

- **Before wiring funds to another firm:** If a lawyer at Firm A emails wire instructions to a lawyer at Firm B, the lawyer or staff from Firm B can call Firm A to confirm the wire instructions. The same process can apply on receiving wire instructions from a financial institution or any other request for payment by wire transfer.
- **Before wiring funds to a client:** As another example, a client may email you to instruct you to wire payments to an account. You can consider calling the client to verify that the client's instructions are valid, and that the client's account has not been hacked.

Firms that have implemented independent verification protocols have successfully foiled fraud attempts. A quick call to verify written wire payments might save you from being a victim of fraud.

Tip 4: Make fighting fraud part of your firm culture

Continue to train yourself and train your staff about fraud risk.

- For related CPD programming on fraud prevention, see our watch-anytime CPD programs on real estate fraud, bad cheque and cyber fraud. These programs are free for you, your colleagues and staff to view, and are eligible for LAWPRO's Risk Management Credit.
- Subscribe to avoidclaim.com for fraud warning updates.

Try incorporating these tips into your practice to help reduce the risk of fraud.

Tip 5: Stay on constant alert

Fraud prevention is not a one and done task. You and your staff need to be constantly vigilant. A few of the fraud scenarios we have recently seen include:

The fake instruction to wire funds

The fraudster sends instructions directing the wiring of funds to a particular account that the fraudster has set up or can access. In recent cases reported to LAWPRO, a fraudster infiltrated a law firm email system, intercepted correspondence regarding a transaction, and then sent wiring instructions from a law clerk's email address. Since they were being sent from legitimate law firm email addresses, there was nothing to suggest anything fraudulent from the email itself. Since the fraudster could see incoming emails, as described further below, only a separate means of verifying the instructions could stop the fraud.

Fake documents may strengthen the credibility of the direction to wire funds

We have seen instances where fraudsters have manipulated documents to alter wire payment instructions. We have even seen "secure" electronic documents prepared by

a law firm intercepted, manipulated to provide new account information for wiring funds, and then sent back to the firm.

Last minute changes are a red flag, but aren't the only flag

Often, the fraud may include a last-minute direction to wire funds to a new account. Any late change in payment instructions should be treated with caution, as this is a red flag of fraud. However, we have also seen cases where the fraudster has sent out the wire fund instructions early in the transaction.

Bottom line – there are all sorts of ways that fraudsters try to trick lawyers and their staff to wire funds to them. Lawyers and their staff should be on constant alert for these frauds and can adopt proactive measures to reduce the risk of these attacks. ■

Juda Strawczynski is Director of practicePRO

Three simple things you can do



Call before you click

Always independently verify wire instructions.



Train your lawyers and staff

Make sure all the lawyers and support staff in your firm are aware of the likelihood of spear-phishing attacks and the need to verbally confirm any changes to wire-transfer instructions received by email.



Warn your clients

Alert your clients of the dangers associated with wire fraud and advise them to verbally confirm with your firm any bank account details received by email.

Watch for real estate frauds involving private mortgages

In a hot real estate market fraudsters are even more motivated than usual – there is a lot of money to be had and lawyers are common targets. LAWPRO is seeing a significant increase in the number of real estate frauds involving private mortgages. The Toronto Police Service recently issued a news release about ongoing mortgage frauds targeting law firms.

The frauds we are seeing are incredibly sophisticated. In some cases, multiple fraudsters are in cahoots with each other participating as different parties to a transaction – i.e., the vendor, the buyer, the mortgage broker and/or the lender could be in on the fraud. Regardless of their role, the fraudsters will have very convincing fake versions of all the usual documentation that someone in their role would typically have.

On real estate deals involving private lenders, our experience is that the following circumstances should be considered red flags indicating a possible fraud. While every real estate deal is unique and may have unusual aspects to it, proceed with caution if you see transactions involving one or more of these red flags:

- 1. Large numbers of referrals from a new source:** After having someone approach you saying they were referred by a friend, that person then sends you a lot of business right away. Keep in mind, fraudsters will frequently take steps to make it appear they are coming from a trusted referral source, and they may also be familiar to you as they were a party in another transaction you were involved in.
- 2. Many similar transactions over a short timeframe:** Within a few weeks you are asked by the new referral source to do the same type of transaction repeatedly, after never having seen these types of transactions before. If anything, the value of the mortgages seem to grow with each transaction you work on.
- 3. “Rush” transactions:** A strong push to close from your client, and in particular the referral source, is a red flag that should not be ignored.
- 4. No funds go through a law firm trust account:** The parties insist on transferring the funds between themselves.
- 5. All of the funds are transferred outside of Canada.**
- 6. It appears that the homeowner didn’t actually receive funds or that no funds were advanced at all.**

7. The lender doesn't require post-dated cheques or pre-authorized payments or you have the sense that there is some informality to the deals, perhaps because the borrowers and lenders know each other.

8. The mortgage agent or broker isn't licensed with FSRA: A licensing search [can be done here](#).

9. The client does not want title insurance, despite the size of the loan: This is a strong indication of a fraud because fraudsters are trying to avoid the scrutiny that a title insurer will raise.

10. You receive or are instructed to write a "direction re funds" that has names you've never seen before with no apparent connection to the transaction or the property: If this happens shortly before closing it is almost certainly a fraud.

11. The current mortgage is being used to pay off one or more private mortgages that were recently registered, often for large amounts: If a borrower goes to another lawyer to act on a new mortgage and a new lender is involved, this has all the earmarks of being a "fake mortgage" fraud where the first mortgage is a fiction designed to induce the next lender to advance real funds.

12. ID and documents that don't look quite right: With the pandemic it's more likely that you will meet clients virtually and sign documents remotely. As noted above, fraudster clients will have government ID, property tax statements, corporate documents and everything else you would normally expect them to have. However, as these documents are fakes there may be something that doesn't look quite right with them. Perhaps the signature line isn't exactly where it would normally be. Perhaps the signature on the ID looks fine, but you notice that it isn't exactly the same as the signature on the documents you've asked the client to sign. Consider doing [a driver's license check](#) with the Ministry of Transportation.

Please share this information with your clerks as they are involved in parts of transactions you may not see and are ideally situated to identify red flags of potential fraud.

If you are an Ontario lawyer acting on a matter that you suspect might be a fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 or email practicepro@lawpro.ca. One of our Fraud Team members will talk you through the common fraud scenarios we are seeing and help you spot red flags that may indicate you are being duped. This will help you ask appropriate questions of your client to determine if the matter is legitimate or not. If the matter you are acting on turns out to be a fraud, we will work with you to prevent the fraud and minimize potential losses and claims costs.

What's wrong with this picture? Be on alert for fake IDs issued by different authorities or different times with identical photos

LAWPRO continues to see high levels of real estate fraud activity. Lawyers and real estate clerks should be on high alert for mortgage frauds.

In some instances, fraudsters appear to have used photo ID, issued by different authorities, or issued years apart, but where the documents used the same picture. In these cases, it's clear that a fraudulent ID is being used.

Also, as of 2012, Citizenship and Immigration Canada [retired the Citizenship Card](#) and replaced it with the Citizenship Certificate. You can find examples from the Government of Canada of both Canadian citizenship certificates and citizenship cards [here](#). If your client is using a citizenship card as ID, proceed with caution. Note that a re-laminated card is not valid as proof of citizenship, as it blurs the security features of the original and makes it difficult to detect fake cards.

Easy tips for verifying ID

- Is the person smiling? Smiling isn't allowed in government ID.
- Compare the images on the different pieces of ID – They shouldn't be the exact same image
- Verify the date on the IDs. Does the person look like they've aged if the ID was from some time ago? If two pieces of ID are many years apart but the image doesn't reflect whether the person has aged, ask questions.
- Does the minister on the ID match who was in office at the time the ID was issued?
- Is the signature similar to your client's?

And lawyers may also find it useful to review the Alcohol and Gaming Commission's [tip sheet](#) on how to ensure IDs are legitimate.

Be on alert for these and other red flags of fake IDs. To learn more about real estate fraud prevention, visit practicePRO's [Fraud Prevention page](#).

Title insurance matters: One of these things is not like the other

You may recall the title as a lyric from a song in a popular kids show many years ago, reinforcing the benefits of being aware and noticing differences.

This same lesson applies when comparing the legal protection coverages offered by other title insurers that compete with the Legal Service Coverage that's included in TitlePLUS policies. The differences are not always obvious and often discovered after a claim, where coverage is not what was expected.

Unfortunately, the lawyer could then be facing a lawsuit from their client, professional reputation damage, and a paid claim under their errors and omissions coverage that may trigger payment of a deductible and claims levy surcharges, often resulting in additional costs of \$17,000 or more over the next five years.

Real Estate remains one of the highest in claims by area of practice, with LAWPRO reporting that 27% of new claims in 2021 were real estate related. As such, it is important to protect yourself and your clients by understanding the differences in the various legal protection coverages offered by title insurers.

Did you know that many legal service endorsements are subject to the same exclusions, limitations, and exceptions contained in the title insurance policy? Be aware, as circumstances may arise where the lawyer is exposed to liability and could be sued.

Scenario- A lawyer closes a purchase of vacant land but misses adding one of the PIN's on a transfer due to an administrative error. When their client attempts to later sell the property, the missing PIN is discovered to be in the prior owner's name. The client submits a claim under the title insurance policy. However, since coverage is limited to the land as legally described in Schedule A, the claim is denied. Further, although the policy included a legal protection endorsement, it is subject to the same exclusions, conditions, and exceptions of the title insurance policy and unfortunately, there is no coverage.

This claim scenario would have been covered if the lawyer had the Legal Services Coverage included in a TitlePLUS policy, as the policy explicitly states there is coverage if the lawyer:

“Commits an error or omission in providing legal services for the Transaction for which liability is imposed by law.”

Other common policies offered by other insurers are those that cover smaller error and omissions claims but have monetary claim payout limits. Limits on the amount of the claim are always a cause for concern, particularly because the average cost of a real estate claim is \$34,000. A TitlePLUS policy has no limitations on payouts other than the policy amount, and the industry standard inflation protection limit on the original policy amount.

Lastly, some legal service options require you to purchase the coverage each time you order a policy. This additional step can be easily missed, especially in a time of competing priorities and busy days. With a TitlePLUS policy, there are no extra steps. Legal Services Coverage is automatically included in most policies - no missed coverage, no extra input, and no extra charge.

TitlePLUS Legal Services Coverage stands on its own and is the coverage many legal professionals rely upon and trust. Visit titleplus.ca to learn more about the many new changes at TitlePLUS including TitlePLUS Legal Counsel Fees.

To learn about the many scenarios where TitlePLUS Legal Services Coverage would respond, watch this video <https://www.youtube.com/watch?v=nOAzv5U044U> ■

Lisa Burdan is Sales Manager, TitlePLUS at LAWPRO

Resources and CPD for Lawyers

| LAWPRO's Practice Management Resources | |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>LAWPRO's Practice Tips Sheets</u> | Helpful tip sheets organized by type of practice error which provide ways to avoid common mistakes. Includes tips on delegation, managing deadlines, conflicts of interest, and other categories. |
| <u>Sample fake IDs, documents, and cheques</u> | Avoidaclaim's collection of sample fake IDs, documents, and cheques from actual fraud attempts |
| <u>Table of Ontario Mentoring Programs</u> | A helpful table of various mentoring programs offered by legal groups and associations for Ontario lawyers |
| <u>Technology Products for Lawyers and Law Firms</u> | A helpful table of software solutions for lawyers |
| Additional resources | |
| <u>Canadian Anti-Fraud Centre</u> | The Canadian Anti-Fraud Centre collects information on fraud and identity theft. We provide information on past and current scams affecting Canadians. |
| <u>LSO: Client identification and verification requirements</u> | Law Society of Ontario bylaws and guidance regarding the identification and verification of clients. |
| <u>LSO: Red flags for fraud in real estate transactions</u> | Law Society of Ontario guidance on red flags of fraud during real estate transactions. |
| Additional CPD for lawyers | |
| <u>Survival tips to prevent fraud</u> | This pre-recorded program from December 2022 draws on actual frauds and close calls and reviews the most recent fraud efforts targeting lawyers, law firms and their clients. It provides practical tips to help lawyers manage these risks. |
| <u>Avoiding the wire fraud nightmare – What you need to know to protect yourself and your clients</u> | In this pre-recorded program from October 2021, hear from the experts about the latest wire scams against law firms and their clients and how to stay a step ahead. You will learn tips you can easily implement in your practice to help prevent wire fraud and other cyber dangers. This is a must-view program for lawyers, their clerks and staff to understand and combat wire fraud. |

SPEAKER BIOS

Adkin Holder



Adkin Holder is a Detective with the Toronto Police Service Financial Crimes Unit where he primarily investigates mortgage frauds.

He has attended courses at the Canadian Police College on mortgage frauds, forensic interviewing and investment frauds. Adkin has provided mortgage fraud training to police officers, mortgage brokers, lawyers, title insurance and bank employees.

Adkin has been a police officer for 32 years and has worked in a variety of areas including uniform, school liaison, plainclothes, undercover and criminal investigations.

Ellie Persichilli



Ellie Persichilli is a Claims Counsel at the Lawyers' Professional Indemnity Company (LAWPRO), where she handles professional negligence claims against lawyers in various areas of law. Ellie is a member of LAWPRO's fraud response team and has handled numerous fraud related claims. As a member of the TitlePLUS claims group, Ellie also handles title insurance claims.

Ellie was called to the bar in 2010. Prior to joining LAWPRO, Ellie practiced insurance defence litigation for several years.

Nadia Dalimonte



Nadia Dalimonte, Manager, TitlePLUS Claims & Counsel, LAWPRO

Nadia Dalimonte's role includes managing TitlePLUS title insurance and professional liability claims for lawyers. Since beginning her career with LAWPRO in 2006, Nadia has had the opportunity to manage cases in a wide variety of areas of law, levels of complexity, and forums, including actions, applications, class actions, and caution hearings. With extensive real estate experience, Nadia has developed special expertise in resolving complex coverage, fraud, and title insurance related claims.

A committed member of the wider legal community, Nadia has shared her claims experience and risk management tips with the legal profession through articles authored for LAWPRO. She is also a member of LAWPRO's fraud response team that provides guidance and support to Ontario lawyers.

Nadia obtained a BBA from the Schulich School of Business in 2003. Her LLB is from Osgoode Hall Law School, and she was called to the bar in 2007.

Ray Leclair



Ray Leclair is Vice President, Public Affairs, responsible for government relations efforts at LAWPRO.

Formerly General Counsel for the Kanata Research Park Corporation, a development company and major commercial landlord in Ottawa, Ray has practised in both major national law firms and as a sole practitioner, and was a part-time professor at the University of Ottawa Law School and Cité Collégiale instructing the French language portion of the real estate law course. He also served for 15 years as the Ottawa senior instructor for the French and English Real Estate Sections of the Bar Admission Course and member of the Law Society of Upper Canada's Solicitor Advisory Group, Licensing Process.

Called to the bar in 1984, Ray is Past-Chair and remains an active participant of both the National Real Property Section of the Canadian Bar Association and of the Real Property Section of the Ontario Bar Association, past Co-Chair and remains a member of the Working Group on Lawyers & Real Estate, and President of the Ontario Real Estate Lawyers Association (ORELA). Member of the Ontario Bar Association Council, past executive member of CBA's National Sections Council, past member of its budget committee and formerly Vice President of the North American Bar-related® Title Insurers, past President of the Advisory Committee for the Cité Collégiale Legal Assistants Program. Ray is a member of the Board of Directors and President of a high-rise condominium corporation in Toronto and has volunteered as Manager of the fundraiser TOM* MensFashion4Hope and a VIP & Sponsor Relations Officer for semi-annual Toronto Men's Fashion Week (TOM*). Ray is and has been a frequent speaker/presenter, in French or English, in numerous programs on various real estate and other law related topics in Canada and the United States.

Shawn Erker



Shawn Erker is the Legal Writer and Content Manager in the Claims Prevention & Stakeholder Relations department at LAWPRO. Prior to joining LAWPRO, Shawn practised as a civil litigator in British Columbia in a full-service national firm after clerking at the British Columbia Court of Appeal. He graduated from UBC Law where he served as Editor-in-Chief of the UBC Law Review.