



Toronto Lawyers ASSOCIATION 

Avoiding the wire fraud nightmare - what you
need to know to protect yourself and your clients

December 2, 2021

brought to you by Title 

Program materials



Be ready with an incident response plan.....	1
Cybersecurity and fraud prevention tips.....	3
Does your firm need cybercrime insurance?	4
Fraud fact sheet: Cybercrime and bad cheque scams	6
Fraud fact sheet: Real estate	10
Putting the fire out: Dealing with the stress of a malpractice claim	14
Wire fraud risk on the rise: 5 tips to reduce your risk	16
What to do if money is diverted to a fraudster's account	19
Speaker bios.....	21

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

© 2021 Lawyers' Professional Indemnity Company (LAWPRO). All rights reserved.
® Registered trademark of Lawyers' Professional Indemnity Company

Prevent wire fraud



Call before you click



Train your staff



Warn your clients



Be ready

with an Incident Response Plan

Because a cybercrime attack can cause irreparable harm, law firms should be prepared to take action immediately. Being able to do this requires an Incident Response Plan, or IRP.

An effective IRP can put a firm in a position to effectively and efficiently manage a breach by protecting sensitive data, systems, and networks, and to quickly investigate the extent and source of the breach so that operations can be maintained or promptly restored. Many firms design IRPs so that they address inadvertent breaches as well – for example, a lost USB key, or a misdirected email. An IRP can help avoid many of the pitfalls of an ad hoc response, such as slow containment (leading to more widespread impacts and damage), lost productivity, bad press, client frustration, and even malpractice claims or discipline complaints.

A complete IRP addresses the detection, containment, and eradication of a cyber breach, recovery of normal operations, and follow-up analysis. When creating your plan, we encourage you to address the following issues:

Build an IRP team.

The size and composition of the team will vary depending on the size of your firm, but teams of all sizes should have a leader. If the firm employs IT staff, they will be key members of the team. There should also be representation from senior management, from the firm's main practice groups, and from the communications and human resources departments, if these exist. Roles and responsibilities for all team members should be documented in the firm's plan. Where necessary, team members should be trained in the procedures required under the plan.



Establish priorities.

In the event of a cyber attack, what should the firm's first priorities be? Presuming no staff are in physical danger, a firm's first priority is often protecting the confidentiality of client information. Identify and rank your priorities (be sure to include the need to notify LAWPRO and/or your cyber risk insurer), and design your response accordingly. For example, the IRP may specify the order in which servers and services will be restored. Ensure that business objectives and priorities are met while negative effects on users are minimized.



Be ready to investigate.

To be able to respond appropriately, you will need to understand the nature and extent of the cyber attack or breach. If you have an IT department, there may be individuals on your staff with sufficient knowledge of forensic investigation to isolate the problem. Firms without an IT department should identify, in advance, the provider that would be contacted to investigate a breach, and record this contact information in the IRP.

Remember – non-IT staff may be the first to discover a cyber incident. Encourage your staff to report indications of trouble. See “How to recognize your computer is infected with malware” on page 16. In the event that a third party (for example, a client) detects a problem – for example, by receiving a phishing email – you should ensure that it’s easy for third parties to identify the appropriate contact person to whom to report the issue.



- log and audit processes;
- use automated intrusion detection systems and a secure firewall; and
- use secure mechanisms for communication.

Have a containment plan.

As soon as a problem is identified, be prepared to make decisions about how to contain damage. IRP team members should have authority to lock down accounts and change passwords, to determine whether and which systems need to be shut down or isolated, and how to decide when it’s safe to restore operation. It is useful for IRP members to document events and responses as they unfold – this record will be invaluable for the analysis of the attack once it’s over.



Have a communication plan.

Prompt and effective internal communication is essential to an effective incident response. The IRP should have a “call tree” with current contact information that will govern communication between staff should an incident occur when many are out of the office. Contact information for outside IT and other service providers should be documented in the plan and kept up to date. It is useful, where the firm is trying not to immediately tip off the intruder, to avoid email communications – in these cases, phone, text, BlackBerry Messenger, or fax communication should be preferred.



It is useful to have a list ready in advance of outside parties who should be notified, along with current contact information. These parties may include the police, clients, insurers, credit card companies, a public relations firm, and your Internet service provider (be sure you have a current contact list saved outside your usual system).

Be technically prepared. While the details of breach prevention protocol are beyond the scope of this article, some of the basic protective steps firms can take are:

- create an inventory of computing resources;
- back up systems and data daily;
- create an offsite record, updated regularly, of client and service provider contact details;
- create a software archive and a resource kit of tools and hardware devices;
- create redundancy capacity for key systems;
- prepare a checklist of response steps;

Effectively eradicate threats.

Once the damage is contained, the firm will need to be prepared to resolve the incident by identifying and correcting all breach points, and eradicating all intruder leavings (malware, etc.). This is a complex and sometimes tedious process that may require external help.



Analyze the incident and the effectiveness of your response to help prepare for the next event.

Once the threat has been contained and then eradicated, the incident should be thoroughly analyzed. How did the intruder get in? What was he/she looking for? What did he/she accomplish?

You should also review the effectiveness of the firm’s response. If there were any areas of confusion or parts of the plan that didn’t work well, consider how those aspects of the IRP might be improved, so you’ll be better prepared for the next attack when it happens.

While it takes some time and effort to create an IRP, being ready to respond to an incident in a coordinated and effective way can reduce damage to records and systems and minimize the impact of a cyber attack on your firm’s productivity. Because the panic associated with a crisis can lead to errors and missed steps, it is much better to have thought these issues through calmly beforehand. ■



Nora Rock is corporate writer and policy analyst at LawPRO

Phishing attacks and other forms of cyberfraud are an increasingly common source of loss for lawyers. Our constantly changing technology, and the changing tactics used by fraudsters, require constant vigilance and adaptation. Here are a few tips to keep your and your clients' information secure and prevent fraud.



1. IMPLEMENT ROBUST COMPUTER AND PHONE SECURITY PRACTICES

- Ensure that you have robust password protocols, including training your staff to use complex alphanumeric passwords along with two-factor authentication.
- Make sure computers have adequate anti-virus protection and are regularly updated. Use end-to-end encryption when transmitting data over the internet.
- Implement regular data back-ups to a secure server or storage to prevent fraudsters from holding your data hostage following a ransomware attack.
- Consider trying penetration testing tools to assess network vulnerabilities.



2. PROVIDE STAFF TRAINING ON IDENTIFYING BAD CHEQUES AND PHISHING MESSAGES

- Train yourself and your staff to notice red flags associated with bad cheques and phishing attacks.
- Visit the practicePRO [fraud prevention webpage](#) for the LAWPRO Fraud Fact Sheets and tips for identifying fraud



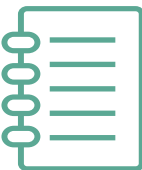
3. VERIFY INSTRUCTIONS RECEIVED BY EMAIL

- Spear-phishing attacks will often involve email instructions that appear to have originated from a client, law firm on the other side of a transaction or other trusted party, but are deceptions by fraudsters. Before following requests that come by email, particularly involving the transfer of funds, call the party providing those instructions on the phone to confirm their accuracy.



4. ENSURE YOU HAVE SUFFICIENT CYBER INSURANCE

- Malpractice insurance only protects certain cyber risks and firms should not assume their general liability insurance will cover all cyber risks. Consider whether a policy directly addressing the costs associated with cyberattacks is appropriate for your practice.



5. MAKE OR UPDATE YOUR INCIDENT RESPONSE PLAN

- Because a cyberattack can cause significant harm, law firms should be prepared to take action immediately. An Incident Response Plan addresses the steps for the detection, containment, and eradication of a cyber breach, recovery of normal operations, and follow-up analysis. LAWPRO's resources on [incident response plans](#) can help you get started.

LEARN MORE ABOUT CYBERSECURITY AND FRAUD PREVENTION TIPS:
See the practicePRO [fraud prevention webpage](#) and the [cyber dangers webpage](#).

Does your firm need cybercrime insurance?

In a study titled *The Cost of Cybercrime*¹, Accenture surveyed 254 companies in seven countries. Over the course of five years, the study revealed a 62 per cent increase in cybercrime attacks. Data breaches during the same period doubled to 130 per year.

Accenture noted that while not every security breach results in a loss, the two most costly types of breaches (malware and web-based attacks) can take days (up to 23 days in the case of ransomware) to resolve and cost firms over \$2 million per incident on average.

LAWPRO first suggested that lawyers consider cyber insurance in the December 2013 issue of *LAWPRO Magazine*. In the article *Cyber Risk Options: Do You Have the Coverage You Need?* firms were advised that their general liability insurance policies (intended to cover bodily injury and property damage scenarios) may offer only a limited amount of coverage for cyber-related exposures. These policies were not designed to cover loss of data or a breach of a law firm network.

In addition, the cyber coverage under the LAWPRO policy is subject to eligibility criteria and a modest sublimit. Says LAWPRO's Assistant Vice President, Underwriting, Victoria Crewe-Nelson: "the LAWPRO cybercrime coverage relates to professional services. If, for example, a loss (e.g. corrupted accounting data, theft from the general account) does not relate to the provision of professional services, LAWPRO coverage

would not apply. To prepare for this kind of risk, lawyers should consider exploring broader cyber coverage available in the marketplace."

The rapid growth of cyber insurance

According to Integro Insurance Brokers of Toronto, 10 years ago there was almost no familiarity with or interest in cyber insurance. Now, despite widespread awareness of the risks, many firms still feel their own IT departments can handle cyber dangers.

In light of recent high profile security breaches, demand for cyber insurance has grown 'exponentially.'² From 2015 to 2016, the Risk Management Society's worldwide *Cyber Survey*³ found a 30 per cent increase in companies procuring stand-alone cyber insurance.

The numbers in Canada may not be quite as high. According to a 2017 FICO-sponsored survey of 350 international organizations (including Canadian law firms) 36 per cent of polled Canadian companies have no cybersecurity insurance. Of those that do, less than 20 per cent believe that the insurance will cover all cyber risks.⁴

What are "professional services"?

The 2018 LAWPRO policy provides the following definition:

PROFESSIONAL SERVICES means the practice of the law of Canada, its provinces and territories, where conducted by or on behalf of an INSURED in such INSURED'S capacity as a LAWYER or member of the law society of a RECIPRO-CATING JURISDICTION (not as a member of the Barreau du Québec), subject to Part II Special Provision A; and shall include, without restricting the generality of the foregoing, those services for which the INSURED is responsible as a LAWYER arising out of such INSURED'S activity as a trustee, administrator, executor, arbitrator, mediator, patent or trademark agent.

¹ accenture.com/t20170926T072837Z_w_/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

² canadianlawyermag.com/author/michael-mckiernan/demand-for-cyber-insurance-on-the-upswing-3400/

³ rims.org/aboutRIMS/Newsroom/News/Pages/2017CyberSurvey.aspx

⁴ canadianunderwriter.ca/insurance/36-polled-canadian-firms-no-cyber-security-insurance-fico-1004114548/

©2018 Lawyers' Professional Indemnity Company.

This article originally appeared in LAWPRO Magazine (Vol. 17 no. 1).

It is available at www.lawpro.ca/lawpromag

The practicePRO and TitlePLUS programs are provided by LAWPRO

These statistics reflect the experience of larger companies, but Crewe-Nelson warns that smaller firms should also take heed: “Cybersecurity at smaller firms may be less sophisticated and there are fewer statistics regarding how many are purchasing cyber insurance coverage. But small firms are at the same risk as their larger counterparts.”

Where do breaches occur?

Some breaches happen at the technology front end: through email, laptops, mobile devices, and desktops. Many hackers find these to be the a firm’s weakest link because they depend on employees’ diligence in following proper security procedures.

Other breaches target the back end of a firm’s IT network: storage, servers, backup systems, and wireless encryption. In addition, new security problems may soon emerge in the context of the internet of things, increased cloud computing, and the constant expansion of social media. Hackers are continually adapting their methods to new technologies. Visit practicepro.ca/cyber to read more about the cyber dangers targeting law firms.

What does a typical cyber insurance policy cover?

First, there is no such thing as a “typical” policy: different insurers offer different products and a wide range of sublimits. If the insurance is purchased through a group plan, the underwriting might be straightforward, but will typically include only modest limits. A more bespoke insurance product may require detailed underwriting, explains Crewe-Nelson, and may include multiple lines of coverage with corresponding separate sublimits. “Consider, as an example,” says Crewe-Nelson “what counts as a business interruption once a cyber-attack occurs: how long does a system have to be down before coverage kicks in, and how soon afterwards will coverage be exhausted?”

Coverage can also include both first-party losses (losses suffered directly by the firm that purchases the policy) and third-party losses (losses suffered by a firm’s clients as a

result of a breach). It can be made available for scenarios in which the cause of the incident is internal (staff or lawyer at the firm) or external hackers.

Coverage can extend to:

- Specified costs associated with an attack, for example:
 - Lost income and operating expenses related to a loss of business due to a cyber-attack or pre-emptive network shutdown; and/or
 - Hardware, software and data recovery costs
- Payments demanded for cyber extortion/ransomware
- Crisis management expenses, such as IT forensics costs and public relations spending
- Defence expenses related to regulatory fines or penalties
- Measures to help prevent a breach
- Technical assistance to respond to an attack or breach
- Assistance with the aftermath of a breach

Why aren’t more companies buying cyber coverage?

Integro states that some of the barriers to wider uptake of cyber insurance policies include confusion around how cyber insurance premiums are set, difficulties in adapting traditional insurance policy language to modern cyber threats, and a lack of data and loss history to make reliable actuarial calculations.

Also, it remains unclear how these policies will respond to claims, and what kinds of breaches will be excluded from coverage. For example, the wording in some policies could be interpreted as excluding breaches caused by human error, mechanical failure or incompatible software. As the market matures and decisions on cyber coverage are made by the courts, there may be more clarity for both law firms and insurers. In the meantime, firms are advised to ask questions of their insurance brokers: it’s worth an investment of time and effort at the outset

to get as much clarification as possible when comparing policies from different insurers.

Some insurers offer prevention resources

It can be challenging for medium and small firms to develop and implement their own cybersecurity policies and infrastructure. Keeping up with the constantly evolving nature of cyber risk can be beyond the expertise of a typical law firm IT department. In addition to coverage for financial losses, a number of insurers provide access to broader technical support similar to that offered by cybersecurity firms (see “Outsourcing Your Firm’s Cybersecurity” available on practicepro.ca). Such services may include:

- Around-the-clock access to cybersecurity specialists
- Training for firm staff to help prevent a breach
- Assistance with notifying clients of the breach

Crewe-Nelson notes that access to a breach coach can be a significant asset in cases of cyber extortion and ransomware: “The coach can help determine whether the ransom should be paid, and can coach staff about how to do it. There are examples of companies phoning up and asking if they can pay for the return of just certain key documents, and being told no. Once the full ransom is paid, the company realizes that the criminals have withheld the sensitive information that the firm helped identify – and that they are now demanding a premium for those.”

If your Ontario firm has not yet explored cybersecurity coverage options, we urge you to do so. The cost of a cyber-breach goes beyond the financial losses of stolen funds, damage to equipment and lost income. There is also the damage to a firm’s reputation and the loss of confidence of its clients. With many insurers now offering cyber risk policies, firms have many options to tailor a policy to their specific needs. ■

Tim Lemieux is Claims Prevention & Stakeholder Relations Coordinator at LawPRO.



FRAUD FACT SHEET

CYBERCRIME AND BAD CHEQUE SCAMS

Cybercrime and bad cheque scams are some of the most common, significant and costly problems for lawyers and LAWPRO®. Fraudsters are successfully duping lawyers, paralegals and law clerks.



Don't be complacent and think you will never be fooled

These frauds are very sophisticated. The matters will look legitimate, the fraudsters will be very convincing and the client ID and other documents you get will look real. Fake cheques are printed on real cheque stock.

Phishing emails will appear to come from your bank and other legitimate companies. Fraudsters will email you posing as colleagues and clients, and corporate records may be altered. Two or more people can collaborate on both sides of a transaction to make the scenario more convincing. Some may come to your office in person, or follow up with you over the phone.

If you aren't completely sure a matter is legitimate, terminate the retainer. Don't be sucked in by your emotions or a strong desire to help. Don't let the lure of a generous fee cause you to ignore your concerns as to the legitimacy of a matter. 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.

What to do if you have a suspicious matter?

Proceed with caution if you have even the slightest suspicion that the matter you are handling isn't legitimate.

1. Look for the red flags of a fraud. See the lists on the following pages.
2. Ask questions and dig deeper, especially if the facts don't add up or are inconsistent. See the next page for a list of things you can do.



Visit the **AvoidAClaim.com** blog to search names and email addresses from the frauds reported to LAWPRO. Click on "All Fraud Warnings" to see a full listing of names of confirmed fraudster clients. If you still aren't sure the matter is legitimate, call LAWPRO at 1-800-410-1013. Our experience with multiple frauds can help determine if you are being duped. If the matter turns out to be a fraud and there is a potential claim, we will work with you to prevent the fraud, if possible, and to minimize potential claims costs.

Report obvious frauds to LAWPRO

Help us help other lawyers by sending obviously fraudulent messages, scans of identification and other documents provided to you to **fraudinfo@lawpro.ca**

Get fraud warnings & updates from AvoidAClaim.com blog

Wondering if you've been duped or your potential client is a fraudster?

For regular updates on fraud and claims prevention, subscribe to the email updates from LAWPRO's AvoidAClaim.com blog.



Do you practice in real estate? See the Real Estate Fraud Fact Sheet at practicepro.ca for common types of real estate fraud, red flags, and tips on how to protect your law firm and you.

Bad cheque scams

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

The red flags of a bad cheque scam

- Initial contact email is generically addressed (e.g., “Dear attorney”) and/or BCC’d to many people.
- The name and/or email address in the FROM line is different from the name and/or email address of the person you are asked to reply to in the body of the email.
- Client uses one or more email addresses from a free email service (e.g., Gmail™, MSN®, 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.net).
- Email header indicates sender is not where he/she claims to be.
- Client raises issues of conflicts or payment of a retainer.
- Client is new to your firm.
- Client is in a distant jurisdiction.
- Client says he prefers 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 shows up and wants the matter completed around or on banking holidays.
- 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 or bank draft arrives at your office in a plain envelope and/or without a covering letter.
- 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 an offshore bank account based on changed or urgent circumstances.
- Client and others involved don’t seem concerned if shortcuts are taken.
- Some or all of the payment is going to third party who appears unrelated to the matters.

Due diligence on a suspected fraudster

Take these steps to cross-check and verify information provided to you by the client:

- Cross-check names, addresses, and phone numbers of the client and other people/entities involved in the matter on Google® and other search engines. (To find exact matches, enclose your search terms in double quotes.)
- Do reverse searches on phone numbers.
- Look up addresses using Street View™ in Google Maps™.
- 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.
- Contact the company to confirm it is expecting debtor’s payment or business loan.
- Hold the funds until your bank confirms the funds are “good” by contacting the other bank, and have the bank confirm, in writing, that it is safe to withdraw from the deposit.

Common types of bad cheque fraud

Equipment/inventory purchase fraud

- Targets business lawyers.
- Fraudster will ask you to handle a purchase (e.g., a dredger).
- Purchase funds are coming from fake buyer.

Business loan or debt collection fraud

- Targets litigators.
- Fraudster will ask for help with a commercial debt or personal business loan collection.
- Debtor will pay up with little or no pushing.

Divorce settlement fraud

- Targets family lawyers.
- Fraudster will ask you to help with collection from ex-spouse, often further to a “collaborative settlement agreement.”
- Ex-spouse will pay up with little or no pushing.

Real estate deposit fraud

- Targets real estate lawyers.
- Contacts realtors, who put fraudsters in touch with real estate lawyers.
- Overseas client sends lawyer a deposit cheque for a property they saw online.
- Fraudster then backs out of the deal, and asks lawyer to wire the deposit funds back (minus any fees and penalties).

Intellectual property rights fraud

- Targets IP lawyers.
- Fraudster seeks damages from a breach of a trademark or copyright agreement.
- The company in breach will pay up with little or no pushing.

Phishing scams

Phishing involves the use of an email, text message or phone call that appears to come from a trusted source or institution, vendor or company, but is actually from a third-party impostor. Phishing messages are intended to trick you into giving fraudsters your information by asking you to update or confirm personal or online account information. Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Fraudsters cast a wide net and make thousands of phishing attempts – they only need one or two dupes to make it pay off.

Phishing is also becoming more sophisticated. Fraudsters can conduct research about you through the internet and other means to obtain information unique to you, including your practice area, your clients, and your personal life. 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, etc. as official messages. They will often include corporate logos and even one or more links to the alleged sender’s real website.

How to spot phishing messages

Phishing scams work because they are convincing and prey on your trust of the source. If you get a phishing message from a bank and you don’t have an account there, you aren’t likely to fall for the scam. However, if you have an account at that bank, the message may look legitimate to you and you are more likely to fall for the scam. 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.

Red flags

- 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 promise of receiving money or another big prize.
- Anyone asking for money – even if you know them.



Some types of phishing

- An irregular salutation from someone you are familiar with, such as “Hello Mr. Smith,” instead of “Hi Johnny.”
- “...suspicious transaction,” “...account outstanding”: An alert to reset 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.

Don’t take the bait

Never respond to phishing requests for personal information in the mail, over the phone or online. Most importantly – this is probably the most common way that personal information is stolen – never ever 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. 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!

All staff can be targeted

Educate 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.

Inside job: Fraudsters in your law firm

Not all fraudsters are strangers. Even partners, associates, law clerks or other employees may turn to fraud because of financial pressures from a divorce, over-extended lifestyle, failed business venture, or other personal crisis.

Red flags

- 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

Preventing insider fraud

- 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.

When a fraudster emails you instructions in the name of the client, counsel, or staff

Beware of fraudsters who are hacking into email accounts of third parties including clients, lawyers and staff within your firm, opposing counsel, and opposing parties. The fraudster will monitor the emails of the hacked party, and figure out that there is a legal matter involving you. When the matter is completed and money is about to change hands, such as following a litigation settlement, real estate closing, or other transaction, the fraudster, posing as

the legitimate party awaiting the funds, will send an email to you redirecting where the funds should go. If you follow through, the money will go to the fraudster.



A simple prevention tip when money is requested is to always call your client directly to confirm instructions, especially when instructions change at the last minute.

Red flags

- Funds requested are to be sent to an account or address that is not associated with the client/lawyer/party.
- Writing style, grammar, or spelling mistakes.

Maintain good password hygiene

We all have more passwords than we can remember, which can make it easy to be lazy. We may use obvious and easy-to-remember passwords – even the word "password" itself. Or worse: we don't use them at all. Bad password habits are often one of the weakest links in data security schemes. Cyber criminals know and exploit this fact. For this reason it is critical that all lawyers and staff in a law office use passwords, and use them properly.

Password tips

- Never ever tell anyone your passwords.
- Never write down your passwords, especially on your monitor.
- Don't save passwords on your computer hard drive.
- Use biometric scanners like fingerprint, voiceprint, facial, and eye scanners.
- Don't use the same password for everything.
- Change passwords on important accounts on a regular basis.
- If you suspect you've been hacked, change your password immediately.
- Don't use the "remember password" feature in your browser and in other applications.
- Create a password using four unrelated words.



Password managers can help. A password manager generates unique randomly generated passwords and stores them in a single place. You need to remember only one password to access the application. While using a password manager is not foolproof, it may be safer than not using one.



Use two-step authentication where available. When offered and enabled, this means you will need two ways to access an account. Typically this means using a password in conjunction with a code texted to your cell phone that is generated at the time you are seeking access.

This information bulletin is published by LawPRO to provide lawyers and law firm employees with an overview of some common types of fraud, and to provide practical advice on ways to minimize their exposure to fraud-related claims. 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. The comments in this publication are intended as a general description of the insurance and services available to qualified customers through LawPRO. Your policy is the contract that specifically and fully describes your coverage and nothing stated here revises or amends the policy.

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

© 2018 Lawyers' Professional Indemnity Company (LawPRO).
All rights reserved.
* LawPRO and the LawPRO logo are registered trademarks of Lawyers' Professional Indemnity Company. All other trademarks are the property of their respective owners.

AvoidAClaim.com

LawPRO

LawPRO
TitlePLUS

@LawPRO
@practicePRO
@TitlePLUSCanada

LawPRO insurance
TitlePLUS Home Buying
Guide – Canada



Printed on recycled paper. This product can be recycled.



FRAUD FACT SHEET

REAL ESTATE

Avoid being duped



Fraudsters are successfully duping lawyers and law clerks using ID impersonations, property flips, value fraud, phishing scams, and more. Real estate frauds can be simple scenarios or sophisticated ones. The matters look legitimate and the fraudsters are convincing. There may even be two or more people collaborating on both sides of a transaction to make the scenario more credible.

Ultimately, if you aren't completely sure a matter is legitimate, terminate the retainer. Don't be sucked in by your emotions or a strong desire to help. Don't let the lure of a generous fee cause you to ignore your concerns as to the authenticity of a matter. If it looks too easy or sounds too good to be true, it probably is.

What to do if you have a suspicious matter?

Proceed with caution if you have even the slightest suspicion that the matter you are handling isn't legitimate.

1. Look for the red flags of fraud, many of which are described on the following pages.
2. Ask questions and dig deeper, especially if the facts don't add up or are inconsistent. See the next page for a list of things you can do.



Visit the **AvoidAClaim.com** blog to search names and email addresses from the frauds reported to LAWPRO. Click on "All Fraud Warnings" to see a full listing of names of confirmed fraudsters. If you still aren't sure the matter is legitimate, call LAWPRO at 1-800-410-1013. Our experience with multiple frauds can help determine if you are being duped. If the matter turns out to be a fraud and there is a potential claim, we will work with you to prevent the fraud, if possible, and to minimize potential claims costs.

Report obvious frauds to LAWPRO

Help us help other lawyers by sending obviously fraudulent messages, scans of identification and other documents provided to you to fraudinfo@lawpro.ca

Get fraud warnings & updates from AvoidAClaim.com blog

Wondering if you've been duped or your potential client is a fraudster?

For regular updates on fraud and claims prevention, subscribe to email updates from LAWPRO's AvoidAClaim.com blog.



Concerned about other types of fraud scams? See the Cybercrime and Bad Cheque Scams Fraud Fact Sheet at practicepro.ca/fraud for common bad cheques or phishing scenarios and tips on how to protect yourself, your law firm, and your clients.

Types of real estate fraud

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 fraud

1. Client uses fake ID to assume identity of existing property owner (or by filing Form 1 to become director/officer of corporate owner)
2. Client sells or mortgages the property, or discharges mortgage from title, then gets new mortgage from another lender
3. Paperwork looks in order, no encumbrances on title, but one or more recently discharged mortgages or recent transfers
4. Client in a hurry and accommodating, may discourage house inspection or appraisal

5. Transaction closes, you pay proceeds to client who may make a few mortgage payments, then disappears with funds
6. Lender sues you for value of mortgage



Advise lenders of recent activity on title and significant changes in value in advance of closing

Flip (value) fraud

1. Happens on purchase or refinance deals
2. Client says she or he is a real estate agent or in business of buying and selling
3. Client promises high fees, lots of business for quick turnaround on deals. (Short

turnaround means proper searches aren't conducted)

4. Once transaction closes, client flips property to accomplice (e.g., appraiser and/or mortgage broker) for much higher value
5. Lender issues mortgage on inflated property value
6. Client uses mortgage proceeds to pay initial purchase price, splits excess funds with accomplices
7. Client may make a few mortgage payments, and then disappears with funds
8. Lender sues you for excess/inflated value of mortgage

Identify potential real estate fraud

Red flags: The client

- Funds directed to parties with no apparent connection to borrower or property
- 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
- Client is "out of sync" with property – e.g., doesn't appear educated/affluent enough
- Stranger who appears to control client attends to sign documents
- One spouse or business partner mortgaging equity in property owned by both
- Client buys and sells often, prefers to deal in cash
- Client contact is only or primarily by email

Red flags: The transaction

- Repeat activity on single property or for single client. Title shows one or more recent transfers, mortgages, or discharges
- Rental and vacant properties especially vulnerable
- Property listing expired without sale (i.e., sale may be unregistered)
- Frequent and quick mortgage discharges on property
- New referral source sending lots of business
- Transaction area is distant from your office
- Deposit not held by agent or lawyer
- May target long time owners (deceased, ill, or elderly who may be less alert to signs their identity is being stolen)
- "Rush" deals, often with promise of more
- Client produces small deposit relative to price
- Amendment to Agreement of Purchase and Sale reducing price, deposit, or adding creditors

- For mortgage transactions, private, less sophisticated lenders may be targeted
- 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
- Use of Power of Attorney



Be Alert

- Avoid having documents executed outside your office
- Include deleted instruments in title search
- If Ontario driver's licence used as ID, consider verifying it on the MTO website

Due diligence on suspected fraudster

Take these steps to cross-check and verify information provided by the client.

- Cross-check names, addresses and phone numbers of client and other people/entities involved in the matter on Google and other search engines, or AvoidAClaim.com
- To find exact matches, enclose your search terms in double quotes.
- Do reverse searches on phone numbers
- Look up addresses using Street View in Google Maps
- Ask banks to confirm that branch transit number and cheque are legitimate
- Confirm entity making payment or loan is aware of transaction
- Contact company to confirm it is expecting debtor's payment or business loan
- Hold funds until all banks involved confirm funds are clear and can be withdrawn



Beware who gets paid from mortgage proceeds. Some title insurance policies exclude coverage for fraud claims when payment from mortgage proceeds is made to "non-authorized" parties. Consult the policy to confirm whether such restrictions exist. TitlePLUS¹ policies do not contain this exception.

Corporate ID fraud

Changing or stealing the identity of corporate property owners is commonly accomplished with the filing of a notice naming imposter directors and officers. The fraudsters then retain a lawyer to help sell or mortgage the corporation's property.

Red flags:

- Corporation has owned vacant, disused or run-down property for a long time, without activity on title or visible use of land
- Property is in highly marketable or developing areas, but subject to restrictive zoning, environmentally sensitive, or lacking road access (risks not always evident to private lenders)
- Real directors/officers/shareholders of the corporation are elderly, remote, or otherwise vulnerable (fraudsters may have knowledge of these circumstances)
- Current officers and directors were appointed very recently (see "Date Began" in Corporate Profile Report). This may not be a concern by itself, but something that is a big warning sign if there are other red flags
- Form 1 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's head office changed to non-existent or problematic address (such as a hotel – Google Street View may assist to determine this)
- Corporate resolutions or minute book with obvious errors or typos
- 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)
- Lender's or borrower's lawyer directed to pay sale or mortgage proceeds to parties with no apparent connection to transaction
- Clients say that title insurance for new mortgage is not required
- Client pushes for fast closing



TitlePLUS title insurance offers protection against fraud before and after purchasing property.

For more information on protecting clients against real estate fraud visit titleplus.ca

Is the fraudster in your office?

Not all fraudsters are strangers. Partners, associates, law clerks, other employees or independent contractors may turn to fraud because of financial pressures from a divorce, failed business venture or other personal crisis.

Red flags:

- Person never takes vacation or sick leave, works long hours, or refuses to delegate
- Person undergoes a sudden change in lifestyle or temperament
- Firm receives mail for corporation for which no client file is opened or billed, or minute book is kept in person's office instead of with corporate law clerk
- Unusual patterns such as sudden increase in payments to a person or entity, or complaints about slow payment from suppliers or clients, or increase in written-off work in progress
- For more information see "When the unthinkable happens" at practicepro.ca/lawpromag

LAWPRO's enhanced coverage for counterfeit certified cheques, bank drafts

The LAWPRO policy provides some overdraft protection to lawyers in relation to their trust accounts where liability for the overdraft results from the handling of a counterfeit certified cheque or counterfeit bank draft. This enhanced protection is subject to several conditions and limitations. Review the FAQs at lawpro.ca/faqs to make sure you understand this coverage and the extra steps you must take to qualify for it.



The one proven method to prevent counterfeit cheque or bank draft scams is to wait an appropriate number of days after depositing the monies before they are drawn from the account (LAWPRO suggests 8 banking days).

Excess coverage

Is your real estate practice growing? That's a good thing. But keep in mind that your risk exposure may be growing along with it.

Higher transaction volumes increase the chance of error or fraud. At the same time, growth in land values can mean that a single claim could easily hit the limit of your professional indemnity coverage. It may be time to consider whether excess insurance is appropriate for your practice.

Test your exposure at lawpro.ca/excess. For more information, contact us at service@lawpro.ca or 1-800-410-1013.

This information bulletin is published by LAWPRO to provide lawyers and law firm employees with an overview of some common types of fraud, and to provide practical advice on ways to minimize their exposure to fraud-related claims. 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. The comments in this publication are intended as a general description of the insurance and services available to qualified customers through LAWPRO. Your policy is the contract that specifically and fully describes your coverage and nothing stated here revises or amends the policy.

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

© 2018 Lawyers' Professional Indemnity Company (LAWPRO).
All rights reserved.


* LAWPRO, TitlePLUS and their logos are registered trademarks of Lawyers' Professional Indemnity Company. All other trademarks are the property of their respective owners.


¹ The TitlePLUS policy is underwritten by Lawyers' Professional Indemnity Company (LAWPRO). Please refer to the policy for full details, including actual terms and conditions.

 AvoidAClaim.com

 LAWPRO

 LAWPRO
TitlePLUS

 @LAWPRO
@practicePRO
@TitlePLUSCanada

 LAWPRO insurance
TitlePLUS Home Buying
Guide – Canada





Putting the fire out:

Dealing with the stress of a malpractice claim

There is simply no doubt about it: making an error or having an action commenced against you is stressful, even for the most successful lawyers. And because almost half of Ontario lawyers in private practice will face a malpractice claim at least once in their career, at some point this stress will be a reality for many lawyers.

From my years of handling professional negligence claims, I have seen lawyers react to this situation in different ways including fear, anxiety, embarrassment, and even anger.

The initial call with a lawyer is one of the most rewarding parts of my job. I am often meeting someone for the first time, learning about their practice, their firm, their clients and their current issue. For my part, I try to assess whether there is a problem that can be fixed or made to go away quickly. For the insured's part, once they get over their initial fear and anxiety and realize they will be helped through the claim and defended as appropriate, they usually feel more comfortable.

Embarrassment

Many insureds experience anxiety over the potential of people finding out about the error or alleged error at issue. This can be tough, for example, in a major litigation file where the insured's error (or potential error) might be discussed in an endorsement or reasons. Worries over losing the client, unsupportive partners, or judgmental peers can be hard to balance with the ongoing practice of law – all while being named a defendant in a negligence action.

If it is some consolation... remember, almost everyone makes an error at some point. Given the statistics, insureds who are willing to confide in colleagues will likely find that they are not alone in having a claim.

Anger

Some insureds are angry that they have been sued or that there is a suggestion that they have made an error. This is especially the case in situations where, in fact, no error has been made. Most insureds get over this anger fairly quickly, but some remain intensely angry throughout the life of the claim. This makes, not only the initial call, but all subsequent calls, challenging. The relationship with the insured usually balances out once they realize that the matter is moving to a resolution and, angry or not, we will assist them.

However, this kind of reaction to a claim emphasizes why it is so important to report a claim or potential claim to LAWPRO. Anger can lead to bad decision making such as retaliatory steps or aggressive letters that might actually undermine the insured's position. Reporting the potential claim and allowing another professional to deal with the situation enables the insured to step back and take a break from the confrontation. Keep in mind that having a claim made against you does not mean it is a *valid* claim. In fact, almost 40 per cent of claim files are closed with no payment at all (including defence costs).

Fear

I have also worked with insureds who are so overwhelmed by the situation that they can barely relay the facts. Take Carol (name has been changed), for example. She negotiated the settlement of her client's divorce proceedings which included each spouse retaining equal share of their holdings in a company they owned together with another party. Only after the final Order was signed did Carol learn that, because the class of her client's shares was different than that of her husband's, there would be an unequal tax effect of \$750,000 each year going forward. Carol had \$2 million in insurance coverage, including excess insurance – far less than the many millions in potential damages. I could barely hear Carol at the end of our initial call when she whispered, "I am going to lose my house."

Carol was often in my thoughts over the next few weeks. I wondered whether she was getting any sleep at all, and whether she had someone to confide in. In the end, there was good news: the matter was repaired and the file closed without any damages having to be paid and without Carol losing her house. That is another rewarding part of my job: telling an insured that their matter has been resolved.

Denial/Avoidance

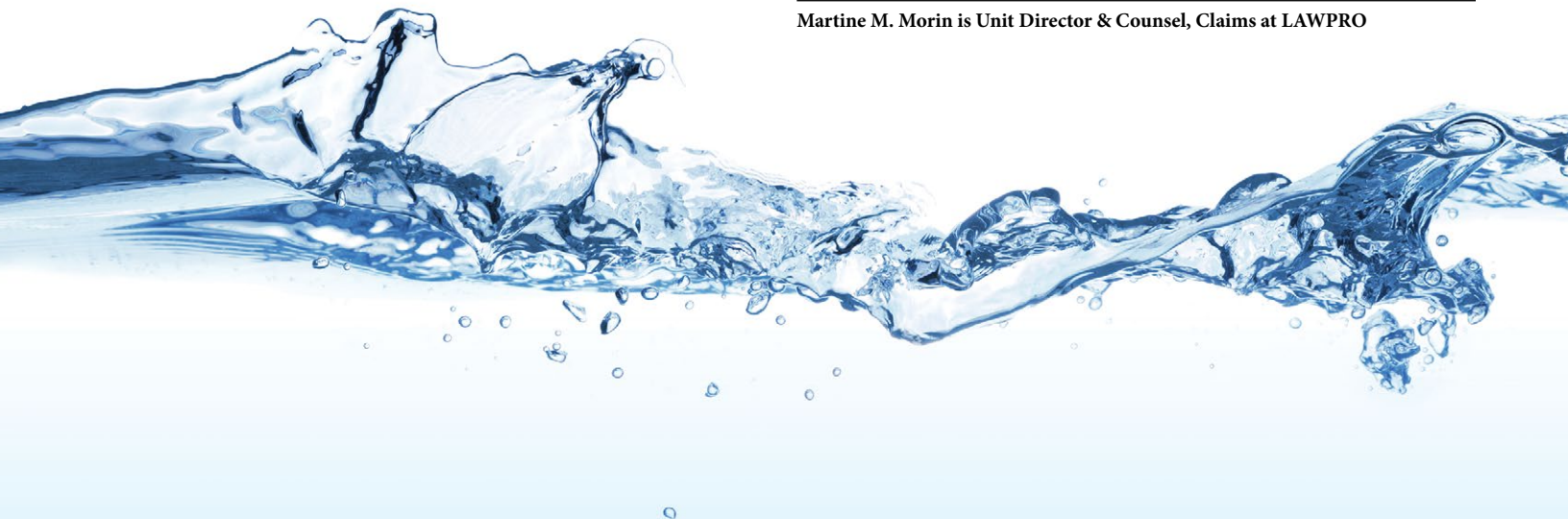
All too often, I see cases in which insureds are so stressed about an error, that they can't bring themselves to report it at all or have waited a significant period of time before doing so. These insureds simply cannot deal with the situation. Once a report is made, some of these insureds avoid dealing with the matter and will not return our phone calls or correspondence. This, of course, makes an already difficult situation worse. The delay in reporting may result in circumstances where it is too late for LAWPRO to repair an error or defend an action. Failing to cooperate may also result in a breach of the insured's obligations under the Policy. Both situations can result in a denial of coverage.

Remember, no good will come from a delay in reporting a claim. Reporting a claim as soon as possible allows LAWPRO to provide early intervention and your best defence.

Making it through

The good news is that 83 per cent of LAWPRO's claims are closed with no finding of liability or indemnity payment. While dealing with a claim is stressful, we are here to help. If you are feeling overwhelmed by an error or a claim against you, consider taking the time to check in with a trusted friend or colleague. If you do not feel comfortable sharing your situation with someone you know, the Member Assistance Program provides confidential peer counselling. ■

Martine M. Morin is Unit Director & Counsel, Claims at LAWPRO





Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk

Juda Strawczynski

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 [here](#).

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 e-mail 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 avoidaclaim.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.

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.

© 2021 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

What to do if money is diverted to a fraudster's account?

Raymond G. Leclair

There are multiple scenarios whereby fraudsters will attempt to have you wire funds to a different account than the one that you had intended to fund. Unfortunately, some of those attempts are successful. LAWPRO has received such claims and heard of many others. Here are some tips to assist you if such a fraud happens to you, your clients or someone you know.

1. Contact the bank:

- The person who initiated the wire should ASAP 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.
- Request that the initiating bank contact the receiving bank to stop the wire. Again, it may have been dispatched but might be pending. 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.

2. Report the matter to your local police as a fraud, and [the Canadian Anti-Fraud Centre](#).

3. [File a claim](#) with LAWPRO as soon as possible, together with all relevant documents in your possession.

4. Consider filing a claim with your other insurers who may have a policy intended to respond to this type of risk, including but not limited to your professional liability excess insurer, cyber, commercial general liability, crime, computer fraud, and fidelity insurance carriers. 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 these regards.

5. Obtain an IT forensic audit 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.

6. Alert your client to the diversion fraud immediately and request that they consider whether their systems have been compromised and they should obtain an IT forensic audit, where appropriate. The systems of third parties with knowledge of the transaction in issue (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.

7. 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.

Fraudsters have sent emails with false bank routing information; they have altered directions or other documents that contained bank routing information and have altered or created false discharge statements with payment directed to their bank account.

Fraudsters have sent emails with false bank routing information; they have altered directions or other documents that contained bank routing information and have altered or created false discharge statements with payment directed to their bank account.

Tips to avoid being a victim:

- Review our article [Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk](#)
- Anytime a lawyer receives instructions to wire money to a bank account and especially if the instructions are updating or changing previous instructions, the lawyer should 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.
- Lawyers should equally advise their clients, or anyone they expect funds from, of the potential for a diversion attempt and to confirm the instructions before initiating the wire transfer.
- Fraudsters will spoof an email address – create 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 very carefully look at all the email address in the message.
- Lawyers should train the members of their offices in what to look out for and should have regular discussions/training sessions to reinforce the message. Someone from the office may see information or indications that others may not. We have been advised of an assistant following up on her curiosity and exposing a false document that would have diverted funds.
- For general cyber prevention tips, review our [Cybersecurity and Fraud Prevention Tips](#), and subscribe to [AvoidAclaim.com](#) for fraud alerts.

Lawyers and their office colleagues must remain vigilant to fraudsters attempts.

If you suspect you are the target of a fraud, call LAWPRO for assistance

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

© 2021 Lawyers' Professional Indemnity Company (LAWPRO). All rights reserved.
® Registered trademark of Lawyers' Professional Indemnity Company

SPEAKER BIOS

Victoria Crewe-Nelson



Victoria Crewe-Nelson is the Vice-President of Underwriting & Customer Service for the Lawyers' Professional Indemnity Company (LAWPRO). Victoria was called to the Ontario bar in 2003 and during the course of her practice had the opportunity to work in a number of practice areas, including corporate/commercial, litigation, estates and trusts, real estate, and admiralty law.

Victoria obtained her degrees (B.A., LL.B.) through her studies at the universities of Toronto, Ottawa and Edinburgh. A past instructor with the bar admission course, Victoria has been published on topics such as professional liability, the *Limitations Act*, class actions, family law, and parental responsibility. As an underwriter for LAWPRO, Victoria focuses on law firm risk management, understanding the ways in which lawyers practise and emerging threats faced by lawyers, clients and the insurance industry.

Victoria lives in Toronto with her husband, children and dogs. She has been involved with various non-profits, mentoring and equity/diversity/inclusion initiatives.

Mouna Hanna



Mouna Hanna is a partner in the Toronto office of Dolden Wallace Folick LLP and the national lead of the firm's Cyber and Privacy Liability Practice Group. Mouna is a Certified Information Privacy Manager (CIPM) designated through the International Association of Privacy Professionals, and holds a Certificate in Privacy Law and Cybersecurity from Osgoode Hall Law School. In 2021, Mouna was recognized by Lexpert as a "Leading Lawyer to Watch" in the area of commercial insurance. She was also the recipient of the 2021 Richard B. Lindsay QC Exceptional Young Lawyer Award, awarded by Canadian Defence Lawyers.

Mouna routinely acts as a cyber and privacy breach coach and defence counsel to organizations across various industries and sectors that are involved in cyber related incidents, breach of privacy claims and third party litigation. She advises clients on their obligations under Canada's various Federal and Provincial privacy laws and has assisted small and large organizations throughout each step of high profile and complex breaches. Mouna also represents IT security companies in the event of a claim against them following a cyber security incident.

Mouna also sits on the Board of Directors of the Canadian Defence Lawyers and on the Ontario Bar Association's Privacy & Access to Information Section committee. Mouna is also a contributing author of the book "Cyber Liability and Cyber Insurance in Canada", published by Thomson Reuters in 2020.

Mouna was called to the Ontario Bar in 2012 after graduating from the University of Ottawa with her law degree in 2011. Prior to law school, she obtained her Bachelor of Arts (French Language and Literature and Psychology) from Western University in London, Ontario in 2008. While in law school, Mouna proudly co-published one of the first academic articles on the legal implications of teen "sexting", privacy and cyberbullying in the Canadian Journal of Women in the Law.

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.

Juda Strawczynski



Juda Strawczynski manages and promotes practicePRO, LAWPRO's innovative claims and risk management initiative, including identifying emerging claims and risk, resource creation, and outreach to the profession.

Prior to joining LAWPRO, he served as a Policy Counsel at the Law Society of Ontario, where he provided strategic counsel with respect to key issues facing the legal profession, including access to justice, professional regulation, governance and legislative issues. Prior to that, Juda practised litigation, and served as a Fellow at Physicians for Human Rights in Cambridge, MA, as President of Canadian Lawyers for International Human Rights (CLAIHR) from 2013 to 2018, and as a Director of the Canada Millennium Scholarship Foundation. Juda has a Bachelor of Arts from McGill University in Humanistic Studies and International Development Studies, and a Juris Doctor from the University of Toronto.

Tannis A. Waugh



Tannis A. Waugh was called to the bar in 2003 and practices in the areas of real estate, corporate/commercial, and estate planning. In 2018, she was certified as a specialist in real estate by the Law Society of Ontario.

As a former Trustee for the Toronto Lawyers Association, Tannis has been involved in advocacy and education initiatives, most notably the moderator and presenter of continuing education programs and writer of articles for the TLA journal. She was formerly on the education committee which is responsible for producing CPD programs for Toronto lawyers.

She is also a member of the Condominium Sub-documents Committee of the Working Group on Lawyers and Real Estate which is responsible for producing province-wide precedent materials for condominium transactions.

Tannis is a frequent presenter for continuing legal education programs and, in the past, has spoken on the issue of real estate, estates and ethics for the Canadian Bar Association/Ontario Bar Association, Law Society of Ontario, The Commons Institute, the Law Clerks Institute and the Toronto Lawyers Association.