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.

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. 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.

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

AvoidAClaim.com
LawPRO
LawPRO
TitlePLUS
@LawPRO
@practicePRO
@TitlePLUSCanada
LawPRO insurance
TitlePLUS Home Buying Guide – Canada

B11/2018