Learn How to Recognize, Avoid and Protect Yourself Against Fraud

Lawyers in Alberta are targeted by fraudsters who go to great lengths to make their schemes appear legitimate by using sophisticated variations of client names, locations, fake documents and back stories. To help lawyers protect themselves, the Alberta Lawyers Insurance Association (ALIA) has created this ALIAlert to raise awareness on how to recognize and avoid scams.

Common Scams

Phishing scams come in many different forms, but contact is most often established via email. Phishing is an attempt to obtain sensitive information such as usernames, passwords, and credit card details, from a purportedly trusted contact in an electronic communication.

In an example of a **Direction to Pay** scam, the fraudster spoofs a lawyer's email address, making it appear that the email is sent from the spoofed lawyer by displaying the lawyer's actual name in the "From:" line. The email asks another lawyer or staff member to transfer funds on some pretext such as urgency, the need for extreme sensitivity, or because the lawyer is away from the office.

In the phony **Change in Payment Instructions** scam, the fraudster sends revised payment instructions by email from someone the lawyer or law firm believes is the client. The law firm then sends the payment to the new account and the money is gone before the firm realizes its error.

In the **Shared Document** scam, lawyers are lured into giving away their passwords or installing malware by way of a fake shared document request, such as DocuSign. Once a lawyer has signed in, with a fake login page, the scammers have everything they need to have access to your email account. From there, scammers can sell your email credentials, use your address to send fake shared document requests to others, and even gain access to your other online accounts (including bank accounts).

The **Fake Dropbox** scam involves what looks like legitimate emails with a Dropbox attachment or link. Appearing to be sent from a known contact, this phishing scam email works in several ways by exploiting the popularity of the file sharing service. The goal is to steal your Dropbox password, your email password and/or lure you into downloading a virus attached to or linked from the email.

In the **Retainer Overpayment** scam, a new client contacts you by email and provides you with a retainer above the amount required. Once the phony cheque/bank draft is deposited, the client requests a refund of the extra funds before you learn that the cheque or bank draft is illegitimate.

A similar fraud is the **Bad/Fake Cheque** scam. An example involves a law firm hired to collect money associated with a failed deal. However, soon after proceedings begin, the client informs the law firm that a settlement has been reached. The goal is to have the law firm deposit the settlement cheque into its trust account and pay the money out to the client before the bank informs the law firm that the cheque is void.

The **Fake Trust Account Auditor** scam involves a fraudster attempting to gain access to lawyers' trust accounts by claiming to be an auditor from ALIA or the Law Society or a third party representing ALIA or the Law Society. This fake auditor will request that all trust account information be made available to them. The fake auditor is now able to access your trust account. Please note that third parties and ALIA do not audit trust accounts. If the Law Society selects you for an audit, you will be advised of it directly by the Law Society.

The goal of the **Fake Professional Complaint** scam is to install malware. A lawyer receives an email purportedly from a regulator regarding a complaint. The complaint can be viewed by clicking on a hyperlink or attachment that instead installs malware and/or ransomware that will block computer login access until the lawyer pays to get it unlocked.

Protect Yourself from Fraud

- Use caution when responding to and engaging with potential clients with whom you do not have a relationship. To protect yourself, follow these Client Identification and Verification Rules.
- Although there is no way to know what the next scam will look like, most scams demonstrate common patterns that if identified, can help prevent fraud and loss. Check out our Red Flags to assist you recognize and avoid a scam.
- Watch for spelling and formatting errors.
- Be wary of clicking on any attachments or links. They may contain viruses, malware and spyware.
- Check email addresses. If just a name appears, hover your mouse over the name to verify the address.
- Check embedded hyperlinks by hovering your mouse over the link to verify the address.
- Prior to sending any funds, contact existing clients in-person or by telephone to confirm that the request is legitimate.
- Establish a protocol that confirms instructions from clients and/or lawyers before any funds are transferred.
- Establish protocol to obtain confirmation from the bank that the incoming funds have cleared prior to issuing a cheque from your trust account.
    - Do not refund any funds until the payment has been fully cleared by confirming you're your bank
    - Check the validity of all credit and debit cards to ensure they are real
    - Issue refunds using the original method of payment
- Protect your computer with anti-virus software, spyware filters, email filters and firewall programs.

- Ensure your anti-virus software is active and up to date. Regularly schedule scans to search and remove already existing malware.
- Keep your operating system and software up to date.
- Make regular back-ups of important files.
- Consider backing up critical data “off-line” (e.g. a hard drive that is not connected to your computer system)
- Be cautious of urgent messages indicating there is a threat to your computer.
- Never click on a pop up that claims your computer has a virus, if you cannot access anything on the computer beyond the pop-up screen your computer is infected.
- Additional information about recognizing and avoiding fraud is available on our Supplemental Resources & Links webpage.

By reporting any fraudulent or suspected fraudulent activity to ALIA, we will be able to protect other lawyers and their firms from future fraud attempts.

Please report any contact you receive that you suspect to be illegitimate, with as much detail as possible, to the ALIAlert mailbox. If you are aware of any theft from your or your firm’s trust or general account, you must immediately report it to the Law Society.