CURRENT SCAMS, CONS, AND SWINDLES

Fraud. It's here to stay and fraudsters are several steps ahead of their targets – that's you. We're sharing some recent scams, cons, and swindles that have been reported to LAWPRO:

Cheque fraud

A lawyer reviewed their cashed cheques and noticed some of them were fraudulent. The numbering sequence was wrong (the lawyer had already used those cheque numbers in the past) and they were older versions of the lawyer's updated cheques. The lawyer immediately contacted the bank and they tried to get the funds back. The lawyer closed the trust account and opened a new account.

Tips

- Cross-check and verify cheque information by Googling name, addresses, and phone numbers of the parties involved.
- Ask your bank or the issuing bank to confirm that the branch transit number and cheque are legitimate.
- Hold the funds until all banks confirm funds are clear and can be withdrawn.
- Search the AvoidAClaim.com database of bad cheque fraud names.

Wire fraud

Lawyer received funds from their client's private mortgage lender by wire transfer. The lawyer then relied on the funds showing in trust and disbursed all the funds, including some to the client. Several days later, the lawyer's bank advised that the wire transfer was fraudulent and the bank requested the funds be returned. The fraud department of the lawyer's bank is investigating.

Tips

- For funds to be truly irrevocable, you need a Payment Confirmation Reference Number (PCRN). Anything else is a risk. Read this articles on how to find the PCRN.
- Use this Wiring Funds Checklist from PracticePro for every transaction that involves wiring funds from your trust account.

A counter fraud strategy that is often overlooked is sharing experiences, information, and best practices. Working together to exchange positive and negative outcomes, what worked, what didn't work, and what steps to take will help you know what to watch out for.

Phishing and Email Breach

1. Lawyer A received an email from Lawyer B that appeared to be trial documents with attachments to download. By clicking on the Download button, malware was installed that affected their email program and re-routed outgoing emails and sent malicious phishing emails from their account. Lawyer B has since been receiving phone calls from other firms that are receiving the same type of suspicious email with attachments to download.

Tip

– Before clicking on any attachments or downloads consider whether you were expecting to receive an email from this person. Check the email address carefully and if in ANY doubt call to confirm that the person actually sent you the email before opening any attachments.

2. Lawyer A sent an email with banking information to Lawyer B. Lawyer B called Lawyer A to double check the authenticity of the account details. Good thing they did – the bank account number had been altered by a fraudster.

Tip

– Verify instructions independently. When you receive instructions to wire money to a bank account, contact the payee directly by an independent method such as a phone call (do NOT reply to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information. Instruct your staff to do the same.

3. A lawyer received an email with wire payment instructions to the lawyer from the bank. The lawyer made the wire transfer t o pay out the client's mortgage. The lawyer reviewed another recent transaction with the same bank, compared the addresses of the payout statement and realized that the two addresses were not the same. This indicated that the new wire instructions were fake.

Tip

– Any time there is a sudden change, this is a flag to be suspicious and take the time to look for inconsistencies. Double check all of the email addresses in the message to see if they are fake. Fraudsters will spoof an email address by creating a very similar looking address by adding an extra letter/number or changing a character(s). And remember, if the other party's email account is compromised, it could be the fraudster sending you email that look like they are coming from your client, the bank, or another lawyer.

4. A lawyer's email was hacked. The fraudster then sent out emails from the lawyer's email account containing a "business proposal" prompting the recipient to enter personal information including password.

Tip

– Never reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother's maiden name or birthday), even if they appear to be from a known or trusted person or business since this is probably the most common way that personal information is stolen. Legitimate businesses should never send you an email asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don't use the number in the email – it could be fake too!

A fraudster accessed Lawyer A's email account and blocked emails sent by Lawyer B to Lawyer A. The fraudster then sent their own emails to Lawyer A pretending to be Lawyer B, and using a spoofed email address, the fraudster provided false contact information and a fake trust cheque. Lawyer A phoned the fake number and confirmed the fake banking details. Lawyer A then sent the funds by wire. Lawyer A later contacted Lawyer B directly after noticing that Lawyer B's law firm was not a numbered company. As a result, Lawyer A was able to reverse the wire transfer and redirect the funds to Lawyer B, although the reversal took several days.

Tip

– Verify instructions independently. When you receive instructions to wire money to a bank account, contact the payee directly, at the original number you had, by an independent method such as a phone call (do NOT reply to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information. Instruct your staff to do the same.

Impersonation

Individuals received mailed letters purporting to be from a lawyer's firm. The letterhead included the firm name, address, and the name of one of the partners, but the postal code, telephone number, website, and email addresses were fraudulent.
If someone emailed the address in the letter, they received a phishing email in reply asking for personal information.

Tips

- Use a standard script in all responses (phone, in-person, or email) to clarify that you and your firm are not involved and advise the inquirer to treat the matter as potential fraud. Keep a record of all inquiries and responses.
- If there is a possibility that the impersonator may contact current or former clients, advise your clients to watch for suspicious emails.
- If your website has been duplicated or your information is used on another website, contact the web provider to request removal due to fraudulent activity.
- Read this article called Firm Websites Being Impersonated by Fraudsters.
- Report to the Canadian Anti-Fraud Centre.
- File a complaint with the LSO through LSO Connects and contact the Practice Management Helpline for additional guidance relating to your professional obligations in the circumstances.
- Preserve all evidence related to the fraudulent activity.

Internal Fraud

A law firm employee drained the lawyer's trust accounts over the course of many years. The employee presented the lawyer with cheques to be signed and the lawyer did not confirm or verify whether the cheques were for legitimate purposes.

Tips

- Conduct regular and random spot audits of lawyers and staff with access to law firm trust accounts.
- Require two signatories for trust cheques. Don't allow one person to both prepare and authorize payments.
- Conduct daily or weekly reconciliations of trust accounts.
- If a cheque is payable to a party that is not a familiar individual or entity, verify the details in the file as to who the party is and put the payment into context.
- Create separate roles for initiating, approving, and reconciling transactions.

Being aware of current frauds and scams and knowing what to watch for is essential in keeping your law practice and business safe. Educating the people you work with and taking proactive measures is also imperative.

If you suspect fraud, call LAWPRO at 1-800-410-1013 or 416-598-5899 and forward any suspicious emails and documents received to fraudinfo@lawpro.ca.

You can find fraud resources on the PracticePRO website and AvoidAClaim.com blog . Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters. ■