This article appeared in the June 2023 issue of *Communiqué*, the e-newsletter of the Law Society of Manitoba.

FRAUD AND A FIB
Firm Wires Sale Proceeds to a Fraudster

TANA CHRISTIANSON, Director - Insurance
IN COLLABORATION WITH THE AUDIT DEPARTMENT

A local law firm was acting for a corporation that was selling a piece of property. An assistant in the firm was doing the legwork.

The Error

The deal closed, and it was time to send the money to the client. The assistant received instructions by email from the client, or so it appeared. The assistant did not call the client to confirm that the instructions had in fact come from the client. When it came time to requisition the funds, the assistant ticked off the box on the firm's checklist, falsely saying the current client had been called to confirm the instructions. This was a fib. The assistant had not called the client.

The Wire

The funds were wired to the fraudster, based on the fraudulent instructions. Over a quarter of a million dollars went to a fraudster instead of the client.

The Email Hack

It turned out that the client's email had been hacked. The fraudster hackers had put in place a rule in the client's email account that all emails from the client's law firm would go directly into a separate folder and skip the client's inbox. This way, the client wouldn't see emails from the law firm but the fraudster could monitor the email account, determine when the law firm was ready to send out the money, and then send instructions to the law firm to send the funds to the fraudster's bank account and not the client's.

Because the fraudster had hacked the client's email account, if the law firm had emailed the client to confirm the change in wire instructions, the fraudster would have intercepted that email and confirmed the instructions. That is why the phone call to confirm, which didn't happen, is so important.

We are trying to get the money back. However, it may be too late.

Phone Call Confirmations

Do not send funds to anyone based on email instructions. Pick up the phone and make a call to the client at the phone number on your file. Not only is making the call critical, but what number you use can also make or break a fraud. DO NOT use any phone number that accompanies the email or accept any phone call initiated by your 'client' as authentic. Why? Fraudsters put phone numbers in their fraudulent emails leading right back to the perpetrator instead of the real client. Fraudsters may go one step further and call you, authorizing the fraudulent payment instructions as a way to try to thwart this control. If this sounds unlikely, consider what generative artificial intelligence can do to manipulate voice samples. If a phone call comes in from someone purporting to be the client or acting on their behalf, put your detective hat on and ask questions only the client would be able to answer, like who they saw when they last came into your office or even a pre-arranged security answer, recorded on your file (like, what is your favourite flower or first car?).

A quick call using the right phone number would have blocked this fraud. Too bad that assistant - who, by the way, has since been terminated for the fib - did not pick up the phone.

WHAT CAN YOU DO TO AVOID FUTURE FRAUDS?

1. Share cyber security and awareness information with lawyers and staff, using the Law Society's Cyber Security Resource Library as a starting point;

2. Educate all lawyers and staff in your firm about fraud risks directed to law firms:

   a) Review and discuss the Law Society's recently updated Fraud Awareness page in the Trust Accounting Fundamentals;

   b) Reference this article as a real-world example of why you need to follow these steps, as well as earlier Communique articles from June 2022, December 2022 and January 2023;

   c) Walk through the Safe Flow of Funds Guideline, found in the Trust Accounting Fundamentals

3. Review and discuss your firm's cheque requisition process, adding a checklist if you don't already use one. If you already have a checklist, review it to ensure key elements and risks are addressed;

4. Include anti-fraud awareness and training as part of orientation of all new lawyers and staff;

5. Refresh existing staff knowledge by ensuring their cyber security knowledge and awareness is kept current; and

6. Review your checklists as you receive new information to ensure they evolve with the ever-changing fraud techniques.

Direct communication with the client in-person or on the phone is a critical defence to this type of fraud. Never accept new or changed payment instructions by email alone. Call before you requisition.