FRAUD ALERT: WATCH FOR UNAUTHORIZED WIRE TRANSFERS FROM YOUR TRUST ACCOUNT

A growing number of LAWPRO insureds are experiencing unauthorized wire transfers from their trust and general accounts. One lawyer discovered $1.6 million dollars was removed in 8 unauthorized transactions over 3 days. These frauds are concerning as the bank's multi-factor authentication (MFA) login and transaction token or notice processes for wire transfers were bypassed. We don't understand and are investigating how the bank's MFA login and transaction token or notice features are being bypassed.

While phishing messages were commonly used to trick lawyers, law firm staff, and clients into revealing their login credentials for email or bank account access, we are seeing more sophisticated frauds. In multiple frauds involving the same bank, it appears the fraudsters used information on legitimate credit card transactions to make it appear they were real bank employees calling to discuss improper credit card transactions. On another claim it appears the fraudsters reported a gas leak at a law firm's office to serve as a distraction late on a Friday afternoon when an unauthorized transaction was initiated. Two more unauthorized transactions happened over the weekend and it wasn't until Monday morning that the firm discovered the unauthorized transfers.

We encourage lawyers to check your trust and general accounts daily for transactions you did not authorize, and especially on Fridays and around long-weekends or holidays.

Please be on high alert for the following:

- If anyone contacts you purporting to be from your bank, and particularly if you are asked to log into your online banking portal or to confirm/change your login name or password.
- If you receive any authentication requests when you are not actively signing into your banking portal or completing a wire transfer
- If you receive any suspicious attachments or links, either by email or text, particularly if they appear to be from your bank or a banking website

If you get suspicious calls or discover unauthorized transactions:

If you receive suspicious calls about your credit cards or bank accounts, call your bank immediately, using a trusted and verified phone number, to review recent transactions and to take steps to secure your account (i.e., change your login and authentication credentials).

If you discover unauthorized transactions in your trust or general accounts, it is critical that you contact your bank's fraud department, immediately upon learning of the fraud. Time is of the essence. Fast interventions by a bank will make it more likely that transactions can be stopped or that funds can be recovered. After calling the fraud department, go to your bank branch in person and speak to an employee who may also be able to assist you in dealing with the fraud. It is also important to contact the bank(s) that received the unauthorized wire transfers to alert them of the fraud. They may help by placing a hold on a transfer.

It is important to secure a copy of the wire transfer confirmations as soon as possible and before your account is potentially frozen and/or inaccessible, so that you may identify the recipient bank and put them on notice of the fraud. These wire confirmations also assist with the investigation of the fraud and the potential recovery of the funds.

Be sure to familiarize yourself with the verified phone numbers for your bank before a fraud happens so that those numbers are easily available to you if required. One of our insureds was transferred multiple times when attempting to contact their bank and struggled to reach an appropriate bank representative who could provide assistance in a timely manner. Be persistent when you call and make sure you ultimately speak to someone that will take steps to respond to the fraud you experienced. Keep detailed notes of your conversation with the bank, and immediately after you speak with the bank file a claim notice report with LAWPRO.

Please share this warning with your staff. Fraudsters will approach staff and ask them to change payment information or verify account or transaction information. Staff can also be in a position to prevent a fraud if they see something unusual. Encourage your staff to watch for unusual circumstances and to bring questions or concerns to your attention. ■

Tips:

- Monitor trust accounts for unauthorized transactions
- Be alert to suspicious calls or email regarding your trust account
- Call your bank immediately if you discover unauthorized transaction
- Report to LAWPRO immediately after you call your bank
- Talk to your staff and share these tips with them – they are often the first ones to notice unusual activity