# Wire fraud scams on the rise:

## 5 tips to reduce your risk

**LAWPRO is seeing an increase in phishing attacks against lawyers trying to trick them into wiring funds out of their trust accounts to the fraudster.**

There are different ways that fraudsters are trying to direct lawyers and law firms to wire money to them. Fraudsters have pretended to be:

- A lawyer in the firm, to direct staff to wire funds to a client or to complete a transaction
- A lawyer or staff at a firm acting for a seller in a transaction, to direct the other side to wire funds
- A financial institution, to direct wire payment to it
- A client, to seek payment of funds by wire

It starts with a hacked email system or impersonation using lookalike fake email address. We have seen cases where the fraudster has hacked into a lawyer or law firm email system, the client's email, or the email system of others related to the transaction. In these situations, fraudsters monitor the emails and send wire transfer instructions from legitimate email addresses to send out wire payment instructions.

Follow the tips below to reduce your risk of falling victim to these increasingly sophisticated fraud scams.

### Tip 1: Don't be spoofed: check the email address

Lawyers should use spam filters and check email addresses to reduce the risks posed by fraudsters impersonating lawyers, law firm staff, clients, financial institutions and others. For more tips to avoid spoof email addresses, see our article "Paying attention to the fraud behind the curtain."

### Tip 2: Check documents to make sure they haven't been manipulated

When sending documents electronically, on receipt back, double check to make sure that key information, such as wire direction instructions, have not been manipulated. If you send out a document with wire instructions or other key financial information, you can check the document on receipt back that this information has not been changed.

### Tip 3: Implement independent verification on all wire payments

Verify all directions to wire funds out of trust by confirming the instructions using a different medium than they were first received. This step can help reduce the risks posed by email hacks and cases where documents have been intercepted and manipulated.

Here are a few examples of independent verification in action:

- **Internal verification**: The law firm partner purportedly emails from the firm address or a personal email address instructing you to wire money out of trust. Walk down the hall to the partner's office to ask if the partner sent the instructions. If the partner is out of the office, rather than replying to the email to confirm the direction (which will not help if the lawyer's email account has been compromised), call or text the lawyer.

- **Before wiring funds to another firm:** If a lawyer at Firm A emails wire instructions to a lawyer at Firm B, the lawyer or staff from Firm B can call Firm A to confirm the wire instructions. The same process can apply on receiving wire instructions from a financial institution or any other request for payment by wire transfer.
- **Before wiring funds to a client:** As another example, a client may email you to instruct you to wire payments to an account. You can consider calling the client to verify that the client's instructions are valid, and that the client's account has not been hacked.

Firms that have implemented independent verification protocols have successfully foiled fraud attempts. A quick call to verify written wire payments might save you from being a victim of fraud.

## Tip 4: Make fighting fraud part of your firm culture

Continue to train yourself and train your staff about fraud risk.

- For related CPD programming on fraud prevention, see our watch-anytime CPD programs on real estate fraud, bad cheque and cyber fraud. These programs are free for you, your colleagues and staff to view, and are eligible for LAWPRO's Risk Management Credit.
- Subscribe to avoidaclaim.com for fraud warning updates.

Try incorporating these tips into your practice to help reduce the risk of fraud.

## Tip 5: Stay on constant alert

Fraud prevention is not a one and done task. You and your staff need to be constantly vigilant. A few of the fraud scenarios we have recently seen include:

***The fake instruction to wire funds***

The fraudster sends instructions directing the wiring of funds to a particular account that the fraudster has set up or can access. In recent cases reported to LAWPRO, a fraudster infiltrated a law firm email system, intercepted correspondence regarding a transaction, and then sent wiring instructions from a law clerk's email address. Since they were being sent from legitimate law firm email addresses, there was nothing to suggest anything fraudulent from the email itself. Since the fraudster could see incoming emails, as described further below, only a separate means of verifying the instructions could stop the fraud.

***Fake documents may strengthen the credibility of the direction to wire funds***

We have seen instances where fraudsters have manipulated documents to alter wire payment instructions. We have even seen "secure" electronic documents prepared by a law firm intercepted, manipulated to provide new account information for wiring funds, and then sent back to the firm.

***Last minute changes are a red flag, but aren't the only flag***

Often, the fraud may include a last-minute direction to wire funds to a new account. Any late change in payment instructions should be treated with caution, as this is a red flag of fraud. However, we have also seen cases where the fraudster has sent out the wire fund instructions early in the transaction.

Bottom line – there are all sorts of ways that fraudsters try to trick lawyers and their staff to wire funds to them. Lawyers and their staff should be on constant alert for these frauds and can adopt proactive measures to reduce the risk of these attacks. ■

Juda Strawczynski is Director of practicePRO

## Three simple things you can do

### Call before you click

Always independently verify wire instructions.

### Train your lawyers and staff

Make sure all the lawyers and support staff in your firm are aware of the likelihood of spear-phishing attacks and the need to verbally confirm any changes to wire-transfer instructions received by email.

### Warn your clients

Alert your clients of the dangers associated with wire fraud and advise them to verbally confirm with your firm any bank account details received by email.