WIRE FRAUD

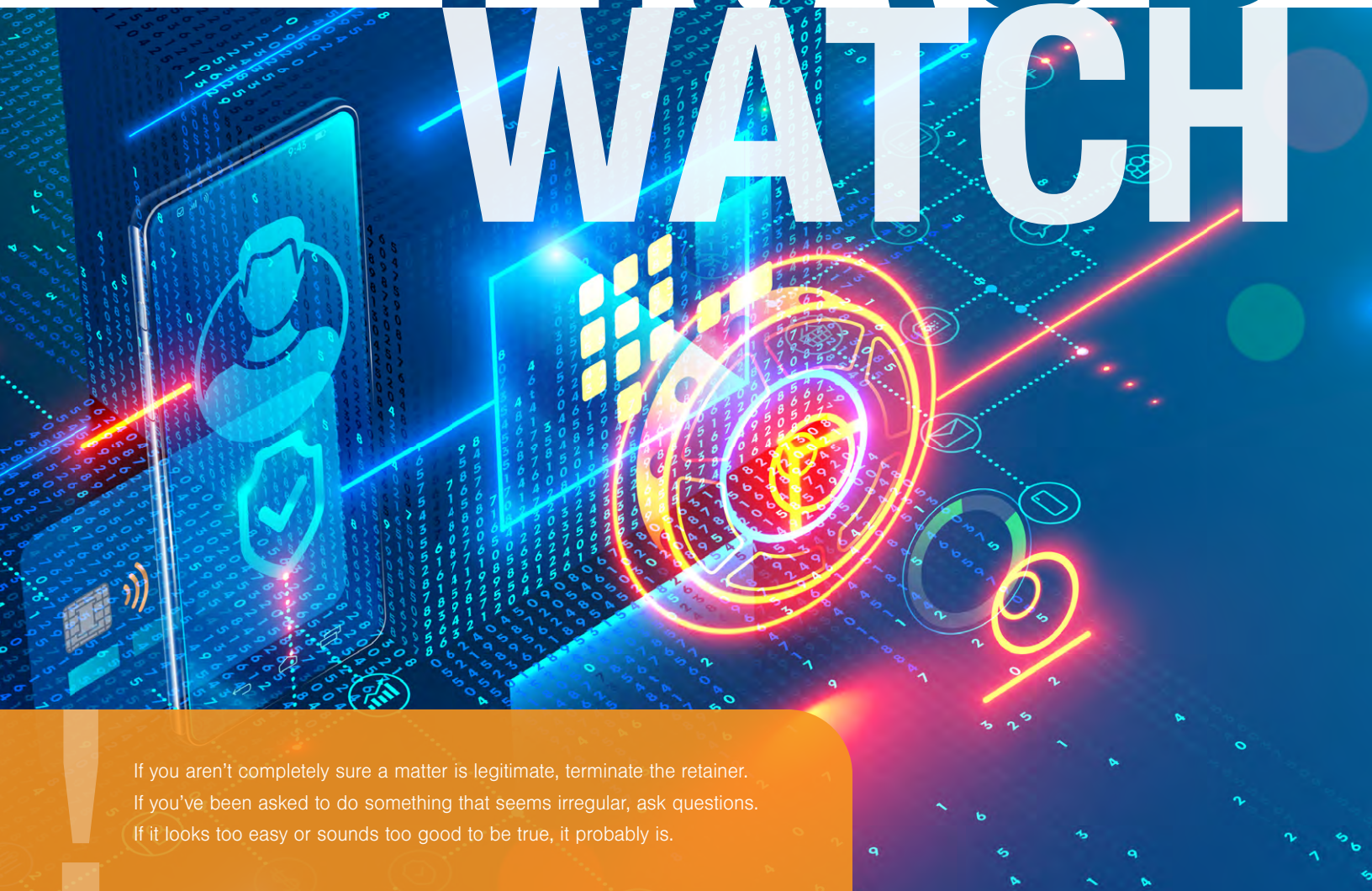
Fraudsters are actively trying to direct lawyers and law firms to wire money to them – often through spoofed emails of people you know or hacking into emails.

Fraudsters have pretended to be:

- A lawyer in the firm directing staff to wire funds to a client or to complete a transaction
- A lawyer or staff acting for a seller in a transaction directing the other side to wire funds
- A financial institution directing wire payment to itself
- A client seeking payment of funds by wire

LawPRO®
Lawyers' Professional Indemnity Company

FRAUD WATCH



If you aren't completely sure a matter is legitimate, terminate the retainer.
If you've been asked to do something that seems irregular, ask questions.
If it looks too easy or sounds too good to be true, it probably is.

It starts with a hacked email system or impersonation using a lookalike fake email address. In the hacked email situation, the fraudster hacks into a lawyer or law firm email system, the client's email, or the email of others related to the transaction (or those copied in the email thread) and monitors the emails. The fraudster then sends wire transfer instructions from legitimate email addresses directing the wiring of funds to a particular account that the fraudster has set up or can access. When using a lookalike fake email address, the fraudster sends instructions that appear to be legitimate. In some cases, corporate records may be altered to add credibility to the scheme.

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 the wire instructions were being sent from a legitimate law firm email address, there was nothing to suggest anything suspicious from the email itself. Given that the fraudster could see incoming emails, only a separate means of verifying the instructions could stop the fraud.

TIPS

Verify instructions independently: Anytime you receive instructions to wire money to a bank account, contact the payee directly by an independent method (not replying to the email sending the instructions) to verify the instructions received and the accuracy of the bank routing information.

Double check email addresses 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). Having hacked into one account, they may spoof other email addresses that were in the email thread to increase your confidence that it is a proper message. It is important to carefully look at all the email addresses in the message. And remember, if the client's email account is compromised, it could be the fraudster sending you emails that look like they are coming from your client.

Implement two-factor authorization on your email systems: Two-factor authentication is an extra layer of security to make sure that people trying to gain access to your email are who they say they are. First, a user will enter their username and password. Then, instead of immediately gaining access, they will be required to provide another piece of information such as a code. Outlook and Gmail both offer two-factor authentication.

Regular training: Train staff in what to look out for and have regular discussions to reinforce the cyber security message. Someone from the office may see information or indications of fraud that others may not.

Educate your clients: Advise your clients of wire transfer risks. If you do not accept wire payments from them, tell them so that if they are approached to send funds by wire, they know it will be a fraud. If you do accept wire payments, explain your process and insist that they call you before they send you payments.

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 one firm emails wire instructions to a lawyer at another firm, that lawyer should call them 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: A client may email you to instruct you to wire payments to an account. You can call 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 blocked fraud attempts. A quick call to verify written wire payments might save you from being a victim of fraud.

Use this wire checklist: Funds Transfer Instructions Verification Checklist.

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. Visit AvoidAClaim.com and click on "All Fraud Warnings" for a list of confirmed fraudsters.