5 TIPS TO REDUCE YOUR RISK OF WIRE FRAUD SCAMS

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. There are 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.

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 e-mail 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.

Tip 4:

Make Fighting Fraud Part of Your Firm Culture

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

Tip 5:

Stay on constant alert

Fraud prevention is not a one and done task. You and your staff need to be constantly vigilant.

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.