You transferred funds to the wrong account what now?

Fraudsters try to trick lawyers into wiring funds to an account that the fraudster controls. Sometimes, they succeed, and the funds get into the hands of criminals. What do you do then?

Below are some examples that have been reported to us:

1. A lawyer's office received a last-minute redirection of monies payable on the sale of a property, which was a spoofed email from fraudsters.

   Without verifying the legitimacy of the redirection (other than by email with the fraudsters through the firm's law clerk), the funds were wired to the account of the fraudsters.

   It was later determined that the email account of the law clerk had been compromised (likely by guessing an easy password or the clerk responded to a phishing email.) It was by hacking into the law clerk's email account that the fraudsters learned about the transaction and were able to read and send genuine emails in furtherance of the fraud. The rules of the email account were re-written so that these emails were sent to folders other than the Inbox and Sent folders so the clerk wouldn't catch on.

2. A lawyer acted for the seller on a non- real estate transaction. The purchaser's lawyer attempted to cc them in an email, but sent the correspondence to an address that was one letter off from the real email address. In response, the purchaser's lawyer received instructions from this fraudulent email address with new trust account information and payment instructions.

   The purchaser's lawyer thought this was suspicious, and called the seller's lawyer, who was able to confirm that the instructions were fraudulent. Independent verification saved the day.

   It is unclear how the email hack occurred in the first place.

Three simple things you can do

1) Call before you click

If you receive instructions from a client, colleague, or other lawyer that involves a change in wire transfer account numbers or relates to a transfer of funds, always pick up the phone and call the individual to verbally confirm those instructions.

2) 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.

3) 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.

What should you do if this happens to you?

What to do immediately

Contact the bank

The person who initiated the wiring of funds should immediately report the diversion to the bank from where the wire was initiated, requesting that they stop the wire. This is not always possible as wires are usually instantaneously dispatched and irrevocable, however, they may get caught in the financial institution's suspicious transaction filters and be pending.

Also, request that they contact the bank they sent the wire to and so on until the trail disappears or the money is found and frozen.

Report to LAWPRO

File a claim (lawpro.ca/claim) with LAWPRO as soon as possible. Provide all the relevant documents in your possession.

Alert your client

Notify your client of the diversion fraud immediately and request that they consider whether their systems have been compromised and they should seek the assistance of IT professionals.

The systems of third parties with knowledge of the transaction (e.g., in the email thread) may have also been compromised. Speak with your client about similarly alerting such third parties to the fraud, with your client's permission. If no system was hacked, consider if this was an inside job.

What to do next

Notify the authorities

Report the matter to your local police as a fraud, and the Canadian Anti-Fraud Centre.

Review your other insurance policies

Consider filing a claim under other policies you may have intended to respond to this type of risk, including but not limited to professional liability excess coverage, cyber insurance, commercial general liability, crime, computer fraud, and fidelity insurance. It is important that you obtain complete copies of all your insurance policies, including the declarations, policy wordings, and endorsements, for purposes of analyzing the potential coverages available to you. Your insurance broker may be of great assistance to you in this regard.

Seek IT help

Obtain the assistance of an IT specialist if it appears that your systems were hacked. Even if you received a spoofed email from a fraudster, the fraudster may have hacked into your systems to determine when to make the request for the wire transfer and which client representative to impersonate.

Be prepared to act quickly and work closely with your insurer(s) and other professionals retained. Cooperation between the parties is vitally important in these types of situations. ■

Tips to avoid being a victim:

Review our article Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk

Verify instructions independently: Anytime you receive instructions to wire money to a bank account and especially if the instructions are changing previous instructions, 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.

Confirm instructions before a transfer: Advise your clients, or anyone you expect funds from, of the potential for a diversion attempt and to confirm the instructions before initiating the wire transfer.

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.

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

Stay up to date: For general cyber prevention tips, review our Cybersecurity and Fraud Prevention Tips, and subscribe to AvoidAClaim.com for fraud alerts.