BARRON'S

ADVISOR PRACTICE MANAGEMENT | ADVISOR POV

Advisors Are Frequent Victims of Wire Transfer Fraud. What to Do if It Happens to You.

By **Kenneth N. Rashbaum**, Barton LLP
July 15, 2022 1:30 pm ET

Wire transfer fraud is an endemic threat in our industry—and it's proliferating. Electronic transfers, which are commonly used by advisors to send requested funds to clients, are increasingly vulnerable to criminals who introduce malware into the computer systems of advisors or clients. They then impersonate the client and trick the advisor into misdirecting funds to their own accounts.

The FBI warns that business email compromise (BEC), also known as email account compromise (EAC), can be one of the "most financially damaging online crimes." If you are the victim of such a fraud involving a large transfer, there are ways to try to claw back the misdirected funds or recover them from sources other than the criminal. But you must act quickly—in such cases time is truly of the essence.

Upon discovery of the fraud, notify your bank and the receiving bank immediately and file a report on the FBI's Internet Crime Complaint Center site with as much information as you possess, including names and addresses of the originating and recipient banks, account and routing numbers of both banks, and the recipient bank's SWIFT number.

The originating bank can then initiate the FBI's financial fraud kill chain—if the following criteria are met:

- The wire transfer is $50,000 or more
- The wire transfer is international
- A SWIFT recall notice has been initiated
- The wire transfer occurred within the previous 72 hours

But let's say you don't discover the fraud for weeks. While that will be too late for your bank to reverse the transfer or for the FBI's fraud kill chain to be effective, there may be alternative means to be compensated for the loss.

First, along with a professional experienced in cyber insurance, review your cyber risk or technology errors and omissions insurance policy as it may provide coverage. Submit a notice of claim as soon as possible referencing the pertinent sections of the policy that indicate the existence of coverage and the limits of coverage for such a loss. Early notice of claim is crucial as the easiest way for a carrier to decline coverage is to allege late notice.

But let's say you don't discover the fraud for weeks. While that will be too late for your bank to reverse the transfer or for the FBI's fraud kill chain to be effective, there may be alternative means to be compensated for the loss.

First, along with a professional experienced in cyber insurance, review your cyber risk or technology errors and omissions insurance policy as it may provide coverage. Submit a notice of claim as soon as possible referencing the pertinent sections of the policy that indicate the existence of coverage and the limits of coverage for such a loss. Early notice of claim is crucial as the easiest way for a carrier to decline coverage is to allege late notice.

Once that's done, obtain a forensic examination of the systems on which you made the wire transfer. The usual modus operandi of wire fraud criminals is to introduce malware into a computer that can snoop on email exchanges and thereby learn of the impending funds transfer. Once they have introduced the malware (also known as spyware), they pretend to be the true recipient and send instructions to the advisor to send the funds to their bank.

Such malware is most often introduced through phishing. If your information system is operated by a third party whose lax security controls permitted the intrusion, you may have a negligence or breach of contract claim against that party.

Pick up the phone. Good practices, some decidedly low-tech, are the best way to reduce the risk of fraud before it occurs. Before completing a wire transfer, carefully examine the sender's email address by hovering your cursor over it. Compare it to previous emails received from the client well before the date of the wire transfer. Do they match exactly? If not, delete the instructions immediately as they were sent by a fraudster.

Remember telephone calls? Believe it or not, our smartphones still enable voice communication. The FBI recommends verifying payment and purchase requests in person, but if that's not possible, by phone. When doing so, verify any change in account number or payment procedures with the person making the request. Additionally, when you confirm the wire instructions verbally with a client, make sure the telephone number is one that you know independently from the client records and that it matches the wire instructions.

It's important to avoid email confirmation of a transfer as the fraudster has most probably hacked into the electronic correspondence and your confirmation email will go to them. If the client's instructions check out, confirm receipt by telephone and ask that confirmation of receipt be sent electronically.

Wire transfer fraud will continue to grow as more commerce is conducted through electronic means. In February, the FBI issued an alert warning of the rise of a variation of this scam involving virtual meeting platforms—another sign cybercriminals will keep expanding their strategies and advisors need to be vigilant.

Photo Illustration by Staff; Photography by Jill Lotenberg

Kenneth N. Rashbaum *is a partner at Barton, where he advises multinational corporations, financial services organizations, life sciences organizations, and other businesses that collect, use, and share electronic information in the areas of privacy and cybersecurity. He is also an adjunct professor of law at Fordham University School of Law. Prior to joining Barton, he was a senior litigation partner in the New York office of Sedgwick.*