How to Recover From Wire Fraud

Tom Cronkright, Published on March 25, 2019

Wire fraud happens. When it does, you have to move quickly to mitigate the loss. In theprevious post in this series, we wrote about how to protect yourself. While protection is important, it is an unfortunate fact that some fraud attempts are successful.

This post will explain how to recover if your company or customer is hit by fraud.

Understanding Why Recovering Funds is Difficult

Fraudsters move fast when they successfully convince a victim to wire money. When the stolen funds arrive in the fraudster's bank account, they engage a network of money launderers who immediately withdraw funds in cash, wire the money to a number of different accounts and/or convert it to cryptocurrency.

This is known as "money muling" and it involves an incredibly sophisticated network of people around the world, skilled in moving money in nearly real time to avoid detection and

recall.

When funds are wired to a fraudster, they typically land in an account belonging to a money mule. While some accounts are under the control of the cybercriminal, many are opened by people tricked or convinced by scammers to be a part of the money laundering process—often without the full knowledge of what they're participating in.

We have spoken previously about how the gangs that commit real estate fraud are often multinational, and they can use their connections to wire money through banks in other countries or cryptocurrency wallets.

The longer the trail between the original account—used to receive the transfer—and the money's final destination, the harder it becomes for the victim to see their money again. Because of this, it is essential that you act quickly when you realize you have become a fraud victim.

Knowing this, criminals use tactics to delay the time it takes for you to react. Many frauds take place on Friday afternoons, so people don't realize it has been committed until after the weekend.

This is particularly effective over federal holidays where the federal reserve and other banks are closed the following Monday. This gives fraudsters another business day to move money overseas once it's left in the United States so that it cannot be recovered.

Additionally, once you have started taking the steps below, fraudsters may contact you or your customer directly (remember, they have all your details). They may claim to be from the bank, title company or the authorities in an attempt to delay the recovery process by analogy in anomaly or suspicious activity in the fact they're looking into it and will be in touch in the next day or so.

Over the past year, fraudsters have shown a willingness to directly engage with the victim to disarm them, putting their mind at ease that the recovery is in motion and there's nothing further they need to do. Buying themselves just a few hours could mean the difference between a successful fraud and one where the money is recalled and sent back to the proper owner.

Ideally, you would let the receiving bank know about the fraud before the stolen money has even arrived in the fraudster's account. Often this isn't possible as wire transfers are nearly instantaneous from the time they are sent until they are received.

Even if you realize too late, the quicker you can follow the steps listed below, the higher a chance you have of recovering your money.

The Recovery Roadmap

The following tips will not guarantee you will get all your money back. However, it is a path that maximizes your chance of retrieving some money. In our own experience, we were able to recover a portion of the lost funds using this method.

Step 1: Contact your bank and initiate a “SWIFT recall“ on the wire transfer that left your account.

You first need to call your bank and let them know the transfer you made was fraudulent and that you are requesting a SWIFT recall to be initiated. You must have all the information about the wire funds transfer in front of you to properly initiate this request.

You also need to ask your bank to contact the fraud department of the receiving bank immediately so they can freeze the funds in the recipient account.

Alternatively, if the funds—or part of the funds—have already been moved, you’ll need to ask the bank to find out where the money was sent. Ask them to contact the third bank (or banks) to freeze the accounts that received the money.

Make a note of the banks and the accounts that received your money as you’ll need this information later.

Step 2: File a complaint with the FBI's Internet Crime Complaint Center (IC3)

The next step is to contact the FBI's Internet Crime Complaint Center. You'll need to provide information about the transaction, the scam itself, and the victim. It's a good idea to add details like the contents of the phishing email, links you clicked, etc. Once you have filed a complaint, the service will give you an IC3 Complaint Number. Make a note of this as you'll need it in step three.

It's worth noting that filing a complaint with the FBI is necessary but does not guarantee a real-time recovery effort. It's up to you to complete the remaining steps to increase your chances of recovery. Be aware that the FBI is flooded with complaints like yours each and every day so you need to stay vigilant and be your own advocate for recovery.

Step 3: Contact your local FBI field office and provide the IC3 complaint number

Find your local FBI field office at this link. You'll then need to contact them and report the details of the crime to the agent in charge of processing financial or cybercrimes. Following this, give them the IC3 Complaint Number and your personal contact information.

If you're an enterprise, now's the time to contact legal counsel to determine if an injunctive order is necessary. If so, send the order to the banks involved. This will ensure that all banks that received your money are no longer able to transfer funds from such accounts.

Step 4: Contact all banks that may have also received your funds

If the fraudsters manage to transfer your money to another bank (or banks), you now must contact these banks. Ask to speak to their fraud department about requesting a SWIFT recall and a 'fraud freeze' on the recipient accounts.

You'll have to provide information about the fraudulent transfers so the banks can identify the transfer and the account. Once the account is frozen, confirm with the bank how long the

freeze will remain in place and that the SWIFT recall protocol has been initiated.

Alternatively, if the money has already been moved on to a fourth bank account, you'll need to follow the same steps as above. You can even request the first bank you visit to send SWIFT recall and 'fraud freeze' requests to all other banks in the chain.

Don't only rely on them though. Repeat the steps until all the accounts that received your money are frozen and that the SWIFT recall protocol is in process.

Remember to write down the number you used to contact the bank, the time of the call, the name of the bank representative you spoke to, and their direct phone number and email address.

If you're an enterprise or business, this is time to contact your insurance provider if you have errors and omissions coverage, professional liability coverage, or any form of cybersecurity or cyber loss coverage.

Step 5: Contact local authorities and file a police report

Next, you need to contact the local authorities and file a police report. Give them all the information they may need. While you're doing so, save the incident number or police report number, and exchange contact information with local authorities for future communication.

Final step: Contact your security team, IT department, or consultant and initiate "The Information Technology Kill Chain"

The final stage of the process is to get your IT/Security team involved. If they haven't already acted out your incident response plan or if you don't have one, here's what you need to do.

First, contact your security team and request that they make an image of your system for forensic purposes. As tempting as it may be, try not to change anything on your system so the security team can see it exactly as it was when the attack occurred. You'll also want to use a clean loaner system to conduct business using a different temporary email address.

Now it's time to determine the source of the breach. Most wire fraud attacks result from Business Email Compromise (BEC). Which means a hacker has gained access to your email system, and it's up to you to find out how.

In more serious cases, the attacker may have installed malware on your machine or network that compromised your email and other credentials. If so, you have to act quickly to identify and eliminate the threat before other sensitive data can be used against you.

If warranted, eForensics investigators can be dispatched from a variety of sources to investigate the incident.

Knowing the Steps in Advance Will Help You React to Wire Fraud Effectively

Falling victim to fraud is an awful experience. Hear from recent fraud victims and the impact it had on their life. Take time in advance to create an internal system to execute immediately in the event of a wire fraud occurring. Reach out to your bank, FBI field office, network security team, legal counsel and your insurance company to align on expectations and protocols to maximize your chances of recovery. By following these steps, you will give yourself the best chance of recovery. Remember to download our full guide, "When Minutes Matter," to find out how to better prepare in the future.