# Wire Transfer Scams: What Happened to the Closing Proceeds?!

By: Ed Barkel, Lewis Roca Rothgerber Christie LLP

Closing day for a home purchase, a real estate transaction or the purchase of a business is always an exciting day. Unfortunately, internet thieves are targeting financial institutions, professionals and individuals participating in financial transactions seeking to steal wire transfers used to fund the deals. According to the FBI, between October 2013 and May 2016, thieves diverted or attempted to divert wire transactions valued in excess of $3 Billion.[1]

Hackers are very sophisticated and very crafty. A frequent scam works like this. Hackers target email accounts of realtors, title companies, business brokers, banks and law firms. They may even search press releases or social media looking for upcoming transactions and new targets. Once they hack into an email system, they use software to search for key words like "closing" and "wire transfer". The hackers then monitor email traffic to identify the date of a transaction, the parties involved in the transaction and wire transfer instructions. In most transactions, an email is circulated describing the breakdown of the closing proceeds, the parties to receive proceeds and wire instructions for each recipient. On closing day, the hacker will try to take over the targeted email account or mimic the sender's email by creating a new fake email domain that looks like the sender's email account.[1]


Then the hacker forwards the original wire transfer instruction email string substituting "updated wire instructions" for the targeted proceeds.

The parties sign the documents, the bank uses the "updated wire instructions" to deliver the purchase funds and everyone is happy, right? Yes, until the bank or the buyer's representative picks up the phone and is asked: "What happened to the closing proceeds?" At that point the money is gone and the buyer, seller, the bank and anyone who relied upon the bogus instructions will be pointing fingers at each other in an effort to avoid liability.

**Best Practice Tips from the FBI**[1]

- Be careful when posting deal information, job duties/descriptions and hierarchal information to social media and company websites. Hackers will lace emails with details designed to enhance credibility.
- Be suspicious of requests for secrecy or pressure to take action quickly. Be on heightened alert if you receive a request to hide changes to the transaction from deal participants or to move up wire transfer deadlines.
- The FBI recommends the implementation of security and verification procedures. For example:
  - Out of Band Communication: Establish other communication channels, such as telephone calls, to verify wire transactions. When using phone verification, use previously known numbers, not a number provided in an e-mail requesting a wire transfer or changing wire instructions.
  - Two-Factor Verification: Arrange a second-factor authentication early in the relationship and outside of the e-mail environment to avoid interception by a hacker. Examples include code words, passwords or authentication numbers. A phone call to verify modified wire instructions after the scam is in motion may be too late. If your company uses a VoIP internet phone system, a hacker who has penetrated your email system may also be able to access the VoIP system. The hacker may have the ability to intercept and redirect phone calls placed to verified phone numbers from the intended recipient to the hacker.
  - Forward vs. Reply: Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from your existing e-mail address book to ensure the intended recipient's correct e-mail address is used.
  - Train Employees to Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give hackers access to your computer system.
  - Two Factor Authentication (TFA): Consider implementing TFA for corporate e-mail accounts. Requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code) reduces the likelihood of access to an employee's e-mail account through a weak or compromised password.

**What to Do If You Are a Victim**

If funds are transferred to a fraudulent account, it is important to act quickly:

- Immediately contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
- File a complaint at www.IC3.gov

In summary, be aware of sudden changes in transaction or business practices. A request to change bank accounts, financial institutions or an email address is a glaring red flag. Before providing final authorization to wire funds, always verify the instructions via other channels to ensure that you are still communicating with the legitimate authorized counterparty. Finally, contact your insurance broker to review your cyber security and breach insurance. Standard fidelity bond, error & omission, director & officer and property & casualty policies are not likely to cover cyber breach or fraud claims.

To obtain additional information please contact: Lewis Roca Rothgerber Christie partners, Ed Barkel or Hillary Wells at http://www.lrrc.com. ***Ed Barkel*** *is the lead partner in the Lewis Roca Rothgerber Christie's Securities Litigation practice group. He defends broker-dealers and individual brokers in arbitrations and litigated matters. A significant portion of his practice is devoted to defending independent financial services firms and their advisors. He also provides consulting services in compliance-related matters including supervisory system design, special investigations, special supervision programs, branch office examinations and regulatory mandated consulting. His securities industry background enables him to offer unique "insider" insight, knowledge, experience and understanding to clients*

[1] https://www.ic3.gov/media/2016/160614.aspx