Wire Transfer Fraud: What You Need to Know and Why

Understanding what it is and how easily it happens

Wire Transfer Fraud is the act of defrauding funds from a company or individual through a scheme most commonly conducted through email communications. Typically, the bad actor will profile their target before the initial intrusion is conducted. By profiling, the hacker will study the people and processes within the organization and who has access and the authority to transfer assets. Because the target has been unknowingly profiled or surveilled for a period of time, the attacker will communicate in a very personalized, seemingly harmless, professional and familiar tone. According to FBI Special Agent Maxwell Marker: **"They know how to perpetuate the scam without raising suspicions. They have excellent tradecraft, and they do their homework. They use language specific to the company they are targeting, along with dollar amounts that lend legitimacy to the fraud. The days of these e-mails having horrible grammar and being easily identified are largely behind us."** (4)

Now that the target has been selected and the profiling has been completed, the bad actor may utilize a man-in-the-middle "MitMA" attack, "Spoofed Email Address" or injecting "Malware". MitMA is a type of eavesdropping technique where the hacker creates or alters messages between the victims. With the MitMA alteration technique, the hacker, rather than creating an entirely new wire transfer request, intercept an email mid-stream and may alter the amount, bank and account destination. Hackers may even clone deceptive invoices for a wire transfer that look, sound and feel as though they are legitimate using the proper language, logo, email signature lines and even the requestor's forged signature (which is acquired during profiling). To insure success, hackers will also request dollar amounts that do not raise suspicion and will go through without requiring additional oversight and secondary approvals.

In the spoofing or forged email example, the hacker will create a message requesting a wire transfer that appears ordinary without raising suspicion. All the while, the victims are deceived into believing they were communicating legitimately amongst themselves. With the spoofed attack, the email request to wire funds comes from a seemingly familiar address using your company logo, signature line and other similarities that have been acquired during profiling. By way of example, the following methods may be used to fool the recipient:

- The from address URL may be altered ever so slightly: john@abcin.com instead of john@abcinc.com
- The sender's name may be altered: johnsmith@abcinc.com instead of john.smith@abcinc.com
- Another URL alteration example: tedd@abcinc.com instead of tedd@abcinc.co

When a hacker employs malware to infiltrate an organization, the bad actor now has access to legitimate email threads concerning billing, procedures, people and invoices to assist in gathering intelligence before initiating the fraud.

Who is susceptible?

Every enterprise - large, medium and small. In fact, according to a recent article by the Cleveland Office of the FBI **"There is no profile for victim businesses. Victims range from large corporations to tech companies, to small businesses, to non-profit organizations. The schemers conduct research to learn about the employees in a company who manage the money, as well as the protocol necessary to perform wire transfers within that business environment. In some cases, information is obtained through a phishing scheme. In others, businesses may be victims of ransomware or other cyber intrusion prior to the B.E.C attack.** [(2)]

How much is being stolen?

According to a PWC article from July 2015 [(1)], in the past 18 months the cost to victims of wire transfer fraud is more than $1 billion. And, according to an FBI Public Service Announcement: **"The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses. The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong".** [(6)]

STATISTICAL DATA

The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses[1]. The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

Domestic and International victims:	22,143
Combined exposed dollar loss:	$3,086,250,090

The following BEC statistics were reported in victim complaints to the IC3 from October 2013 to May 2016:

Domestic and International victims:	15,668
Combined exposed dollar loss:	$1,053,849,635
• Total U.S. victims:	14,032
• Total U.S. exposed dollar loss:	$960,708,616
• Total non-U.S. victims:	1,636
• Total non-U.S. exposed dollar loss:	$93,141,019

The costs extend beyond monetary

In addition to monetary losses, companies that are attacked can be exposed to reputational damage, regulatory scrutiny and customers churn. In addition to the costs just described, a considerable amount of time and resources will be spent investigating and attempting to recoup a wire transfer fraud event.

If a victim, your recourse may be limited

Wire transfers are immediate, hard to reverse and quite commonly the defrauded funds are immediately withdrawn or transferred to another location which may be offshore. A great example is the Choice Escrow & Title cyber heist that occurred in March 2010. In this example, an unknown hacker stole credentials (username and password) to Choice's online bank accounts and initiated a wire transfer in the amount of $440,000 to an offshore account located in Cyprus. Following suits and counter suits between Choice and their bank (BancorpSouth), the judge ruled that Choice was responsible and BancorpSouth was not. **The judge cited in this ruling that Choice "failed to follow its recommended security procedures and therefore had only itself to blame, failed to implement commercially reasonably security measures, and the bank said it had specifically asked Choice to adopt a dual-control process where two individuals would be needed to sign off on all wire transfer requests. Choice officials had declined the control, despite being warned about the risk of fraudulent wire transfers, the bank noted in a motion seeking a summary dismissal of the lawsuit."** (5)

Suspicious Activity Reports ("SAR")

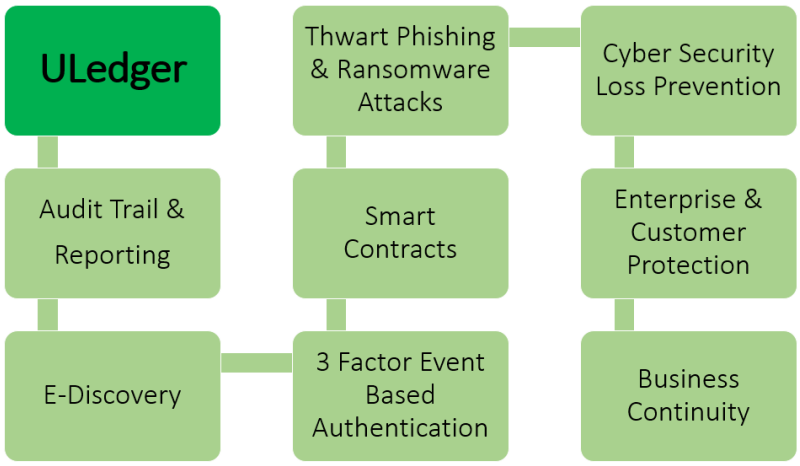
Financial institutions (i.e. banks and credit unions, securities dealers, insurance companies, mortgage companies and money service businesses) are required to file a SAR when there is suspicious or potentially activity. Reports are filed by those suspecting suspicious activity through the FinCen BSA E-Filing System within 30 days. FinCen is an agency of the United States Department of the Treasury with the ultimate goal of assisting the government in identifying those involved in fraud, money laundering and other crimes.

How to prevent or mitigate

Traditional technologies and methods including: IP Blocks, greylisting, firewalls, multi-factor authentication, threat detection & screening technologies, internal protocols and employee education are a start. Prevention requires a multi-faceted approach requiring technology, diligence, protocols and constant adaption as the hackers themselves are always adapting and finding new methods to infiltrate an organization and exploit a weakness.

A 3rd party defense - Your Digital Witness

How does one defend against this fraudulent activity that is growing exponentially? Uledger's ***3 Factor Event Based Authentication*** solution insures that you know with certainty who you are communicating with. Within Uledger's suite of services, all of your electronic communications including your authentication activities are encrypted at rest, immutable, permanent and logged to your dedicated ledger. The benefits include crucial assistance in audit, compliance, litigation, e-discovery while improving business continuity and mitigating social engineering and wire fraud attacks.



(1) http://www.pwc.com/us/en/cfodirect/assets/pdf/in-the-loop/wire-transfer-fraud-scams-executives.pdf
(2) https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals
(3) http://www.computerworld.com/article/2495894/cybercrime-hacking/victim-of--440k-wire-fraud-can-t-blame-bank-for-loss--judge-rules.html
(4) https://www.fbi.gov/news/stories/business-e-mail-compromise
(5) http://www.computerworld.com/article/2495894/cybercrime-hacking/victim-of--440k-wire-fraud-can-t-blame-bank-for-loss--judge-rules.html
(6) https://www.ic3.gov/media/2016/160614.aspx