Attackers have stolen billions of dollars from unsuspecting companies over the years by posing as employees, vendors, or partners to initiate fraudulent wire transfers. The FBI released a public service announcement in May 2017 warning about these sophisticated business email compromise (BEC) scams and reported exposed dollar losses of $5.3 billion — a 24x increase from two years prior.

In contrast to previous years in which attackers used URLs or malware to initiate their attacks, BEC-based attacks use emails that impersonate high-level officers or managers in the company to get ahold of wire funds or personally identifiable information (PII). In some cases the attackers impersonate vendors or partners leveraging social engineering to substantiate the request.

Financial Institutions a Prime Target

While BEC hits all major business sectors, it is particularly relevant in the financial services sector for a number of reasons. First, financial institutions are targeted by the various scams outlined below just as aggressively as firms in other sectors. Second, there are risks related to the client relationship that come into play, which represent a paradigm shift in how these attacks are being conducted. For example, with BEC attacks, the institution is conducting a transaction on behalf of a real client yet the bank has no way of knowing that the request is being made on behalf of an impersonated officer of the company. Often the client will become confused during the process and may lose trust in the security of the financial institution due to the incident. According to SC Magazine, “For 2016 there were 1,684 attacks on financial services firms, an attack being defined by IBM as a security event identified as ‘malicious activity that is attempting to collect, disrupt, deny, degrade, or destroy information system resources of the information itself’. This is up from the 1,019 attacks that took place in 2015.”

Beyond monetary and personal information losses, however, there are other risks in the Financial Services sector including liability when customer accounts are compromised, as well as potential compliance risks.

How Money Flows in BEC

Understanding the risks and mitigation steps for BEC requires a clear understanding of how these scams are initiated, what the various roles are, and how money flows from the victimized bank to the attacker. Let’s look at a generic example of how it works.

“In 2016 there were 1,684 attacks on financial services firms, an attack being defined by IBM as a security event identified as ‘malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources of the information itself’. This is up from the 1,019 attacks that took place in 2015.”

— SC Magazine

There are three common entities in a typical BEC attack: the attacker, the financial institution(s), and the money mule. While the first two are familiar to most, the money mule is worth some explanation. In order to receive money from a victim, an attacker needs someone as a go-between. This person may be an unsuspecting victim of a romance scam. Often the scammer will cultivate an online relationship with this person until they have reached a point in which the scammer can ask for a favor: to accept money on their behalf — into their U.S. bank account — so that it can be forwarded to the scammer’s account.

As the scam progresses, the money will be transferred from account to account, over international borders, so that it becomes vastly more difficult to trace. It is worth noting that in this diagram, five of the eight entities depicted below are financial institutions, hence the need for companies in the Financial Services industry to be particularly vigilant.
Four Types of BEC Scams

There are four basic BEC schemes: the fake invoice scam, finance industry wire fraud, fake lawyer scam, and human resources scam. These are described below, after which we show an actual recent attack on Agari in which a wire fraud attempt was initiated.

Fake Invoice Scam

Sometimes called the Supplier Swindle, this attack typically involves the impersonation of a company’s trusted supplier. This type of attack has made headlines recently with Google and Facebook being conned out of $100m.²

The attacker, in this scheme, requests funds to be wired for an invoice payment but instead of being a legitimate account for that supplier, it is a fraudulent account. This impersonation is often achieved using a spoofed email and relies on social engineering.

CFO/CEO Wire Fraud Leveraging Financial Services

In this scam, attackers identify themselves as high-level executives of the target firm such as the CEO, CFO, or COO. They typically pretend to be handling urgent, confidential matters and request a wire transfer to an account within their control (e.g. the money mule’s account). In some situations they make the request directly to the corporation’s financial institution insisting funds be sent urgently.

² "Facebook and Google Were Conned Out of $100M in Phishing Scheme,” The Guardian, April 28, 2017.
Fake Lawyer Scam

In this scam the attacker contacts employees pretending to be a lawyer with Corporate Counsel or another law firm. They often claim to be handling confidential and time-sensitive matters. They request the employee to handle a transfer of funds. The request may reference matters which are actually occurring at the company like a merger or acquisition. It may be timed near the end of the business day when employees are tired and/or in a rush to leave their desk and more vulnerable to mistakes.

Human Resources Scam

Here, the attacker poses as someone from a specific functional area in the company, most typically, an employee in Human Resources. The account of this employee is compromised or spoofed and used to send the request. However, instead of asking for money, they ask for personally-identifiable information (PII). Once received, this information can be used itself to make money or it can be used as a jumping off point for a more damaging attack against the company.

Most of these scams use social engineering but do not require detailed knowledge of the victim. Unlike phishing attacks, BEC scams use low-volume email campaigns to avoid being flagged as malicious. In BEC attacks the victims are tricked into doing the transfers for the attacker.
Best Practices to Inhibit Fraudulent Transactions

While the data above may present a somewhat gloomy picture for enterprises today, and especially for financial institutions, there are things you can do to protect yourself. First, there are practical suggestions for improved business processes provided by FSISAC in our BEC Fraud Alert. Some of these include:

1. Confirm any change-in-payment instructions by phone using an independently-acquired phone number — not from the electronic communication.
2. Maintain a file of vendor contacts for those authorized to approve changes in payment instructions.
3. Limit the number of employees who have the authority to conduct and/or approve wire transfers.
4. Use out-of-band authentication to verify requests such as calling the executive for verbal verification, establishing a PIN, or sending the executive a text with a one-time PIN and a phone number to use for approval.
5. Delay any wire transfer requests coming from a bank until additional verifications can be performed.
6. Require dual approval for large sums or any new business relationships.

Automating the Protection of Your Organization

While the above best practices may help, the best solution is to use email security technology to ensure attacks never reach employees’ inboxes in the first place.

Agari focuses on protecting corporations from BEC by discerning identity deception, thereby identifying inauthentic emails so that employees never receive the attack in the first place. The Agari Identity Graph™ looks closely at the identity of the alleged sender by modeling good sender behavior based on trillions of emails worth of data and billions of new emails passing through the system each day. We eliminate spoofing all together by addressing the three primary email attack methods:

- **Display Name Deception:** the email display name looks like a trusted brand or known contact but doesn’t match the actual email address.
- **Look-alike Domains:** actual, registered domains that are constructed to look like other, recognized brands.
- **Exact Domain Spoofing:** inauthentic emails are created using the actual domain of the inbound company, which are allowed through if companies do not have DMARC in place.
Actual Attacks Engaged by Agari

BEC attacks are common enough that finding an example of a real-world attack is not difficult. Agari was able to not only detect these attacks (mostly waged on our customers but some of them directly on Agari) but described below was actually targeted at Agari’s founder, Pat Peterson and detected by our software. Our researchers then engaged with the attacker. Here are the details.

A $44,000 Wire Fraud Attempt

This actual wire fraud attempt was sent to Agari requesting $44K in funds. After the initial contact was made by the attacker, we responded and got a subsequent request for the wire transfer. After contacting the financial institution to which the attacker requested funds be transferred, the account was closed by the institution.

Engaging with the Attackers

Of the many attacks we have seen, we selected 20 attacks with which to engage; some interesting data came out of these interactions. The map below shows the location of the email servers from which the attacks came, the banks to which the wire requests were directed, the money mules, and the scammers. While the servers, banks, and money mules were predominantly in the U.S., the attackers were mostly on African soil.
As we pursued the closure of the bank accounts with the respective financial institutions, this process uncovered a number of other accounts related to the same attacker(s) which were also closed. One interesting piece of data was uncovered when we sent a “dummy” check to one attacker. In working with FedEx to determine who was tracking the package, they discovered 600 other packages that had been tracked by the same individual. BEC has, indeed, become big business for cyber criminals.

About Agari

Agari is transforming the legacy Secure Email Gateway with its next-generation Secure Email Cloud powered by predictive AI. Leveraging data science and real-time intelligence from trillions of emails, the Agari Identity Graph™ detects, defends and deters costly advanced email attacks including business email compromise, spear phishing and account takeover. Winner of the 2018 Best Email Security Solution by SC Magazine, Agari restores trust to the inbox for government agencies, businesses, and consumers worldwide. Learn more at www.agari.com.