Business email compromise and executive impersonation: are financial institutions exposed?

David Zweighaft

Abstract

Purpose – *To explain the fraud schemes known as business email compromise (BEC) and executive impersonation that are growing in popularity, and the threat they pose to financial institutions.*

Design/methodology/approach – *This article explains BEC and executive impersonation and how they are carried out, and discusses how regulations and practical operational steps are trying to address this fraud issue.*

Findings – *Financial institutions should understand the potential for legal and regulatory risks posed by BEC and executive impersonation, and consider taking steps to create a proactive, culture of skepticism and heightened awareness to combat this type of fraud.*

Originality/value – *This article is adapted from the original report issued by the American Institute of CPAs and has been updated to address specifics concerning financial institutions.*

Keywords *Data breaches, Identity theft, Business email compromise (BEC), Cyberattack, Executive impersonation fraud, Financial institutions*

Paper type *Technical paper*

David Zweighaft (dzweighaft@dszforensic.com) is managing director at DSZ Forensic Accounting and Consulting Services LLC in New York, New York, USA.

The regular disclosure of data breaches continues to concern consumers and corporations. One form of cyberattack risk on the rise: business email compromise (BEC). In 2015, the FBI's Internet Crime Complaint Center (IC3) issued three public service announcements[1] related to the use of a company's email system to criminally extract funds, noting that in 2014 US companies lost $179 million[2]. The number of BEC attacks became so prevalent that the American Institute of CPAs in 2016 issued a report[3], which I authored, to provide guidelines on how to address the topic. Much of the content of this article is from that report.

BEC is a variation of the practice of *spear phishing*, in which spoof or fraudulent emails are directed at company personnel in an attempt to obtain account numbers, access codes, or other sensitive information. The newest incarnation of this scheme is more sophisticated, requires significant research and diligence on the part of the criminal hacker, and can have a huge financial impact on the victim company.

That scheme is *executive impersonation*. The perpetrator is a criminal creating a fake email that closely resembles the victim company's own email and appears to come from a high-ranking executive. The recipient is an unsuspecting mid- or lower-level employee selected for his or her access and authority to transfer large sums of money between subsidiaries or to suppliers on behalf of the company.

BEC scams usually begin in one of two ways: by getting an unsuspecting employee to click on an email attachment that compromises the network (that is, malware), or by sending an email impersonating a high-ranking official in the company. Sophisticated hackers,

however, usually research their target and the company as a whole in order to craft highly convincing emails. Using information gleaned from mining corporate websites and social networks, the impersonations used in the BEC emails can be extremely accurate and convincing. Because the email appears to come from a known and trusted source, the request to release valuable data or take urgent action appears more plausible[4].

In order for a BEC scheme to be successful, the criminal researches social media, the business press, and other company resources to get information about the corporate culture; the executive's personality, phrasing, and use of language; the target employee's position and responsibilities; and information about other employees in the corporate accounting or treasury group. This information is then translated into a carefully crafted "look-alike" email, purportedly coming from the executive, requesting an emergency transfer, immediate payment of an urgent invoice, or payment in anticipation of an undisclosed merger or secret acquisition. The request is usually characterized by a high degree of urgency ("ASAP" or "immediately").

The psychology behind BEC's success is that the employee is motivated to be responsive to the executive's request and is willing to bypass the typical controls associated with a normal wire transfer request. The more credible the appearance of the email, and the more authentic the tone and wording of the message, the more likely it will succeed. To enhance the authenticity of the scheme, the fraudulent email generally contains attachments on company letterhead directing the target employee to wire corporate funds to a particular person (usually a trusted vendor contact) at an overseas bank.

Key characteristics

The following are important characteristics of an executive impersonation cyberattack:

- Email requests come from a senior (C-suite) executive or a key vendor or supplier.
- The email address is substantially similar to the purported sender's address, with very minor, subtle differences. For example, if the actual address is CEO@victimco.com, the impersonator address might be CEO@vicitmco.com. Alternatively, the email display name may appear correct, but when the cursor hovers over the email address, a different underlying address is displayed.
- Requests occur when the executive is traveling and cannot be contacted.
- There is an element of urgency or secrecy regarding the disbursement.
- The amount is within the normal range of transactions so as not to arouse suspicion.
- Other employees are referred to or copied in the email, however, their email addresses are modified as noted previously.
- Requested payments are payable to a foreign bank.

The two most common variations of BEC schemes are the urgent transaction request from the boss and the strong-arm vendor request.

In the *urgent transaction request from the boss*, a corporate accountant receives a spoofed email that appears to be from the CEO of the company requesting an urgent wire transfer relating to a top secret acquisition. The email contains instructions to wire corporate funds to a new bank account of a known business partner at an offshore bank. The accountant, wishing to appear responsive to his or her boss, drops everything and wires the funds immediately. By the time the accountant and CEO speak in person and realize the error, the money is long gone from the fraudulently opened offshore bank account.

In the *strong-arm vendor request*, a business receives a fraudulent invoice from what appears to be a long-standing supplier requesting that the next payment be sent via wire to an alternate account. The fraudulent email contains a PDF file of an invoice that appears

to be from the trusted supplier, and the email text and header information appear to contain the hallmarks of an actual business communication from the supplier. Because the supplier is located overseas and in a different time zone, it is common practice that communication about payment of invoices be done electronically, rather than verbally. The unsuspecting business wires the funds to the new account, and the money disappears almost immediately. Weeks later, the legitimate supplier follows up with the business, sending an angry email expressing frustration that the funds were not sent in a timely manner. When the two business partners realize the mix-up, it is too late to recover the funds.

Financial institutions are not immune to this this type of fraud. Consider the experience of Wells Fargo as an example. On November 6, 2012, a registered representative at Wells Fargo Advisors received an email from customer "GS" with an attached letter of authorization (LOA) requesting the transfer of $18,971 from the customer's brokerage account to a third-party account in Lima, Peru. As it turned out, the email was not sent by customer GS, but by an imposter.

Per the regulatory proceedings, the "email address was not one known to be associated with the customer, but contained the customer's name in the email address".

Under such circumstances, it would appear that the sender's use of a previously unknown address might have alerted the representative and others to be wary – or at least make sure to follow the firm's protocols for handling such email requests. In fact, the records assert that the representative did not call the customer to confirm the wire request, but merely processed the transfer. Worse, the record alleges that the representative "falsely claimed that he had spoken with GS, that he knows him personally and recognized GS's voice. [He] falsely entered 'pmt to friend for personal loan' in the Service Request as the intended purpose for the wire".

On December 5, 2012, the representative received a second email from an imposter with attached LOA seeking a transfer of an additional $48,561 to the Lima account. It is unclear from the record whether this second email came from the same imposter as the November 6 communication. The record explains that "[t]his email was a variation of the email address used in the November 6, 2012 request and was also not an email address associated with the customer".

In response to this second transfer request, the representative again did not call the customer to confirm and went ahead and processed the wire and also offered the same false assurances to his firm concerning his efforts at verification[5].

Wells Fargo was fortunate because the amounts involved were in the tens of thousands of dollars. Other companies have faced liability in the millions of dollars.

Are financial institutions prepared?

Spear phishing in the form of executive impersonation attacks is the newest weapon in the cyber-criminal arsenal. It is being used more and more frequently because it is effective and difficult to investigate and prosecute. This scheme is occurring worldwide, and there is no silver bullet to prevent these attacks.

These BEC schemes, like others that prey on human fallibility, can be mitigated. More robust controls, including two-step authentication of transactions, enhanced employee awareness training, informed verification of transfer requests and evolving IT controls can detect BEC attempts before they result in losses. These same policies and procedures indicate a company's intent to implement reasonable safeguards to prevent data breaches, which will be questioned in the event of a lawsuit or government investigation following the material event.

With respect to financial institutions, relying on regulatory alone guidance to build appropriate defenses to BEC and executive impersonation will leave these institutions vulnerable to these schemes.

Current regulations

The risks of cybersecurity attacks have been addressed by the US Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) in an effort to raise awareness and require policies and procedures to address and mitigate the risks to accountholders, individual institutions, and the industry as a whole. Based on current regulations and standards, the risk landscape under consideration encompasses systemic cyberattacks (e.g., hacking, penetration, distributed denial of service, *force majeure* events), organized criminal activities, such as money laundering, and acts of terrorism[6]. However, they do not address the specific issues of BEC and executive impersonation.

The SEC in November 2014 adopted Regulation Systems Compliance and Integrity and Form SCI to strengthen the technology infrastructure of the US securities markets. This required key market participants to have comprehensive policies and procedures in place surrounding their technological systems as part of the Electronic Code of Federal Regulations (e-CFR Title 17, Chapter II Part 248, Subpart C)[7]. Within this part of the regulations is Regulation S-ID (Identity Theft Red Flag Rules), which has its provenance in the Fair Credit Reporting Act of 1970 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010[8]. While this regulation is focused on protecting the private information and customer assets relating to an individual's account, the specific recommended safeguards do not contemplate the potentially catastrophic effects of a single BEC event, which could wipe out an entire account balance, for either an individual or a corporate investor.

Admittedly, it is unrealistic to expect regulatory guidelines to address the growing myriad of specific fraud scheme risks present in the business environment. Real-time changes in technology, business models and other regulatory pronouncements would render transaction-specific regulations obsolete before the ink was dry. Instead, the language of Regulation S-ID focuses on the need for the financial institution or credit card issuer to "detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account"[8].

The first section of Regulation S-ID sets forth the scope of the regulation and the required definitions and enumerates what is required to establish an Identity Theft Prevention Program. Within this regulation, "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft[9].

With respect to Red Flags of Identity Theft, the required elements of the program include policies and procedures to (i) identify, (ii) detect and respond appropriately to any Red Flags that are encountered, and (iii) ensure that the program is updated periodically to remain responsive to the current risk environment.

Notably lacking were any mention of the variants of Identity Theft that are central to BEC or executive impersonation schemes discussed elsewhere in this article.

Granted, within Appendix A to Subpart C of Part 248 (Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation), there is broad language assist in establishing a program to meet the requirements of Regulation S-ID. This contains guidance of a more operational nature, including:

- *Identifying relevant red flags* – what types of information to consider in assessing the Identity Theft risk universe
- *Detecting red flags* – obtaining and authenticating identity information

- *Preventing and mitigating identity theft* – responding to breaches of cybersecurity (data breaches) and having protocols in place to contact customers, monitoring subsequent account activity, and determining the necessity of changing customer account numbers and other information.
- *Updating the program* – responding to changes in technology, new fraud schemes, changes in the entity's business model and product/service offerings.
- *Administering the program* – oversight and ownership of the program at the appropriate level of management, proper design of policies and protocols and periodic testing, reporting and review of the program's operating effectiveness.
- *Other applicable legal requirements* – compliance with relevant regulations (e.g., Bank Secrecy Act, Patriot Act, FCPA).

However, an element specifically called for in the establishment and administration of the program is to "Train staff, as necessary, to effectively implement the Program"[10]. This is a key element for the effective operation of any anti-fraud program that also can play a critical role in preventing, deterring and detecting BEC schemes and identity theft.

When these schemes are examined from a distance, BEC and identity theft have an almost "chicken-and-egg" relationship, because the initial email allegedly from the executive requesting the funds transfer is the condition precedent necessary to execute the crime. This is identity theft in its most unvarnished form.

In the context of a covered account at a financial institution, a current Identity Theft Prevention Program protocol for requests to purchase or liquidate investments, move funds, or other transactions typically requires that requests be initiated over a recorded or monitored phone line, via an online trading portal, or other means. These requests are often verified by two-factor authentication which limits the risk of spoofed or impersonated emails. However, on some occasions, a manually signed transaction order attached to an email may be sufficient to initiate an order. Given the current state of technology, the existing access and transaction controls relating to all of these methods can be circumvented. Increased training for employees can make a critical difference in addressing situations of identity theft and BEC by ensuring the effectiveness of these safeguards or in backstopping lapses in protocol.

Yet, the training that staff receives relating to identity theft and other anti-fraud programs may be insufficient in the current environment. Institutions offer rapid order execution as a selling point to their institutional clients, touting effectiveness and efficiency. Rarely are compliance and transaction risk management mentioned as benefits. In a transaction-focused organization, the institutional goals of greater volume at reduced cost may cause employees to place greater emphasis on performance and less on compliance.

Therefore, the issue becomes how to better create a compliance-focused organization. This occurs at the recruiting and hiring stages of employee training. Instead of hiring employees who excel at following organizational dogma and not questioning directions, they should instead be instructed in skepticism and ensuring that all transactions are in fact being initiated by bona fide, authorized individuals. Such training at all levels of the organization will result in the development of a more robust anti-fraud culture and a related lower incidence of fraud events.

Awareness, training, repetition

What the regulations refer to as preventing, deterring and detecting, I like to call awareness, training and repetition. Whatever mantra you prefer, it represents the most important factors in foiling BEC-type cyberattacks.

Compliance and training are often viewed by management as expensive and impediments to the efficiency of operations. When compared the cost of data breaches, customer account compromises, and identity theft, the business case favors compliance training.

In a study by the Ponemon Institute of 383 companies that experienced data breaches in 2016, the average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158 in this year's study. Regulated industries, such as healthcare and financial services, have the costliest data breaches ($355 and $221 per account record, respectively) because of fines and the higher than average rate of lost business and customers. In the United States, of 64 cases reported, the root cause frequencies and related per account record costs were given in Table I[11]:

The study also noted that "abnormal churn grew 2.9 per cent, which is defined as the greater than expected loss of customers in the normal course of business. The loss of customers increased the cost of data breach [. . .] Industries with the highest churn are financial, health and services [. . .] While a small sample size prevents us from generalizing the effect of industry on customer churn rates, financial, health and service organizations experienced relatively high abnormal churn" of 6.2, 5.3 and 5.1 per cent, respectively[12].

With the business case hopefully established, financial institutions should consider the following recommendations to prevent BEC and executive impersonation fraud from happening to them:

- Increasing the frequency of training for employees responsible for wire transfers, and placing a focus on educating them about BEC schemes like executive impersonation and data security.
- Engaging cyber-risk security consultants to identify, monitor and mediate spear-phishing threats, including identifying employee-targeted attacks on social networks, finding and taking down fraudulent and impersonating accounts, and continuously monitoring important employee and company accounts for signs of compromise.
- Reviewing policies and procedures for requesting, initiating and approving wire transfers. Email requests should be verified by phone calls to company-registered phones. Require two employees to approve wire requests and authenticate the recipient's identity before the wire is released.
- Conducting a risk assessment of the wire transfer process to identify weaknesses that could be exploited. Identify "look-alike" domains and register them in the name of the company to prevent hackers from attempting BEC attacks.

While awareness, training and repetition are the best steps you can take to prevent executive impersonation fraud, when this type of cyberattack is suspected, early mobilization and assessment of the impact are crucial. A company should be ready to quickly assemble a response team, including in-house counsel, the CIO and staff responsible for IT security, and outside consultants.

Working under the direction of outside counsel under attorney-client or attorney work-product privilege will facilitate an internal investigation to gather all the relevant facts for management and the board of directors to keep them apprised of all developments and support their decision-making. Proceeding in this manner will also provide a foundation for

Table I

Root cause	*Frequency (%)*	*Cost per capita*
Malicious or criminal attack	50	$236
System glitch	27	$213
Human error	23	$197

responding to law enforcement and government investigators in the event the breach must be reported.

Conclusion

Current regulations do not provide sufficient specific guidance for implementation of programs to prevent, deter and detect identity theft and BEC schemes. Financial institutions should consider instituting more robust training and proactive prevention programs, balancing the cost of such programs with the potential for legal and regulatory risks, and lost revenues due to customer account defection as a result of such events. To prevent BEC-type fraud from occurring, they should consider taking steps to create a culture of skepticism and heightened training and awareness that focuses on making staff aware of this type of fraud, providing appropriate training to recognize it, and repeating this information to staff frequently.

For those interested, the AICPA's Forensics and Valuation Services specialty subject area, which supports the Certified in Financial Forensics (CFF) credential for CPAs, offers a wealth of information to assist companies in dealing with fraud and cyberattacks. Information on combatting fraud can be found at www.aicpa.org/InterestAreas/ForensicAndValuation/Pages/ForensicValuationHome.aspx

Notes

1. I-012215-PSA Business Email Compromise, I-082715a-PSA Email Account Compromise, and I-082715b-PSA Business Email Compromise posted on available at: www.IC3.gov
2. I-012215-PSA Business Email Compromise.
3. David Zweighaft, *Eye on Fraud, Spring 2016, Issue 1*, (American Institute of CPAs, 2016).
4. See available at: www.martindale.com/business-law/article_Jones-Day_2216506.htm
5. See available at: www.brokeandbroker.com/2667/awc-email-/
6. FINRA Report on Cybersecurity Practices – February 2015, p. 4.
7. Available at: www.ecfr.gov/cgi-bin/text-idx?SID=5621786ec1a831400e4b64f3e92198bd&mc=true&node=pt17.4.248&rgn=div5#sp17.4.248.c
8. SEC.gov-rules-final-2013-34-69359.
9. 248.201(b)(10).
10. 248.201(e)(2)(3).
11. 2016 Cost of Data Breach Study: Global Analysis, pp. 10-12. Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC June 2016, available at: www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
12. 2016 Cost of Data Breach Study: Global Analysis, p. 17.

Corresponding author

David Zweighaft can be contacted at: dzweighaft@dszforensic.com