Best Practices for Businesses to Detect the Business Email Compromise (BEC) Scam

CHECK. CONFIRM. COACH.

These best practices are based on the FBI alerts and conversations with financial institutions that have successfully detected this scam. This is a comprehensive list, and most businesses cannot practically implement all of these suggestions but implementing those that are realistic and practical for your specific operations and resources will decrease the risk of being victimized by this scam.

CHECK

- ☐ Check to see if the request is consistent with how earlier wire payments have been requested. How often does the CEO or CFO directly request a wire payment? Do they typically submit requests when traveling (these attacks often are timed when the executive is out of the office)? Have earlier requests included the phrases “code to admin expenses” or “urgent wire transfer”, which have been reported by victims in some of the fraudulent email requests?
- ☐ Check to see if the payment is consistent with earlier wire payments – including the timing, frequency, recipient, and country to which prior wires have been sent.
- ☐ Be suspicious of requests for secrecy or urgency, and emails that request all correspondence stay within the same email thread, such as only use Reply, not Forward.
- ☐ Establish a company domain for company email instead of using open-source email services such as Gmail. Businesses using open-source email are most targeted. Register domains that are slightly different than the actual company domain and might be used by fraudsters to spoof company email.
- ☐ Look carefully for small changes in email addresses that mimic legitimate email addresses. For example, .co vs .com, abc-company.com vs abc_company.com, or hijkl.com vs hljkl.com. If you receive an email that looks suspicious, forward it to IT for review.
- ☐ Program your email system to add “-e” to the end of all external senders’ email addresses, thereby flagging email coming from domains that don’t match the company domain. The system will detect minor changes to the domain name and flag it as external, making it easier for employees to detect fraudulent emails.
- ☐ If you don’t need web access to email, turn webmail off as it provides another attack point for criminals. If you must provide web access to email, limit accessibility by implementing VPN or another security control.
- ☐ If the request is from a vendor, check for changes to business practices. Were earlier invoices mailed and the new one is emailed? Were earlier payments by check and they’re now asking for a wire transfer? Did a current business contact ask to be contacted via their personal email address when all previous official correspondence used a company email address? Is the location or account to which the payment is to be sent different from earlier payments to that vendor?

CONFIRM

- [ ] Use an alternative mechanism to verify the identity of the person requesting the funds transfer. If the request is an email, then call and speak to the person using a known phone number to get a verbal confirmation. If the request is via phone call or fax, then use email to confirm using an email address known to be correct. Or forward the email (instead of using Reply) and type in a known email address. Don't reply to the email or use the phone number in the email.
- [ ] While many people may be hesitant to question what appears to be a legitimate email from their boss or the CEO, consider which would be worse in light of how common this scam is: asking the CEO or CFO to reconfirm the request, or having the money stolen.
- [ ] Limit the number of employees who have the authority to submit or approve wire transfers.
- [ ] Implement dual approvals for financial transactions. If you do not have written procedures, develop them. Avoid having the two parties responsible for dual approvals in a supervisor/subordinate relationship as it could undermine the effectiveness of the process. Once they're in place, be sure to always follow established procedures.
- [ ] Use a purchase order model for wire transfers to ensure that all payments have an order reference number that can be verified before approval.
- [ ] For employees that frequently travel and are authorized to request funds transfers, develop a unique way to confirm requests. Perhaps develop a coding method that isn't documented within the network (in case of an intrusion search).

COACH

- [ ] Spread the word. Coach your employees about this type of fraud and warning signs. Alert receptionists, admins, and others to not provide executive's travel schedules over the phone to unknown callers. Be suspicious and diligent and encourage employees to ask questions.
- [ ] Be careful what is posted to social media and company websites, especially reporting structure and out of office details. Criminals have been known to launch the attacks when they know the CEO or CFO is traveling and therefore not easily available to confirm the request.
- [ ] Slow down. Fraudsters gain an advantage by pressuring employees to take action quickly without confirmation of all the facts. Be suspicious of requests to take action quickly.
- [ ] Trust your financial institution. If they question a payment, it's worth a couple minutes to cooperate with them to confirm it's legitimate.
- [ ] Executives need to be tolerant and supportive of employees' double-checking requests.

What to do if you're hit by the BEC Scam

Report the Attack

Businesses that have been victimized by the BEC scam (regardless of dollar amount), are encouraged to file a report with the IC3 at www.IC3.gov or contact their local FBI office.

Businesses also are encouraged to contact their financial institution to report the attack, ideally within 24 hours, after which it is rare that funds can be recovered.

Timing is critical. If notified immediately, financial institutions and law enforcement have a better chance of recovering the stolen funds, even if the funds were sent internationally. Waiting even 24 hours to report an incident can greatly diminish law enforcement's ability to recoup funds.

When reporting the incident, identify the complaint as "Business Email Compromise" or "BEC" and provide:

- ✓ A general description of this crime, how and when it occurred
- ✓ Header information from the email message the executive sent internally to request the funds transfer
- ✓ The specific wiring instructions, including beneficiary and account details for where the transfer was to be sent
- ✓ Attempted and actual loss amounts
- ✓ Details on when and how you believe you were defrauded
- ✓ Other relevant information you believe is necessary to support your complaint

Keep all original documentation, emails, faxes, and logs of all telecommunications. You will not be able to add or upload attachments with your IC3 complaint if it's filed online; however, retain all relevant information in the event you are contacted by law enforcement.

Complete an Internal Review

Businesses are encouraged to conduct an internal review to determine how the attack occurred and if changes are needed. Specifically:

- ✓ Was the email system hacked, giving criminals access to executive's email accounts? If so, are additional protections in order?
- ✓ What actually happened, and who was involved? This may indicate where training is needed or if there might actually be an insider element to the attack, although this is rare.
- ✓ What allowed the attack to happen? Do processes and controls need to be revised to prevent such a loss again?

Federal Financial Institutions Examination Council (FFIEC) has provided the following Appendix:

Threat Landscape and Compensating Controls

Threats

Federal Agencies are concerned that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement. Many of these schemes target small to medium-sized business customers since their account balances are generally higher than consumer accounts and their transaction activity is generally greater making it easier to hide the fraudulent transfers.

An effective tool in the fraudster's arsenal is keylogging malware. A keylogger is a software program that records the keystrokes entered on the PC on which it is installed and transmits a record of those keystrokes to the person controlling the malware over the Internet. Keyloggers can be surreptitiously installed on a PC by simply visiting an infected website or by clicking on an infected website banner advertisement or email attachment. Keylogging can also be accomplished via a hardware device plugged into the PC which stores the captured data for later use. Keylogger files are generally small in size and adept at hiding themselves on the user's PC. They often go undetected by most antivirus programs. Fraudsters use keyloggers to steal the logon ID, password, and challenge question answers of financial institution customers. This information alone or in conjunction with stolen browser cookies loaded on the fraudster's PC may enable the fraudster to log into the customer's account and transfer funds to accounts controlled by the fraudster, usually through wire or ACH transactions.

Other types of more sophisticated malware allow fraudsters to perpetrate man-in-the middle (MIM) or man-in-the browser (MIB) attacks on their victims. In a MIM/MIB attack, the fraudster inserts himself between the customer and the financial institution and hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are funds transfers to accounts controlled by the fraudster. The fraudsters conceal their actions by directing the customer to a fraudulent website that is a mirror image of the financial institution's website or sending the customer a message claiming that the institution's website is unavailable and to try again later. Fraudsters may have the capacity to delete any trace of their attack from the log files.

MIM/MIB attacks may be used to circumvent some strong authentication methods and other controls, including one-time password (OTP) tokens. OTP tokens have been used for several years and have been considered to be one of the stronger authentication technologies in use. Since the one-time password is generally only good for 30-60 seconds after it is generated, the fraudster must intercept and use it in real time in order to compromise the customer's account.

Controls

The Agencies are aware of a variety of security techniques which can be used to help detect and prevent the types of attacks described above. Some of these techniques have been in use for some time, while others are relatively new. Financial institutions should investigate which of these controls may be more effective in detecting and preventing attacks as part of the institution's layered security program. However, it is important to note that none of the controls discussed provide absolute assurance in preventing or detecting a successful attack. These controls may include the following:

Anti-malware software may provide a defense against keyloggers and MIM/MIB attacks. Anti-malware is a term that is commonly used to describe various software products that may also be referred to as anti-virus or anti-

spyware. Anti-malware software is used to prevent, detect, block, and remove adware, spyware, and other forms of malware such as keyloggers. It is important to note that anti-malware is generally signature based, and some advanced versions of malware continuously alter their signature.

Transaction monitoring/anomaly detection software has been in use for a number of years. Similar to the manner in which the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped. Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring/anomaly detection could have assisted in preventing many fraudulent money transfers as they were clearly out of the ordinary when compared with the customer's established patterns of behavior. Automated systems may also look at the velocity of a transaction and other similar factors to determine whether it is suspicious.

The Agencies are aware of the fact that a number of institutions are requiring the "out-of-band" authentication or verification of certain high value and/or anomalous transactions. Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised. For business customers, the out-of-band authentication or verification can be provided by someone other than the person who first initiated the transaction and can be combined with other administrative controls. Additionally, the use of out-of-band authentication or verification, for administrative changes to online business accounts, can be an effective control to reduce fraudulent funds transfers.

In response to the rising malware infection rates of customer PCs, a number of vendors have developed USB devices that increase session security when plugged into the customer's PC. These devices can function in several ways, but they generally enable a secure link between the customer's PC and the financial institution independent of the PC's operating system and application software. Typically, the device's firmware is "read only" and cannot be altered by the customer or the malware infecting the PC.

The use of restricted funds transfer recipient lists or other controls over the administration of such lists can reduce funds transfer fraud. Fraudsters must frequently add new funds transfer recipients to an account profile in order to consummate the fraud.

Overall, the Agencies agree with security experts who believe that institutions should no longer rely on one form of customer authentication. A one-dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk. This concept of layered security is consistent with expectations the Agencies have discussed previously. Layered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using restricted funds transfer recipient lists, in addition to robust logon authentication, can help to reduce the possibility of fraud.

The banking, payment, and security industries have continued to innovate in response to the increasing cyber threat environment. In addition to some of the control methods previously discussed, other examples of customer authentication include keystroke dynamics and biometric based responses. Additionally, institutions can look to traditional and innovative business process controls to improve security over customers' online activities. Some examples include:

- ✓ establish, require and periodically review volume and value limitations or parameters for what activities a business customer in the aggregate, and its enrolled users individually, can functionally accomplish while accessing the online system.
- ✓ monitor and alert on exception events.
- ✓ establish individual transactions and aggregate account exposure limits based on expected account activity.
- ✓ require every ACH file originating entity to provide a proactive notice of intent to originate a file prior to its submission; and
- ✓ require business customers to deploy dual control routines over higher risk functions performed online.

ADDITIONAL RESOURCES:

- Better Business Bureau Cybersecurity for Businesses: https://www.bbb.org/all/cybersecurity/cybersecurity-for-businesses
- Department of Homeland Security - Cybersecurity: https://www.dhs.gov/topic/cybersecurity
- Federal Trade Commission – Data Security: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- Fraud Advisory for Businesses –Account Take Over Fraud: https://www.ic3.gov/CrimeInfo/AccountTakeover
- Internet Crime Compliant Center (IC3) : https://www.ic3.gov/default.aspx
- National Cyber Security Alliance Stay Safe Online: https://www.staysafeonline.org/resources/online-safety-and-privacy

REPORT ANY SUSPICIOUS OR FRAUDULENT ACTIVITY TO

First Community Credit Union

FRAUD & RISK MANAGEMENT DEPARTMENT

Risk Department Email: risk.dept@myfccu.com

Chelsey Francis, Risk & Compliance Manager (701) 253-5152

chelsey.francis@myfccu.com