Business Email Compromise Playbook

Prepared by:

Regions Bank

Jeff Taylor
Senior Vice President, CTP

REGIONS

Your Defense Against Business Email Compromise

Business Email Compromise (BEC) fraud is the No. 1 fraud vector impacting businesses today. According to the recent Association for Financial Professionals 2022 Payments Fraud and Controls Report, 68% of businesses surveyed reported being a victim or target of BEC in 2021. While these numbers have shown a decline over the past four years, fraudsters continue to adjust their tactics to successfully perpetrate BEC and inflict significant losses on those who fall victim.

We are here to help our clients combat fraud attempts through our education and awareness campaigns, using analytics to screen for unusual payments, and working with clients and other financial institutions to recover funds after fraud occurs. However, stopping fraud requires the participation of everyone along the fraud journey. Implementing strong controls and security protocols within your organization is the first step toward stopping these types of fraud before the payment is made. Organizations can establish controls such as:

- Regular education about the numerous fraud threats, especially BEC
- Implementing internal payment and technology controls
- Developing a thorough response plan in the event a fraud event occurs

There are no silver bullets or fool-proof processes to prevent payment fraud. The same AFP survey indicated that more than 7 out of 10 companies responding reported being the target of payments fraud. In most cases, the speed at which you notify your financial institution and federal law enforcement will make a huge difference in our ability to help recover funds lost to fraud. While there is no guarantee of recovery once the payments are originated, our teams work diligently on your behalf to help.

It's also extremely important that you take phone calls from us regarding unusual transactions seriously and respond quickly. Many times, these payments look very much like any other payments you originate. Review your processes if you receive a phone call or email from our teams. Make sure to ask yourself if your call back control was followed or if the payment was the result of an email request. Remember, transactions originated under your legitimate credentials are your responsibility, and while we are here to help, fraudsters move the money quickly and we are not always successful in our attempts to recover funds.

Here's How BEC Works

Email accounts are a fertile field for fraudsters. Compromises may occur in a variety of ways. The three most popular compromises involving email are:

- Executive email intrusion: Fraudsters compromise (or impersonate) the email of a company executive or trusted authority figure to request a payment or a change to an existing payment
- Vendor email compromise: Your vendor’s email has been attacked and is used to request a change in the details of an existing payment
- Employee email compromise: An employee of your company experiences a compromise or impersonation of their email account and sends a request to change payroll direct deposit information

Each of these can be carried out by a compromise of the existing email account platform, or by the creation of a look-alike email address using one of the free email services. There have even been instances where the fraudster indicates they are working remotely and using their personal email due to a problem connecting to their work email. This, and other similar techniques, seek to convince the victim to follow the instructions in the fake email without verification.

The following graphic provides a view of the typical process:

1. Fraudster leverages social media and information found online to research their target

2. Fraudster creates a look-alike email domain (LAD) to impersonate the legitimate vendor

3. Fraudster sends phishing email to the target requesting a change in payment terms

4. Victim's legitimate vendor sends an invoice to the victim

5. Victim pays the legitimate vendor's invoice, but to the account provided by the fraudster

The greatest opportunity for penetrating defenses is through phishing, smishing, or vishing. Phishing involves the use of email as the fraud vehicle, Smishing involves mobile phone text messages, and vishing leverages voicemail messages that may appear to come from an authority like the IRS or FBI. In almost all BEC cases, the fraudsters use these means to obtain credentials or information necessary to commit the crime. This further emphasizes the need for effective employee awareness and education programs.

You can see how easy it is for fraudsters to perpetrate this crime and hijack legitimate business payments. Without close scrutiny and awareness, businesses can face significant losses and operational disruption. Due to the typical collection cycle for vendor payments, many of these cases are not discovered for 45-60 days. As a result, the fraudsters have likely moved the funds out of the original beneficiary account and on to another financial institution.

Real Life Examples of BEC

BEC can take many different forms and variations of the three iterations previously mentioned. These are a few real-life examples of client experiences with BEC:

- A company Controller receives an email appearing to be from the CEO while he is traveling overseas. The CEO has discovered a distributor of raw materials used by the company is experiencing a cash flow issue and has declared a deep discount sale on the raw material. The deal calls for secrecy, immediate action and payment via wire transfer to an international beneficiary bank. The CEO instructs the Controller to wire $2.5 million U.S. dollars to a specific routing and account number to complete the purchase. The Controller completes the transaction immediately. Upon the CEO's return the next week, the Controller reports his actions and inquires as to the delivery dates of the raw materials. To his surprise, the CEO is completely unaware of any such deal or email. Upon investigation, it was determined that the CEO's cell phone, containing access to his email accounts, was compromised and resulted in the fraudulent request and subsequent loss.

- An Accounts Payable Associate received an email from an employee requesting a change in direct deposit of payroll information before the upcoming payroll cycle. The cycle ends in two days requiring the Accounts Payable Associate to act quickly to process the request. The employee presses the issue due to a personal problem involving the current account. The request is processed without verification and the next payroll is directed to the new account. After the employee reported being unpaid, the investigation revealed the email address contained one additional letter making it different from the legitimate address.
- A long-time vendor of a company was undergoing a management transition and published the names of the new CEO, COO, and CFO on social media. Customers of the company received email communications announcing the new executives and the new banking relationship for all accounts receivable payments. During the next invoice cycle, customers of the company originated ACH payments to the new routing and account number, as per the instructions. After two payment cycles, the customers were contacted regarding late payments and fees. A thorough forensic investigation revealed that fraudsters had compromised the email account of the vendor, had hidden themselves within the email platform, and generated the fraudulent requests for payment changes.

With the proper controls in place, all three of these very costly situations may have been avoided.

Protection Against BEC

Unfortunately, businesses of all sizes and segments have been victimized by some form of BEC. Executive impersonation and redirected vendor payments typically represent the highest dollar exposure and disruption, but employee impersonation can create a real hassle when payroll is involved. One of the most significant (and easiest) ways to mitigate the risk of BEC is to establish a call back control. We call it STOP-CALL-CONFIRM.

STOP – **DO NOT** process the request received via email

CALL – Call the "sender" using a legitimate phone number known to you. **DO NOT** reply to the email, and **DO NOT** call the number listed in the email

CONFIRM – Verify that the real vendor or employee did, in fact request the change

Implementing this control and ensuring its inclusion on any request for payments or changes to payments received via email will make significant strides toward remediating BEC fraud. It's not perfect, but that five-minute phone call might save you a ton of grief and loss!

Here are a few other steps you can take:

- Establish a training program for employees in payment related functions like Accounts Payable, Vendor Management, and Payroll. Use the materials we provide on www.regions.com/stopfraud to develop your training plan
- Establish an attitude of caution and realize that email alone cannot be trusted
- Be suspicious of vendors who frequently change their payment information
- Use dual control for payment changes – a second set of eyes may help
- If you receive a call or email from us regarding a suspicious payment, take it seriously and respond quickly. It could be your last chance to stop a fraudulent payment, and the faster you let us know the more effective we will be in recovering funds.
    - Double check that your controls were properly executed
    - Keep your contact information up to date
    - Educate your employees to review and respond

Five Industry Suggested Practices

No plan is 100% effective against fraud. But not having a plan or not following these suggested practices will certainly result in increasing your exposure. Here are five industry suggested practices:

1. Guard Your House
    - Develop good Cyber Hygiene habits
    - Conduct a thorough IT vulnerability assessment
    - Work with your IT Department to create efficient and effective firewall protocols that guard and protect your systems, web domain, and confidential information
    - Develop warnings to flag incoming emails from outside sources to warn Associates to be more diligent when opening any attachments
    - Regularly patch and update security systems and back up critical data offline
    - Leverage fraud prevention tools - Positive Pay, ACH Positive Pay & Account Reconcilement

2. When possible, prohibit the use of email for requests to change payment terms, vendor and employee payment information, and system updates
    - If not possible, institute a mandatory call back process (calling a number known to you) or a second approver
    - Thoroughly investigate the email address and the source of the request
    - Implement Multi-Factor Authentication and Dual Control
    - Create a secure employee portal for changes to direct deposit information

3. Create an Associate training program to educate critical payment stream positions
    - Utilize the videos and information on regions.com/stopfraud and regions.com/fraudprevention
    - Perform regular phishing testing on Associates
    - Continually educate Associates
    - Encourage Associates to be aware of potential points of compromise
    - Read and circulate fraud education emails from the bank

4. Perform daily reconcilement of your accounts

- Monitor previous day and current day transaction reports
- Immediately investigate and report suspicious activity
- Leverage the available alert functionality

5. Create a fraud and risk governance plan
   - Identify and document risk tolerance
   - Establish internal controls
   - Create a robust vendor management program
   - Document a detailed fraud response plan
   - Obtain Executive- and Board-level approval

Conclusion

Billions of emails traverse the world every day, and many of these are business communications. While monitoring and processing these important communications presents a risk, the vast majority of these are legitimate requests and conversations. Fraudsters have discovered how to hide behind the anonymity of digital communications and use that to impersonate and deceive. Implementing and performing the proper effective controls, education, and monitoring of potential fraudulent email requests can provide another level of protection for businesses.

Be cautious and Be Fraud Aware to protect your business and assets from fraud. It isn't going away and will likely become even more intrusive as tactics and techniques employed by the fraudsters evolve. For more resources on fraud, visit our websites at regions.com/stopfraud, regions.com/fraudprevention, and doingmoretoday.com/category/fraud-prevention.