ECKERT SEAMANS ATTORNEYS AT LAW

December 20, 2024

Cybersecurity, Data Protection & Privacy Update

Business Email Compromise Fraud – What It Is and What You Can Do

By Matthew H. Meade, Laura A. Decker & Gregory P. Mazmanian

It's a nightmare scenario for all businesses and local governments: you receive an invoice from a vendor that you were expecting and pay it without a second thought. Two weeks later, the vendor calls wondering why the invoice has not been paid. A quick examination of the email reveals that it is suspiciously different than your typical correspondence with the vendor. You realize that you wired the payment to a cybercriminal impersonating the vendor and that your company is now potentially out the total of the misdirected wire payment and is still on the hook for the unpaid invoice. Unfortunately, this is an all-too-common scenario.

Business Email Compromise – What is it, How Does it Occur, and How Can it be Used to Commit Fraud

Business Email Compromise ("BEC") is a cybercrime that the Federal Bureau of Investigation ("FBI") describes as a "sophisticated scam targeting both businesses and individuals performing transfers of funds."[1] BEC scams are executed by fraudsters who gain access to email accounts and/or other forms of communication, through social engineering or computer intrusion techniques, to conduct an unauthorized transfer of funds by redirecting legitimate payments or by creating false pretenses to obtain payment from the victim organization. The FBI reported that it received 21,489 BEC complaints via its Internet Crime Complaint Center in 2023.[2] These incidents resulted in adjusted losses of $2.9 billion dollars to organizations, an increase from the $2.7 billion dollars in losses reported in 2022.

There are two main categories of BEC: unauthorized access to the victim's email account or social engineering; although, most incidents of fraud involve some aspects of both.

A threat actor using unauthorized access to an email account, sometimes called man-in-the middle attacks, can be particularly hard to catch because these events allow a threat actor to hide their fraud within expected and legitimate communication. Threat actors often will gain access to an email account through compromised passwords. Threat actors can obtain compromised credentials through many different means including: (1) phishing the victim's account directly; or (2) purchasing the credentials on the Dark Web. Once inside the victim's account, the threat actor can gather intelligence about vendors, suppliers, clients, invoicing, and payments details. The threat actor can use that intelligence to alter wiring instructions, create a fake invoice, interject themselves into a legitimate email string, and/or use the expected timing of invoices to perpetuate a fraud. Threat actors can also use their access to send fake invoices or altered wiring instructions to business partners, ultimately committing fraud which can cause an organization financial and reputational harm. While in the email account, the threat actor can use different tools, such as inbox rules, to hide their activity, providing additional time and flexibility to commit a fraud before their presence in the account is known to the victim.

[1] Federal Bureau of Investigation, Internet Crime Report 2023, https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.
[2] *Id.*

Social engineering is the manipulation of an email recipient into taking certain actions such as sharing personal information, clicking on a link, or wiring money.[3] Social engineering scams continue to become more sophisticated and complex, making them increasingly difficult to detect. Social engineering emails typically come from outside the victim's internal network. They will often be from a spoofed email with a hard to catch typo to make the email appear legitimate. They may also appear to come from known sources such as Microsoft, Dropbox, or other well-known companies. Additionally, with the proliferation of artificial intelligence, threat actors can create phishing emails without a lot of the telltale grammatical or structural errors that people are used to looking for when evaluating an email. When in combination with unauthorized access, either to the victim's email or a trusted third-party, social engineering can be very difficult to detect. A threat actor can use the intelligence gained from email access to design an email that looks legitimate and is expected by the recipient. Additionally, using unauthorized access, the threat actor can insert the spoofed email into a legitimate email string making it extremely difficult to detect. For example, a victim may be communicating with someone with an @xyzcorporation.com email address until a threat actor introduces an email from @xyzcorportaion.com. This carefully orchestrated change may not be caught until a fraudulent money transfer is discovered.

How To Protect Yourself

The FBI recommends that organizations take measures to protect against BECs, such as adopting two-factor authentication to verify requests for changes in account information, prohibiting automatic forwarding of email to external addresses, training employees to detect suspicious email activities, and verifying that incoming emails match the sender's address.[4]

Additionally, if a vendor or business partner requests a change to its usual method of payment via email, the payor should always call a known contact at the requesting business and confirm the changes verbally. The payor should avoid calling a phone number included in the email with the change of payment instructions. Instead, the payor should opt to call a number of a known contact or obtain a different number such as from the company website.[5]

What to Do if you are the Victim of Wire Fraud

If an organization discovers they are the victim of a wire fraud, every second counts. The primary investigatory bodies for internet financial crime are the FBI and the United States Secret Service ("USSS"), both of which work with the U.S. Treasury Financial Crimes Enforcement Network ("FinCEN"). FinCEN reports "greater success in recovering funds when victims or financial institutions report fraudulently induced wire transfers to law enforcement within 72 hours of the transaction."[6] If a fraudulent wire transfer occurs, an organization should take the following steps immediately:

1. Contact their bank to report the fraud and initiate the wire recall process.
2. File an Internet Crime Compliant Center ("IC3") form which notifies the FBI of the incident.
3. Report the incident to the United States Secret Service ("USSS"). This can be done through calling the local field office and reporting the crime. The USSS will work with the banks to freeze the funds so that the threat actor is unable to withdraw or move the funds so that they can be recovered.

---

[3] IBM, What is Social Engineering, https://www.ibm.com/topics/social-engineering.

[4] Federal Bureau of Investigation, Business Email Compromise, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise.

[5] *Id.*

[6] FinCEN Fact Sheet, Fact Sheet on the Rapid Response Program (RRP), February 11, 2022, https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf

For both the IC3 and reporting to the USSS be prepared to provide the following information:

Transaction Date:
Wire Amount:
Originating Bank:
Originating Bank Account Number:
Beneficiary Bank:
Beneficiary Bank Account Number:
Beneficiary Bank Routing Number:
Beneficiary Name:
SWIFT number (if applicable):

Other Considerations for Victims of a BEC

In addition to fraud, another legal concern stemming from BECs is unauthorized access to protected personal information. All U.S. states and certain federal laws such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Family Educational Rights and Privacy Act of 1974 ("FERPA"), and the Gramm-Leach-Bliley Act ("GLBA") have breach notification laws/provisions that require notification to individuals and sometimes regulators when there is unauthorized access to personally identifiable information ("PII"). How PII is defined varies by statute, but all laws require notification to individuals when an unauthorized actor obtains and/or accesses data containing a person's first and last name, or first initial and last time, in combination with Social Security number, driver's license number, and/or financial account information. Some laws are more expansive in their definition of PII and require notification for additional data elements such as health/medical information, insurance information, passport number, date of birth, etc. In addition to federal laws that apply to certain industries, state law notification requirements are determined by the impacted individual's state of residence.

If an organization is the victim of a BEC, they are required to conduct a reasonable investigation into the incident and notify any individual whose protected information was accessed without authorization.

How We Can Help

If you are the victim of wire fraud, reach out to the Data Privacy and Cyber Security group at Eckert Seamans or your Eckert Seaman's attorney. We can facilitate notifying law enforcement of the incident. Additionally, if you are the victim of a BEC, with or without fraud, we can assist with conducting a forensic investigation to determine what occurred and whether any access to PII occurred. If access to PII did occur, we can provide guidance on applicable laws and facilitate the necessary legal notifications to individuals and regulators.

Additional Resources

- Federal Bureau of Investigation, Internet Crime Report 2023, https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.
- Federal Bureau of Investigation, Business Email Compromise, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise.
- Federal Bureau of Investigation, Public Service Announcement, Business Email Compromise: The $50 Billion Scam, https://www.ic3.gov/PSA/2023/psa230609.
- Microsoft, What is business email compromise (BEC), https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec.
- Proofpoint, Business Email Compromise, https://www.proofpoint.com/us/threat-reference/business-email-compromise

Contact Us

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Laura Decker at 215.851.6623 or ldecker@eckertseamans.com, or Gregory Mazmanian at 215-851-8439 or gmazmanian@eckertseamans.com, a member of our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.