LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

February 20, 2020 | Number 2590

# The Pervasive Threat of Business Email Compromise Fraud — and How to Prevent It

***Eliminating the risk of business email compromise (BEC) attacks requires all parties to a financial transaction to pay close attention to email security, financial controls, and communication protocols.***

**Key Points:**

- The FBI has identified BEC fraud as the **No. 1 financial threat** to businesses in the US.
- The FBI's Internet Crime Complaint Center (IC3) estimates that global "exposed dollar losses" to BEC fraud has exceeded US$26 billion in the past three years.[1] In 2019 alone, the IC3 recorded 23,775 complaints about BEC, which resulted in losses worth some US$1.7 billion.
- All parties to financial transactions must be aware of this fraud risk. Each should put in place not only appropriate security controls for email, but also financial controls for bank account and wiring-instruction verification.

## What Is Business Email Compromise?

Business email compromise is a type of Internet-based fraud that typically targets employees with access to company finances — using methods such as social engineering and computer intrusions. The objective of the fraud is to trick the employee into making a wire transfer to a bank account thought to belong to a trusted partner, but that in fact is actually controlled by the fraudster.

According to the FBI, between May 2018 and July 2019, there was a 100% increase in identified global exposed losses due to BEC.[2]

To illustrate one common form of BEC attack, a fraudster who has gained unauthorized access to a victim's corporate email account (*e.g.*, by stealing the victim's web mail password) can search the email account to learn about an upcoming financial transaction, and then send emails designed to trick unsuspecting colleagues or clients into sending funds to bank accounts under the fraudster's control. These attacks are often "long cons" that involve significant planning and sophistication designed to fool even personnel who would consider themselves well trained on cybersecurity and phishing risks. The fraudster will inject fraudulent communications, dialogue, or instructions at strategic points in a long course of dealing among companies and their advisors, vendors, or other trusted commercial partners,

and monitor email traffic in stealth mode for weeks or months, waiting to spring the con at the perfect moment.[3]

The email with new banking instructions will often appear as a reply to an existing email thread (since the cybercriminal has been spying on legitimate email traffic), and may be sent from the email account of the user who has been hacked. Given this attack vector, BEC fraud can be difficult if not impossible to identify using traditional anti-phishing techniques.

In another example, an attacker might send an email that appears to be from an executive such as the CEO (either "spoofing" the CEO's email account, or using the CEO's actual account if the fraudster has managed to obtain unauthorized access to it) to a senior financial officer, ordering that person to complete an expected wire transfer, but changing the wire instructions at the last moment to an account the attacker has opened for this purpose. Often, by the time the deception is revealed, the funds are long gone. Sophisticated multimillion-dollar attacks typically involve complex money-laundering techniques, where the bank receiving the initial fraudulent wire has also received instructions from the account holder of the fraudster's account to split and wire the stolen funds to multiple other foreign accounts.

These attacks impact all companies, no matter the size, in every industry sector, exploiting vulnerabilities in the technical and human processes that govern how money moves out of corporate financial and even personal or payroll accounts.

## How to Avoid Becoming a Victim of BEC Attacks

A BEC attack can materialize on any email thread involving multiple parties. For each party to be protected, all parties must have appropriate cybersecurity controls on their email systems. It is not enough if only one party has appropriate controls. Therefore, each party must educate the other parties in the transaction and ensure that those other parties have appropriate controls as well.

One critical control is for the payer entity to always **verify any banking instructions** (*e.g.*, wire instructions, SWIFT details, ABA details) **by phone with a known contact at the payee entity**. Again and again, this simple step has prevented the theft of many millions of dollars.

As a best practice, at the beginning of every transaction for which banking information will be shared, the parties should set a **procedure for how that information will be circulated and verified among the parties**. Ensure that voice verification is originated by the payer entity, as only an outbound call to a known phone number can be trusted; caller ID on an inbound call can be spoofed in certain jurisdictions and should not be trusted as a means of caller verification. Implement controls with financial institutions, designating a specific person and requiring phone authorization for certain transactions or transactions over a threshold amount.

Include BEC schemes as part of **cyber-incident response planning and testing**, identifying the financial institution, law enforcement, and other key contacts that are best positioned to stop a fraudulent transfer or attempt a recovery of funds.

Further, all parties involved in a transaction should be suspicious of any banking details that change over the course of the transaction. In particular, a change in payment instructions should be treated with increased suspicion and lead the party receiving the change instruction to follow the voice-verification process.

Finally, all parties should take appropriate measures to secure their email accounts from compromise. Any password selected for an email account should be unique and not be the same as or similar to any password used by the user for any other online account. (Email accounts are often hacked using user credentials stolen from other websites.) Further, companies should implement multi-factor authentication on webmail accounts as an important additional safeguard against the risk of an attacker using a stolen password to gain access to a corporate email account. Companies may also wish to consider blocking auto-forwarding rules from being placed on an account, or setting an alert if such a rule is placed on account, as auto-forwarding rules are often used by an attacker to monitor account traffic after they have gained access to the account.

The FBI makes the following additional recommendations:

- Ensure any email domain or hyperlinks contained in an email is associated with the business it purports to be from. If the email domain or hyperlink is suspicious, forward it to an IT security team for analysis or threat review.
- Be alert to email addresses or hyperlinks that contain misspellings of the sender's name or domain name.
- Do not supply log-in credentials or personal information in response to a text or email.
- For cross-border businesses, be mindful of language differences (*e.g.*, non-native alphabet characters) that may hide a fraudulent email address. Use a secondary channel, or start a new thread with the known correct address when in doubt.
- Refrain from supplying log-in credentials or personal information (such as TaxID, payment card details) in response to any emails.
- Monitor all financial accounts (including personal accounts) on a regular basis for irregularities, such as missing deposits. Many BEC scams target the most highly compensated individuals in the company personally to misdirect outbound wires for large purchases (*e.g.*, real estate, luxury items) or hijack inbound compensation (*e.g.*, annual bonuses, salary).
- Actively supervise and monitor email system security: Is there a documented, adequately resourced program in place to keep all software patches on and all systems updated?
- Verify the sender's email address matches the true email address of the person the email purports to be from, especially when using a mobile or handheld device, which often display only the sender's display name (rather than email address) in the address fields..
- Ensure the settings on company computers are enabled to allow full email extensions to be viewed, so that employees may check to see if a sender or recipient matches known information or what is intended. [4]

## What to Do if You Suspect a BEC Attack Is in Progress

If you discover you are the victim of a fraudulent incident, immediately contact the originating financial institution as soon as the fraud is recognized to request a recall or reversal as well as a Hold Harmless Letter or Letter of Indemnity.

Next, contact law enforcement — the FBI and US Department of Justice have task forces and representatives who are expert in attempting to block or retrieve fraudulent wires. In certain cases, they have had significant success in recovering funds.

## Conclusion

The FBI statistics on BEC attacks are staggering in terms of the number of events, the simplicity of the steps required to avoid the scams, and the total dollars lost. Latham & Watkins has advised clients on many dozens of such events, which morph and evolve over time, and seem only to increase in severity and frequency.

---

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

**Jennifer C. Archie**
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

**Serrin Turner**
serrin.turner@lw.com
+1.212.906.1330
New York

**Tim Wybitul**
tim.wybitul@lw.com
+49.69.6062.6560
Frankfurt

**You Might Also Be Interested In**

Data Privacy & Security Partner Shares Lessons From Data Breach War Stories (Video)

Financial Firms Beware: Dangers Lurk in the Cloud

General Data Protection Regulation Resource Center

Global Privacy & Security Compliance Law Blog

---

**Endnotes**

1 US Federal Bureau of Investigation, 2019 Internet Crime Report, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

2 https://www.ic3.gov/media/2019/190910.aspx.

3 Useful examples of common fraud patterns are available in this FBI summary: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1501791870.pdf. The US Securities and Exchange Commission has expressed serious concern about these types of cyber-threats and losses as well. Release No. 84429 / October 16, 2018 *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements*, available at https://www.sec.gov/litigation/investreport/34-84429.pdf.

4 Additional tips are available on this FBI tear sheet: https://www.fbi.gov/file-repository/email-compromise_508.pdf/view.