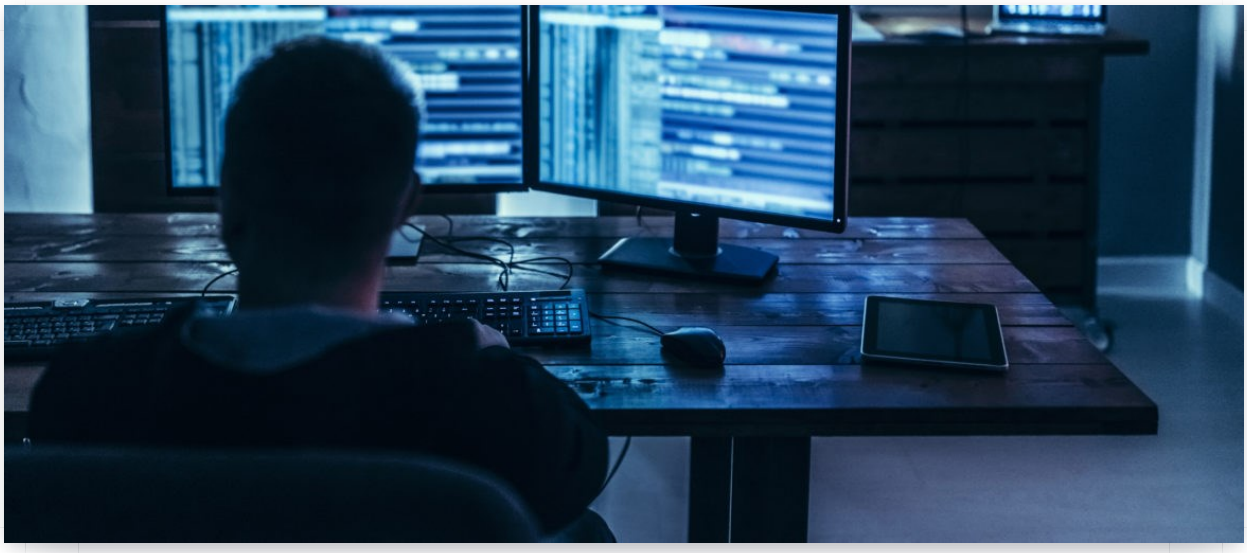
Debevoise & Plimpton | Data Blog

CYBERSECURITY

# FBI Warns of a Rise in Business Email Compromise Scams — Tips for Preventing and Responding to BECs in Remote Work Environments

BY: AVI GESSER, ZILA REYES ACOSTA-GRIMES, CHRISTOPHER S. FORD, ROBERT MADDOX AND BRENNA RAE SOOY - JUNE 11, 2020



On June 9, Calvin A. Shivers, Assistant Director of the Criminal Investigative Division of the FBI, testified before the Senate Judiciary Committee regarding a variety of frauds during COVID-19, including Business Email Compromise ("BEC") frauds and the FBI's response.

BECs are among the most successful and persistent forms of cyber attacks. Indeed, the FBI has seen increases in cyber-enabled financial fraud like BECs every year since 2013. In 2019 alone, the FBI reported 23,775 BECs and email account compromise complaints that led to adjusted losses of over $1.7 billion. For example, on May 13, the Norwegian Investment Fund for developing countries, Norfund, announced it was the victim of a BEC fraud, whereby cyber criminals diverted a $10 million loan intended for a microfinance institution in Cambodia. The fraud took place on March 16, but it was not discovered until April 30 when the hackers attempted a second fraud. Further, on April 6 and April 13, the FBI warned that, due to COVID-19-related disruptions, many businesses have become more vulnerable to BECs.

In this Debevoise Client Update and Data Blog post, we summarize common BEC scams, new COVID-19-related BECs, tips on how to mitigate the risk of a BEC and key considerations for the aftermath of a successful BEC attack. We are also working on an article addressing who bears the loss when a BEC cyberattack succeeds, which we hope to post here in the near future.

**General BECs**. The common BECs that companies face include:

- **Executive Email/Voice Fraud**: An attacker (1) pretends to be a senior company executive, (2) sends instructions to a person at the company who regularly wires money (such as the finance team), and (3) instructs that person to send funds (usually in significant amounts) to the attacker's bank account. The instructions are often sent by email and appear legitimate because the attacker has compromised the executive's email account through phishing.

  In some cases, rather than accessing the actual email account of the executive, the attacker uses a spoofed email account. In this scenario, the message appears as if it is coming from the executive's real email address, but it is actually coming from the attacker using a very similar domain name (e.g., the attacker sends the email from John.Smith@businesss.com instead of the legitimate John.Smith@business.com). Often, the attacker urges that the wire transfer be sent immediately due to an emergency and requests the transfer be kept confidential (*e.g.*, the wire is needed to finalize an important transaction that is only known to a very small group of people).

  In at least one instance, an attacker used AI-based software to imitate the CEO's voice on the phone to convince another executive to send money to the attacker at what was described as the bank account of one of the company's suppliers. Spoofed voices created by AI are also referred to as "deepfake" recordings or audio.

- **Bogus Invoice Scheme**: Another variation involves the attacker compromising or spoofing the email account of a supplier or vendor, and sending the company what appears to be a legitimate payment request with wire instructions for the attacker's account. Attackers will often use copies of actual invoices identified in a compromised employee's mailbox to make the request appear legitimate. We have also seen attackers compromise multiple employees'

email accounts to help ensure payment requests obtain the necessary internal approvals.

- **Gift Cards/Payroll**: In other BECs, the attacker pretends to be an executive and requests that someone purchase and send them gift cards for employees or clients. The attacker may also instruct the payroll department to change direct deposit account information for compensation payments.

**BECs in the Time of COVID-19**. The FBI and the Department of Justice identified several examples of recent COVID-19-related BECs, including:

- An employee of a financial institution received an email that appeared to be from the CEO of a company that had previously scheduled a transfer of $1 million. The email requested that the transfer date be moved up and the recipient account be changed due to COVID-19. The email address used by the attacker was almost identical to the CEO's actual email address, with only one letter changed.
- A bank customer was emailed by an attacker who was posing as one of their customers in China. The attacker requested that all invoice payments be changed to a different bank because the company's regular bank accounts were inaccessible due to "Corona Virus audits." The company then sent several wires to the new bank account, at a significant loss, before discovering the fraud.
- Fraudulent charities sought donations using websites and domain names that look like legitimate organizations (*g*., www.redcross.com instead of the legitimate www.redcross.org).

**Tips for Avoiding BECs**. Companies should consider the following measures to mitigate the risks of BECs:

- **Email Two-Factor Authentication**: Consider implementing multifactor authentication ("MFA") for remote access to corporate email mailboxes. MFA creates a second layer of security other than the username and password (such as a pin number or security question) before an email account can be accessed.
- **Wire Transfer Two-Factor Authentication**: Consider implementing a policy requiring a verifying phone call with the person who is purportedly making a wire transfer request before anyone can execute a financial transaction above a certain threshold, and before any change to existing wire instructions is implemented. Because of the new risk of deepfake audio being used to imitate voices, verification should be done using a previously known phone number, or one that can be independently associated with the person providing the verification, or through videoconference. In addition, because phone numbers can be spoofed, it is more effective if the company initiates (rather than receives) the verification phone call to a recognized number. Some companies are also instituting a verbal keyword that must be provided by the authorized person to confirm their identity. To avoid being compromised, the verbal keyword should not be relayed through email.

- **Training**: Consider having employees who are responsible for wire transfers receive regular phishing training and testing, including during the COVID-19 crisis, when it is perhaps even more important, as we have discussed here. Training should cover means of identifying and avoiding BEC scams in particular, including the possibility of attackers utilizing deepfake audio. Employees should also be advised to pause before wiring large sums of money to new accounts, especially if the directions are coming on an urgent basis by email.
- **Color Coding Emails**: Consider implementing an electronic color coding system, or an email banner message, which allows employees to clearly distinguish between emails coming from within an organization and those coming from outside, to better identify spoofed email addresses. This system can be implemented for email received on desktops, laptops, tablets and phones.
- **Domain Control**: Consider registering and/or blocking email domain names that are similar to the organization's domain name, and updating the block list on a rolling basis.
- **Automatic Forwarding**: Consider prohibiting automatic forwarding of emails to external addresses to prevent cyber criminals from forwarding emails to another account without the user's knowledge, which is often a part of sophisticated BEC scams.
- **Unfamiliar Logins**: Consider enabling alerts or additional access requirements for suspicious activity, such as logins from overseas or at strange hours.
- **Updates**: Consider monitoring ic3.gov for FBI updates (or local equivalents in other jurisdictions such as the NCSC in the United Kingdom) on new variations of BEC scams and other internet crimes, and making sure the appropriate employees are informed promptly of new risks and best practices.
- **Insurance**: Companies should consider reviewing their applicable insurance policy to understand what BEC-related losses are covered. In some jurisdictions, wire diversions may commonly be excluded by cybersecurity specific policies and instead covered by general crime policies, which may have substantially lower coverage limits.

**Responding to a BEC**. Companies that believe they are the victim of a successful BEC-driven wire diversion scam should consider:

- **Immediately Starting the Kill Chain**: Law enforcement can stop wires in progress if they are notified soon enough after the wire is sent. If you determine that a fraudulent wire was sent, immediately contact the bank that received the money and submit the relevant data to https://bec.ic3.gov in the U.S. to trigger FBI efforts to reverse the wire and/or to notify other local authorities as appropriate. Wire transfers are not usually instantaneous, and quick action may allow the bank or law enforcement to cancel the wire. Even if reversing the wire is not possible, it is important to take action quickly to demonstrate reasonable action to mitigate losses to any third parties.

- **Assess the Impact**: Conduct a search for other emails from the attacker, other possible fraudulent transfer requests, and mailbox rules. Once you establish the nature of the BEC, and whether the attacker may have acquired a copy of the compromised mailbox, you can begin assessing what other obligations the company may have under applicable laws (such as the GDPR). It may also be important to look beyond the BEC and determine whether the company's wider computer system has been compromised (and if so, what data, if any, has been accessed or acquired) and whether additional email security measures are needed. This step may prove crucially important if the successful BEC negatively affects third parties. Prompt assessment of any parties that could have been affected and notification to those parties can help the victim company demonstrate that reasonable efforts were taken to mitigate any damage.
- **Notification Determinations**: If data was accessed by the attacker, consider regulatory or contractual notification obligations that may have been triggered. This may sometimes necessitate e-discovery to identify potentially impacted personal information. If the company has relevant insurance coverage, consider whether there is an obligation to notify the insurer promptly to preserve coverage.

For clients facing a breach, the **Debevoise Data Portal** (now in beta testing) will provide a secure online suite of tools that uses a simple, query-based system to help clients assess and respond to their data breach notification obligations across all 50 U.S. states and federal laws, including the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act.

If you are interested in joining the small group of Debevoise clients who are beta testing the **Debevoise Data Portal**, please contact us at dataportal@debevoise.com for more information.

* * *

To subscribe to the Data Blog, please click here.

**Avi Gesser**

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

## Zila Reyes Acosta-Grimes

Zila R. Acosta-Grimes is a member of Debevoise's Financial Institutions Group based in the New York office. Ms. Acosta-Grimes' practice focuses on banking regulatory, transactional and compliance matters. She can be reached at zracosta@debevoise.com.

## Christopher S. Ford

Christopher S. Ford is an associate in Debevoise's Litigation Department who is a member of the firm's Intellectual Property Litigation group and Data Strategy & Security practice. He can be reached at csford@debevoise.com.

## Robert Maddox

Robert Maddox is an associate based in the London office and a member of Debevoise's White Collar & Regulatory Defense and International Dispute Resolution Groups, as well as the firm's Data Strategy & Security practice. His practice focuses on complex multi-jurisdictional investigations, disputes and cybersecurity matters. He can be reached at rmaddox@debevoise.com.

## Brenna Rae Sooy

Brenna Rae Sooy is a corporate associate and a member of Debevoise's Financial Institutions Group. She can be reached at brsooy@debevoise.com.

PREV POST

The Debevoise Data Strategy & Security Practice Announces the Launch of Its Data Blog and Data Portal

NEXT POST

Six Tips for Getting Rid of Old Electronic Files, Which Reduces Cyber and Privacy Risk and Is Now a Legal Requirement for Most Companies

## Related Posts

Four Takeaways from the SEC's Proposed Cybersecurity Rules

FEBRUARY 16, 2022

Webcast – Fireside Chat with NYDFS Cyber Chief Justin Herring

FEBRUARY 5, 2022

Credential Stuffing Continues Practical Guidance to Protect Customer Information

JANUARY 31, 2022