PROGRAM MATERIALS
Program #29206
November 1, 2019

The Rise of Deepfake Audio Means It's Time to Revisit Business Email Compromise Scams and Ways to Reduce Risk

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

The Rise of Deepfake Audio Means It's Time to Revisit Business Email Compromise Scams and Ways to Reduce Risk

Presented by **Avi Gesser** | **Clara Y. Kim**

November 1, 2019

Davis Polk

Agenda

1 What are BEC Scams?

2 How is the Threat Evolving?

3 What are the Regulatory Risks to Consider?

4 Practical Considerations

5 How to Avoid BEC Scams

What Are BEC Scams?

Davis Polk

What Are BEC Scams?

TRADITIONAL BEC SCAMS

The Business Executive Scheme:

- The email account of a CEO or CFO is exploited.
- The fraudster sends an employee a request for a wire transfer, posing as the CEO or CFO.
- The fraudster asks that the request be completed on an urgent basis and to keep the request strictly confidential.

Bogus Invoice Scheme:

- The email account of a supplier with which the company has a long-standing relationship is spoofed or hacked.
- The fraudster uses the compromised email account to make fraudulent payment requests.

What Are BEC Scams?

OTHER BEC SCAMS

- **Executive Compensation:** Fake calls or emails from senior executives changing their bank accounts for the direct deposit of their compensation.
- **Client Gifts:** Fraudsters pretending to be senior executives asking for the purchase of gift cards, usually under the guise of needing them as gifts for clients.
- **Targeting HR Personnel:** Fraudsters asking for personal information of employees, such as tax forms, to use in future attacks.

What Are BEC Scams?

WHY COMPANIES SHOULD PAY ATTENTION

According to the FBI, over the last three years (between June 2016 and July 2019):

- BEC scams have cost businesses over $26 billion.
- There have been 66,349 BEC incidents.

Any company can become the next victim – the FBI warns that cyber criminals target small, medium, and large businesses as well as personal transactions.

How Is the Threat Evolving?

Davis Polk

How Is the Threat Evolving?

Deepfake Audio:

Cybercriminals are using increasingly sophisticated methods to trick companies into wiring money to them, including using AI-based software to mimic the voices of executives.

Case Study:

In a recent case, the AI was sophisticated enough to recreate the slight German accent of a CEO such that the targeted executive thought he recognized his CEO's voice and wired money according to the fraudster's instruction.

What Are the Regulatory Risks to Consider?

3

Davis Polk

What Are the Regulatory Risks to Consider?

OCTOBER 2018 SEC SECTION 21(A) REPORT OF INVESTIGATION

- The SEC examined nine unnamed public companies that had been victims of cyber fraud involving BEC scams or a "phishing" scheme where employees were tricked into wiring money to accounts by bad actors posing as company executives or vendors, resulting in aggregate losses of approximately $100 million.
- The SEC emphasized the importance of assessing the likelihood of cyberattacks when designing internal accounting controls and conducting training for personnel responsible for their implementation.
- The SEC focused on not just public disclosures, but internal operations.

What Are the Regulatory Risks to Consider?

SEC REGULATION S-P (SAFEGUARDS RULE)

- Title V of the Gramm-Leach-Bliley Act (GLBA) governs how financial institutions use nonpublic information of customers.
- SEC has rule-making and regulatory authority over registered investment advisors, broker-dealers, and mutual funds to implement Title V. In 2000, the SEC adopted Regulation S-P (Safeguards Rule).
- The Safeguards Rule requires entities to adopt "written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

What Are the Regulatory Risks to Consider?

FINRA OCTOBER 2019 INFORMATION NOTICE REGARDING CLOUD-BASED EMAIL ACCOUNT TAKEOVERS

- FINRA issued a notice stating that it has been notified that several member firms have experienced email account takeovers while using cloud-based email platforms over the past six months.
- Attackers then used compromised accounts to request fraudulent wire requests (effectively instituting BEC scams) or to steal confidential firm information or nonpublic personally identifiable information.
- FINRA gave recommendations on how companies should respond to account takeovers.

Practical Considerations

4

Davis Polk

Practical Considerations

- Whether employment action is appropriate for any of the employees involved in an incident.
- Conduct regular phishing training and testing, and consider what discipline if any should be given to employees who repeatedly fail phishing tests.
- Whether the company's computer system has been compromised (and if so, what data has been accessed), and whether additional email security features are appropriate.
- Whether to file a complaint with the FBI or notify any other law enforcement agencies.
- Keep any evidence related to the incident.
- Whether the company has any reporting obligations to auditors, regulators, stakeholders or customers.
- Whether notifying the auditors and audit committee of any BEC scams might be appropriate, since internal controls are often implicated.

How to Avoid BEC Scams

Davis Polk

How to Avoid BEC Scams

- Verify Money Transfer Requests
- Train Employees Who Make Wire Transfers
- Block Similar Company Domains
- Two-Factor Authentication
- Email Archiving
- Email Account Access Logs
- Review Insurance Coverage
- Establish a Law Enforcement Contact
- Monitor New Threats

Cyber Blog

Focused commentary on the latest in cybersecurity preparedness, regulatory compliance and incident response

The Rise of Deepfake Audio Means It's Time to Revisit Business Email Compromise Scams and Ways to Reduce Risk

By Avi Gesser, Clara Y. Kim & Thomas Harris-Warrick (The Crypsis Group) on September 16, 2019

We first wrote about Business Email Compromise ("BEC") scams in **2015**. Over the last four years, these attacks have continued unabated. **According to the FBI**, in just the last year alone, there were over 20,000 reported BEC scams, with adjusted losses of over $1.2 billion. One reason this threat persists is that cybercriminals have used increasingly sophisticated methods to trick companies into wiring money to them instead of the legitimate payee.

Indeed, in a twist on traditional BEC scams, **a fraudster recently used an AI-based software to mimic the voice of a CEO on the phone**, successfully tricking another executive into sending money to a supplier. The AI was sophisticated enough that it was able to recreate the slight German accent of the CEO such that the executive thought he recognized his CEO's voice. With the rise of AI and deepfakes, BEC scams may get harder to detect, so it is worth revisiting the measures companies should consider employing to reduce those risks.

Traditional BEC Scams

BEC scams generally refer to email, voicemail, or live phone call scams that are designed to convince company employees who are responsible for executing financial transactions to wire funds to accounts that are controlled by the perpetrators of the scam.

Two common forms of BEC scams are as follows:

- The Business Executive Scheme: The email account of a high-level executive within a company (usually the CEO or CFO) is exploited, either through spoofing or hacking. A fake email is then sent by the perpetrators of the scam to the company's controller (or other employee who normally handles wire transfers for the company). That email, which looks like it is coming from the executive's email account, asks the controller to wire a significant amount of money to a bank account. Usually, the fraudulent email asks that the wire be executed on an urgent basis to facilitate a transaction and to keep the request strictly confidential because the transaction is not yet public.
- Bogus Invoice Scheme: The email account of a supplier with which the company has a long-standing relationship is spoofed or hacked, and is then used to make fraudulent payment requests.

Other BEC scams involve fake calls or emails from senior executives changing their bank accounts for the direct deposit of their compensation. But not all BEC scams involve the wiring of money. Another common BEC scam involves fraudsters pretending to be senior executives asking for the purchase of gift cards, usually under the guise of needing them as gifts for clients. HR personnel at companies may also be targeted, with fraudsters asking for personal information of employees, such as tax forms, to use in future attacks.

Increasingly, successful BEC scams involve the perpetrators doing research on the target business and its personnel, either by hacking the organization's email system or by exploring all available public sources about the business and the employees who are relevant to the intended scam.

How to Avoid BEC Scams

The traditional advice on how to avoid BEC scams involves implementing a policy requiring a verifying phone call or in-person contact with the company officer who is purportedly making the wire transfer request before anyone can execute a significant financial transaction or a change in wiring instructions.

With the rise of deepfakes that can mimic the voice of senior executives, voice verification may not be enough. Policies must also require that the voice verification come from a phone number that can be independently associated with the person providing the verification. Recognizing that phone numbers can also be spoofed, some companies are not relying on an inbound call for verification. Instead, they are requiring the verification process include initiating (rather than receiving) a call to a recognized number, such as a senior executive's desk or known cell phone number. In addition, companies that rely heavily on voice authentication may consider instituting a verbal keyword, never previously relayed through email, that must be provided to validate that the authorizing person is truly who they claim to be.

Training for employees who make wire transfers should cover BEC scams as well as the possibility of deepfake audio. Employees should be trained to pause before wiring large sums of money to new accounts, even if—and perhaps especially if—the directions are coming on an urgent basis from a senior executive.

Having an established law enforcement contact can also help by allowing companies to respond to fraudulent transfers more quickly once they are discovered. Companies should also determine whether insurance would provide coverage for BEC scams, and if not, whether obtaining coverage should be considered.

Finally, companies should monitor **www.ic3.gov** for updates on new variations of the BEC scam and other internet crimes, and educate company leadership and employees on recommended best practices.

Of course, each company must implement cybersecurity measures that are appropriate for its own risks, and what is reasonable will depend on factors like the size of the company, the kind of data it has, and the threats it faces. The **Davis Polk Cyber Portal** is available for clients to meet their evolving cybersecurity and privacy obligations, and we will continue to monitor the evolving threat of BEC scams closely here at the Davis Polk Cyber Blog.

This article has also been posted at the Compliance & Enforcement **blog** sponsored by **NYU Law's Program on Corporate Compliance and Enforcement**.

Business Email Compromise Scams Pose Significant Risk

May 21, 2015

A large number of U.S. businesses have recently been the target of a very sophisticated email scam that is designed to convince company employees who are responsible for executing financial transactions to wire funds to overseas accounts that are controlled by the perpetrators of the scam. The FBI's Internet Crime Complaint Center ("IC3") refers to these kinds of frauds in their various forms as Business Email Compromise ("BEC") scams, which are usually aimed at companies that regularly wire money outside of the United States. In recent months, there have been over 2,000 reported incidents of these scams, resulting in hundreds of millions of dollars in losses. According to the FBI, the two most common forms of BEC scams that may be relevant to your organization are:

- **The Business Executive Scam**: The email account of a high-level executive within a company (usually the CEO or CFO) is exploited, either through spoofing or hacking. A fake email is then sent by the perpetrators of the scam to the company's controller (or other employee who normally handles wire transfers for the company). That email, which looks like it is coming from the executive's email account, asks the controller to wire a significant amount of money to a foreign bank account. Usually, the fraudulent email asks that the wire be executed on an urgent basis to facilitate a foreign transaction and to keep the request strictly confidential because the transaction is not yet public. Sometimes, the fake email from the executive also identifies an outside attorney who is working on the purported transaction, and is followed closely by a call from a person posing as that outside attorney.
- **Bogus Invoice Scheme**: This is similar to the Business Executive Scam, but here, it is the email account of a supplier with which the company has a long standing relationship that is spoofed or hacked, and is then used to make fraudulent payment requests.

Why BEC Scams Are Successful:

The perpetrators of BEC scams extensively research the target business and its personnel, either by hacking the organization's email system or by exploring all available public sources about the business and the employees who are relevant to the intended scam. As a result:

- The fraudulent email requests to initiate a wire transfer are well-worded and tailored to the particular business being victimized.
- The individuals responsible for handling wire transfers within the company are identified and directly targeted.
- The dollar amounts selected for the requested transfers are typical for the particular business.
- Follow-up phone calls from someone posing as the outside lawyer identified in the fake executive email add to the appearance of legitimacy.

How to Avoid BEC Scams:

- Implement a policy requiring a verifying phone call or in-person contact with the company officer who is purportedly making the wire transfer request before anyone can execute a significant financial transaction that was requested by email, text or fax.
- Train employees to recognize red flags, including requests:

  - that the employee act very quickly on a financial transaction,
  - that the employee keep the transaction strictly confidential, and
  - that are made at unusual times and for payments to accounts to which money has not been previously sent.
- Periodically inform employees about recent email scams, what to look out for, and how to avoid them. The IC3 regularly issues press releases with this kind of information (http://www.ic3.gov/media/default.aspx).

Decisions and Considerations:

Companies that fall victim to BEC scams face a number of legal and practical considerations, including:

- How, when, and to which law enforcement agency, to report the incident. The IC3 unit of the FBI is very experienced with these frauds and allows for the reporting of incidents online at http://www.ic3.gov.
- Is the loss covered by insurance, which will depend on the relevant policy exclusions.
- Whether employment action is appropriate for any of the employees involved, which will depend in part on whether any company policies were violated.
- Has the company's computer system been compromised (and if so, what data has been accessed), and whether additional email security features are appropriate.
- Does the company have any reporting obligations to auditors, regulators, stakeholders or customers, which will depend on a variety of factors including: whether the company's computer systems were breached, whether the loss was material to the company, and whether any third parties had an interest in the money that was lost as a result of the fraud.
- Did any company employee disclose confidential business or client information to the persons who were posing as the executive or the outside lawyer, or did the perpetrators of the scam obtain such confidential information by other means, and if so, what steps need to be taken to minimize any associated risks.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Avi Gesser	**212 450 4181**	avi.gesser@dpw.com
Neil MacBride	**202 962 7030**	neil.macbride@davispolk.com

Adding Insult to Injury: SEC Warns That Cyber Incidents May Lead to Enforcement Action

October 18, 2018

On Tuesday the Securities and Exchange Commission issued a **Section 21(a) report of investigation** emphasizing the importance of assessing the likelihood of cyberattacks when designing internal accounting controls and conducting training for personnel responsible for their implementation. The SEC's enforcement division examined incidents at nine unnamed public companies that had been victims of cyber fraud, resulting in aggregate losses of approximately $100 million. Each incident involved a "business email compromise" or "phishing" scheme in which employees were tricked into wiring money to accounts controlled by bad actors posing as company executives or vendors. The SEC investigated the companies' compliance with provisions of the Securities Exchange Act of 1934 requiring maintenance of a system of internal accounting controls that give reasonable assurance that company assets are only accessible in accordance with management's authorization. While the SEC concluded that enforcement action was not warranted against the companies, which spanned industries including financial services, consumer goods and machinery, the regulator warned that internal accounting controls "may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds." The report thus effectively serves as notice that in the future, a company experiencing a cyber event could later find itself in the SEC's crosshairs.

Two types of schemes were investigated:

- **Email from a fake executive**

  In this type of fraud, the perpetrators emailed personnel of a company's finance department using a spoofed email domain purporting to be the address of a company executive, often the CEO. The emails sometimes directed finance department employees to work with outside attorneys and send wire transfers to foreign bank accounts controlled by the perpetrators. The outside attorneys appeared to work for real law firms, but telephone calls to them were answered by skilled impersonators. The communications were usually urgent in nature and concerned time-sensitive "deals," some of which even purported to be under SEC oversight. Most transfers were made to foreign banks, and while the companies did have foreign operations, the transactions were nevertheless out of the ordinary and thus might have raised red flags. Additional warning signs included the fact that the emails were sent to mid-level employees who rarely interacted with the purported senior-level senders, and featured numerous grammatical and spelling errors. The SEC noted that these spoof emails were not sophisticated from a technological point of view.

- **Email from a third-party vendor**

  In the second type of fraud, emails purporting to originate from a company's vendor instead were the product of hacking into the vendor's email account and falsifying payment details in what otherwise appeared to be legitimate payment requests. These emails were more technologically sophisticated and had fewer warning signs than the fake executive emails, and were revealed to have been fraudulent when the actual vendors sought payment.

The SEC has previously counseled public companies on their disclosure obligations relating to cybersecurity risks, as we discussed in our February 2018 **memo**. Yesterday's report focuses not on a company's public disclosures, but on its internal operations – its books and records. The regulator cautioned that public companies should pay close attention to their obligation to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . transactions

are executed in accordance with management's general or specific authorization" and that "access to assets is permitted only in accordance with management's general or specific authorization." The SEC emphasized the importance of taking into account both cybersecurity threats and "related human vulnerabilities" when designing these controls, since cyberattacks need not be particularly sophisticated to cause significant harm through clever exploitation of human weaknesses. In a recent SEC settlement order, the SEC found that Voya Financial Advisors Inc. did not have reasonable cybersecurity policies and procedures in place to detect identity theft risks or respond to cybersecurity attacks, resulting in a $1 million penalty and an agreement to retain an independent consultant to review its policies and procedures for compliance with the Safeguards Rule and the Identity Theft Red Flags Rule, even though there was no finding of harm to any customers. The SEC likely expects companies to review their controls and procedures, including employee training, to see what may need to be strengthened in order to defend against the ever-evolving cyber threat matrix.

* * *

Some measures that companies can consider implementing to reduce the risk of falling victim to a business email compromise scheme include:

- **Two-factor authentication for certain wire instructions**

  Consider establishing an alternate communication channel, other than email (such as telephone calls or in-person communications), to verify significant wire transactions, as well as any changes to wire account instructions, including changes to direct deposit instructions for employees. When using phone verification as part of the authentication procedure, consider only using previously known phone numbers, not numbers provided in an e-mail request.

- **Phishing training and testing**

  Consider training and testing for employees involved in payments to raise awareness about common phishing schemes and educate them on cybercrime prevention.

- **Look-alike company domains**

  Consider registering and blocking Internet domains that are similar to the company's actual domain name (e.g., davisp0lk.com, davispo1k.com, davispollk.com).

- **Establish law enforcement contacts**

  Consider establishing a law enforcement cyber contact, which can help companies effectively respond to fraudulent transfers more quickly once they are discovered.

- **Insurance coverage**

  Determine whether your insurance would provide coverage for a business email compromise, and if not, whether to obtain coverage.

- **Check for updates on the latest business email compromise scams**

  Consider having someone at the company monitor www.ic3.gov for updates on new variations of these scams and other internet crimes, and educate company leaders and employees on the latest recommended best practices.

- **Notification of auditors and audit committee**

  Consider notifying the auditors and audit committee of any such cyber events since internal controls are often implicated.

Similar tips and resources to assist our clients in their efforts to maintain compliance with their cybersecurity regulatory obligations are now available through the Davis Polk Cyber Portal.

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Richard D. Truesdell, Jr.	**212-450-4674**	**richard.truesdell@davispolk.com**
Michael Kaplan	**212-450-4111**	**michael.kaplan@davispolk.com**
Joseph A. Hall	**212-450-4565**	**joseph.hall@davispolk.com**
Bruce K. Dallas	**650-752-2022**	**bruce.dallas@davispolk.com**
Sarah K. Solum	**650-752-2011**	**sarah.solum@davispolk.com**
Avi Gesser	**212-450-4181**	**avi.gesser@davispolk.com**
Li He	**011-852-2533-3306**	**li.he@davispolk.com**

Information Notice – 10/2/19

Cybersecurity Alert: Cloud-Based Email Account Takeovers

Summary

Several member firms recently notified FINRA that they have experienced email account takeovers (ATOs) while using cloud-based email platforms, including Microsoft Office 365 (O365). Attackers used compromised email accounts to defraud member firms by requesting fraudulent wire requests or stealing confidential firm information or non-public personally identifiable information (PII).

This Notice outlines the attackers' tactics in executing ATOs, as well as steps taken by member firms to address ATO risks when using cloud-based email systems.

Questions concerning this Notice should be directed to:

- David Kelley, Surveillance Director, at (816) 802-4729.

Background and Discussion

During the past six months, several member firms have notified FINRA staff that they have experienced ATOs, primarily on the O365 email platform. A large number of firms have migrated to cloud-based email platforms in the past 12 to 18 months, or plan to do so in the near future, so attackers may be intentionally targeting these firms to take advantage of weaknesses in their access and other controls.

FINRA reminds member firms that, under the U.S. Securities and Exchange Commission's Regulation S-P, they are required to have policies and procedures that address the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.

Attackers have executed email ATOs at member firms using techniques such as:

- phishing emails that impersonated support personnel requesting log-in credentials;
- credential stuffing, where the attackers automatically enter previously breached credentials into various websites and applications until they successfully match to an existing account;
- stolen passwords from a user's personal email account; and
- "brute-force attacks," where the attackers submit a large number of potential passwords until one of them works.

After gaining access to an email account, attackers typically monitor the account over several weeks or months to:

- observe email traffic;
- develop an understanding of the firm's processes for submitting financial transaction and wire requests to the back office;
- monitor communications with clients or other external parties; and
- identify possible opportune moments (e.g., days when the email account owner will not be monitoring their email) to carry out the next step of their attack.

Following execution of the email ATO, the attacker may:

- email back-office personnel asking about wire transfers and other money movement procedures, or instructing them to transfer funds to a fraudulent external bank account;
- email firm clients instructing them to transfer funds to a fraudulent external bank account;
- install malware that creates a new avenue for attackers to access the users' accounts; or
- forward client information to another email account.

Whatever form the attack may take, the fraudsters typically hide their tracks by changing the compromised account's mailbox rules to hide or delete the emails they send from the account. As a result, the account owner may remain unaware of the sent emails until well after the fraudsters have achieved their intended effects, such as transmitting confidential information or causing a fraudulent money transfer.

Attackers have also successfully taken over accounts of firm staff with administrative privileges. This type of ATO creates heightened risks for firms and clients because accounts with administrative privileges may provide the attacker with a powerful platform to launch a larger-scale attack.

FINRA has observed that recovering from an ATO attack was particularly challenging for firms that had not configured their email systems to retain key data logs because they did not have sufficient information to analyze the full scope of the attackers' activities and determine the extent of the fraud. Notably, many firms could have prevented an ATO attack if they had implemented two-factor authentication (2FA).

Preventing ATOs

FINRA has observed that some firms have taken the following steps to configure their cloud-based email environments to help address possible ATO attacks:

- **2FA** – Implemented 2FA for all email account log-in activity outside of the firm's network for general users (e.g., for registered representatives and, internal administrators). On the O365 platform, some firms also implemented 2FA for Microsoft Partners and used the Microsoft Authenticator application on users' mobile devices or a dynamically generated personal identification number (PIN) sent via SMS text to provide the second factor.
- **Email Archiving** – Retained and archived all emails in a separate location from the email server to provide the firm with an additional copy of all inbound and outbound emails. In addition, some firms implemented alerts to appropriate firm personnel if there were interruptions in email archiving services.
- **Logs** – Maintained and retained logs of all email account access for an adequate period of time.
- **Administrator Accounts** – Carefully managed all firm administrator accounts by:
  - closely supervising which individuals received administrator accounts to limit access to specifically authorized individuals and minimize the number of individuals with such accounts;
  - reviewing the level of access granted to administrator accounts;
  - monitoring administrator accounts' activities, especially those of "global admin" accounts; and
  - on the O365 platform, confirming administrative privileges delegated to Microsoft Partners and evaluating whether Microsoft Partners should receive "full admin" rights or if "limited admin" privileges are sufficient.[1]

Firms also provided training on the appropriate configuration of cloud-based email services, as well as on phishing emails that could compromise email account security.

Responding to an Attack

FINRA has observed firms respond to ATOs by:

- immediately shutting down the email account by disabling access or resetting the compromised email account with a sufficiently complex password prior to reinstating the account;
- evaluating whether appropriate forensic expertise was available within the firm or whether a third-party service provider should be hired;
- making a copy of any affected email account, including all emails across all folders (such as those hosted by the record retention provider) to capture all information potentially accessed by the attacker at the time of the compromise;
- reviewing all of the email content in the compromised account, including attachments, to determine whether the attacker had access to sensitive or confidential information, such as PII;
- determining whether any client information was breached and notification required under federal or state law;
- confirming that any malware or viruses were deleted and unnecessary user accounts were closed;
- reviewing the overall cybersecurity environment to address any other potential impacts of the attack;
- implementing 2FA controls, if not already in use; and
- notifying appropriate law enforcement agencies (e.g., the local Federal Bureau of Investigation field office) and their FINRA Regulatory Coordinator of the attack.

Endnotes

1. See, e.g. Microsoft Azure, About Admin Roles (providing additional information about access privileges for roles in O365).