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