CONSTRUCTION
ALERT
June 2021

A. Robert Rosin · Michael M. Lum · Roger F. Liu
Gregory S. Gerson · Timur Bilir · Tony J. Stavjanik
Janette G. Leonidou (Of Counsel)

777 Cuesta Drive, Suite 200
Mountain View, California 94040
(650) 691-2888
(650) 691-2889 (fax)

DEFEND YOUR COMPANY AGAINST EMAIL FRAUD SCHEMES

Business email compromise ("BEC") schemes are on the rise. Sophisticated, email-based attacks are increasingly common. Two of our clients in the past year have had significant payments diverted through BEC schemes.

Analysis by the U.S. Treasury Financial Crimes Enforcement Network reveals that manufacturing and construction companies are the most common targets in BEC schemes, comprising 25% of reported BEC cases. In a common scenario, a BEC hacker will send an email from a compromised account. The BEC email will provide new wire instructions and request expedited action (possibly referencing a known and/or regularly scheduled payment or transfer of funds). A recipient may not realize that the email is fraudulent and wire the money without further verification. The fraud is only discovered when the original recipient never receives an expected payment.

Who is responsible for losses from a BEC scheme – the company whose email was hacked or the company that pays the funds?

Current caselaw is unsettled, but courts that have looked at this issue generally undertake a detailed analysis of who was in the best position to identify the fraud and prevent it. In one case, *Bile v. RREMC, LLC*, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. Aug. 24, 2016), the district court ruled that the party who failed to exercise "reasonable care" should bear the loss from the fraud. If the owner of the hacked email account failed to take reasonable precautions to prevent the compromise of its account and/or was aware of the hack, a court could find that party primarily at fault. On the other hand, if the employee that sent the wire to a new account knew or should have known that such a request was suspicious, e.g., this wire was for a recurring payment from a general contractor to a subcontractor and a similar payment had been made successfully multiple times on a monthly basis using different payment arrangements, a court could find that the wiring employee's

employer would be responsible, because the company should have taken further steps to verify the changed wiring instructions, such as a telephone call to a known individual at the payee company.

What you can do to minimize risks of BEC schemes:

- Provide computer/email security awareness training to all your employees.
- Consider purchasing comprehensive cyber insurance (not just coverage to replace computers).
- Always use strong passwords and consider password management software. Some web browsers can also create and save strong passwords.
- Never use the same password for more than one website or e-mail account.
- Change your passwords regularly.
- Be on the lookout for suspicious e-mails, and always call to verify changed payment instructions. Remember to call a phone number saved to your phone or from the signature block of an old e-mail that you know was legitimate.
- Always call to verify wire instructions and verify using an out-of-band method (don't rely on email alone and don't use telephone numbers or website addresses in emails, which themselves can be fraudulent).
- Another good idea is to establish a rule that any changes in vendor payment must be approved with two different employee sign-offs. This further increases the likelihood of any fraud being detected.

Additionally, the FBI suggests that you take the following steps:

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing!) and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust. BEC attackers frequently send emails from a compromised business email account or will send emails from a domain very similar to a known domain, e.g., joe@attt.com (with 3 t's).
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.