GOLENBOCK EISEMAN
ASSOR BELL & PESKOE LLP

CLIENT ALERT

ATTORNEYS AT LAW | 711 THIRD AVENUE | NEW YORK, NY 10017 | 212 907 7300 | WWW.GOLENBOCK.COM

BEWARE OF PAYMENT INSTRUCTIONS OVER EMAIL

January 11, 2021

We have been seeing a growing trend of a criminal cyber-fraud scheme affecting large and small businesses, individuals and banks: A payor that owes money to a payee receives an email appearing to come from the payee with new or revised payment instructions. The payor executes a wire transfer in accordance with the payment instructions. Unbeknownst to the payor and payee, the email in fact was sent by a criminal posing as the payee, and the account referenced in the payment instructions belongs to the criminal. Upon receiving the funds, the criminal immediately drains its account, never to be found, leaving a dispute between the payor and the payee over who bears responsibility for the loss.

This scheme is not entirely new, with a handful of cases working their way through the courts starting a few years ago. However, given the widespread reliance on email for conducting business, criminals still appear to be finding a growing number of targets. We are helping clients resolve these disputes after the fraud is discovered, including in litigation, but the law is still developing in this area, and thus the best practice is to be proactive and avoid becoming a victim.

This Alert provides an overview of how criminals commonly carry out this scheme to help you be aware of what to watch out for, discusses the difficulty under the law in determining responsibility when this fraud occurs, and provides some preliminary methods to mitigate the risk.

The Scheme

This email fraud scheme has arisen in an array of contexts, from payments for the sale of goods, to down-payments or rental payments for real estate, to settlement payments. Criminals have carried out this scheme in at least two ways. One method is to hack the payee's email account, so that the criminal is able to send and receive emails directly from that account. To avoid detection by the account owner, the criminal may clandestinely change the settings in the email account so that certain conversations will automatically go to the deleted items folder, and thereby the account owner is less likely to see them. Another method is for the criminal to create a "shadow" email account that appears like the payee's email account but may be off by one character, such that the emails will still appear in the recipient's inbox as if they were sent by the payee. In either case, the criminal will typically have conducted reconnaissance prior to executing the scheme so

that the criminal knows when a payment is due to be made and can then intervene with the fraudulent email, and so that the criminal also has knowledge of the transaction and can mimic the writing style of the payee and thereby avoid detection.

Determining Responsibility For The Loss Is Not Clear-Cut

When the criminal successfully executes this scheme, the question arises as to who bears the loss. Oftentimes by the time the fraud is discovered, the criminal has already received and withdrawn the funds, and thus the parties should not expect that the bank will be able to reverse the payment. These cases typically result in the payor and payee pointing fingers at each other. From the payor's perspective, it paid the funds in good faith and therefore believes it is entitled to the goods or services it paid for, arguing that the payee is at fault for failing to properly protect its system from the hack. From the payee's perspective, it never received payment and therefore will demand payment from the payor, which would effectively require the payor to pay twice. The payee may argue that the payor failed to properly confirm the payment instructions or failed to notice anomalies in the emails. There is no bright-line rule under the law to determine liability in these circumstances. Rather, the case law shows that determining liability is a highly fact-specific inquiry, which has resulted in drawn-out litigation.

A leading case that reached the United States Court of Appeals for the Sixth Circuit provides a good example of how this scheme may play out, and the complexity of litigating responsibility for the loss. A car dealer, Beau Townsend Ford, agreed to sell 20 Ford Explorers to another dealer, Don Hinds Ford, for $736,225.[1] Don Hinds stated over email that it intended to pay by check. But it received an email in reply, purportedly from Beau Townsend, stating, "Due to some tax related procedures we will prefer a wire transfer, let me know when you need wiring instructions," and this was followed by an email with wire instructions to an account at Bank of America. Over the next several days, Don Hinds picked up the vehicles from Beau Townsend and wired the money in three installments. Each time Don Hinds wired the money, it received confirmation emails from Beau Townsend.

Several days later, Beau Townsend called Don Hinds to ask when payment would be made by check. It turned out that the emails Don Hinds received relating to wire payment were sent by a criminal who had hacked the email account of a Beau Townsend manager. As a result, Beau Townsend was out the 20 vehicles and never received any payment, and it sued Don Hinds. The district court ruled in favor of Beau Townsend on a pre-trial motion for summary judgment, holding that Don Hinds breached the parties' agreement by failing to pay Beau Townsend, and ordered Don Hinds to pay the entire $736,225 again. On appeal, the Sixth Circuit held that "the district court failed to adequately analyze this complex issue," and held that a trial was required to decide whether and to what degree each party was responsible for the loss.[2] The Court indicated that a jury could find that both parties shared responsibility, in which case the jury would need to apportion the loss between them: "[I]f Beau Townsend had failed to exercise ordinary care in maintaining its email server, thus allowing the hacker to pose as [a manager], then Beau Townsend could be liable for Don Hind's reasonable reliance on the hacker's emails. In addition, any potential liability would be reduced if Don Hinds also failed to exercise reasonable care."[3]

[1] *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 F. App'x 348 (6th Cir. 2018).

[2] *Id.* at 349.

[3] *Id.* at 358.

That case involved a substantial sum that made litigation economically practical – and even then the parties were relegated to an expensive jury trial with an uncertain outcome. However, these schemes often target much smaller payments under $100,000, where the cost of litigation may exceed the amount at issue. This leaves the parties in a very difficult position with no clear resolution, further underscoring why it is important to be aware of, and take precautions to avoid, these fraudulent email schemes.

Ways To Mitigate The Risk

Given the sophistication of cyber-criminals and their ever-changing methods, it is difficult to eliminate the risk of cyber-fraud entirely. But there are preliminary ways to mitigate the risk of this email fraud scheme:

- Awareness is the first step in prevention, and thus employees with responsibility for sending or receiving payments should be educated about this type of email fraud.
- Procedures should be implemented prohibiting the use of, and reliance on, emails alone for payment instructions.
- If you do receive payment instructions by email, even if the email appears in all respects to be legitimate, call the sender to verify the payment instructions. Do not rely on confirming the instructions by email, because you may be unknowingly communicating with the criminal.
- The parties can anticipate this issue, and address responsibility for any loss, in their written agreement. For example, the parties can specify the payment instructions in the written contract or invoice and/or specify a procedure that must be followed for payment instructions to be updated (which should not include email alone), and provide in the written agreement that any loss resulting from a party's failure to adhere to these procedures will be borne by that party.
- Nobody wants a criminal lurking in their email account in the first place. Ways to mitigate the risk of an email hack are to change passwords on a routine basis, and to not click on untrusted links. Consult with a cyber-security professional about two-factor authentication, anti-virus software and other prevention and monitoring techniques that may be appropriate for your system.
- Even with precautions in place, cyber-fraud may nevertheless occur. Check your insurance policy to determine whether it may cover this type of loss, and speak with your insurance broker about coverage options.

If you feel we might be of assistance to you in this area, please reach out to your primary contact at GEABP or to the attorneys listed below.

David Eiseman (212) 907-7330
Email: deiseman@golenbock.com
Matthew Daly (212) 907-7329
Email: mdaly@golenbock.com
Michael Devorkin (212) 907-7348
Email: mdevorkin@golenbock.com
Martin Hyman (212) 907-7360
Email: mhyman@golenbock.com
Michael Munoz (212) 907-7345
Email: mmunoz@golenbock.com
Preston Ricardo (212) 907-7341
Email: pricardo@golenbock.com
Jacqueline Veit (212) 907-7391
Email: jveit@golenbock.com

# # #

GOLENBOCK EISEMAN
ASSOR BELL & PESKOE LLP