Meltzer Lippe

SOCIAL MEDIA, SOFTWARE & PRIVACY CLIENT ALERT

October 15, 2019

SOCIAL MEDIA, SOFTWARE & PRIVACY PRACTICE GROUP

Our Social Media, Software & Privacy practice is one of the fastest growing practice areas within the firm. Clients turn to our social media, software & privacy attorneys to devise website terms and conditions for the online aspects of their business; to seek advice on digital best practices related to corporate disclosure; to pursue non-compete enforcement resulting from online activity of a former employee or competitor; and, in general, for their thoughtful application of long established law to new technology.

ATTORNEYS

Pedram A. Tabibi
Loretta M. Gastwirth
Christopher P. Hampton
Michael H. Masri
Joshua D. Sussman

Meltzer, Lippe, Goldstein & Breitstone, LLP
190 Willis Avenue
Mineola, NY 11501

P:516.747.0300
www.meltzerlippe.com

Businesses Beware: How Scammers May Target Your Wire Transfers

Before parting with company funds, make sure you are sending them to the right place.

Typically, a business wire transfer is straightforward. For example, your company owes $100,000 to a supplier for goods purchased. The time comes for you to pay the funds to the supplier, and as in past instances, you have the supplier's bank information – routing and account numbers – in hand. Then, just before the wire transfer is to proceed, you get an email from someone supposedly in the supplier's accounts receivable department stating that the wire transfer instructions have changed and requesting, for some bogus but credible reason, that you send the funds to a different bank account. The fraudster has spoken!

Based on your history with the supplier, you comply and initiate the wire transfer. Days or weeks later, you get a request from the actual supplier as to when the $100,000 payment will be sent. Confused, you reply that the wire transfer was sent some time ago. A subsequent investigation will discover that both parties have fallen victim to an all too prevalent scam nowadays, a business email compromise or "BEC" scam. By then, the $100,000 is gone from your account and the bank may be unable to reverse the wire transfer.

BEC scams can severely damage your company and are occurring at an alarming rate. In 2018, the FBI's Internet Crime Complaint Center received over 20,000 complaints of BEC scams and other email account compromise scams, with adjusted losses of more than $1.2 billion, according to the FBI's 2018 Internet Crime Report (source: https://pdf.ic3.gov/2018_IC3Report.pdf).

While there is minimal case law to date addressing BEC scams, at least one federal court, in Bile v. RREMC, LLC, 2016 WL 4487864 (E.D. Va., Aug. 24, 2016), held that **the party who failed to exercise ordinary care and could have prevented the loss during the transaction should bear the losses from the scam.** The facts of each situation differ, of course, and require careful evaluation but sellers want to be paid and buyers don't want to pay twice for the same goods or services, because the first payment went to a smart, polished fraudster's bank account.

Thankfully, there are ways to help prevent your company from falling victim to BEC scams. A comprehensive company plan to protect against BEC scams may include, among other things:

- Having appropriate technology and security practices in place to avoid email accounts from being compromised and used as a vehicle to conduct a BEC scam.
- Having a written company policy – both internally and in business agreements – that require any change in payment instructions, including wire transfer instructions, be confirmed both in an email and also a second way, such as verbally on the phone.
- Having a company cyber insurance policy to cover the losses from a BEC scam.

Please contact the author Pedram A. Tabibi at ptabibi@meltzerlippe.com or any of our other Meltzer Lippe Social Media, Software and Privacy attorneys to see what steps you can take to reduce the risk of your company having to pay the price – possibly twice – for a BEC scam.