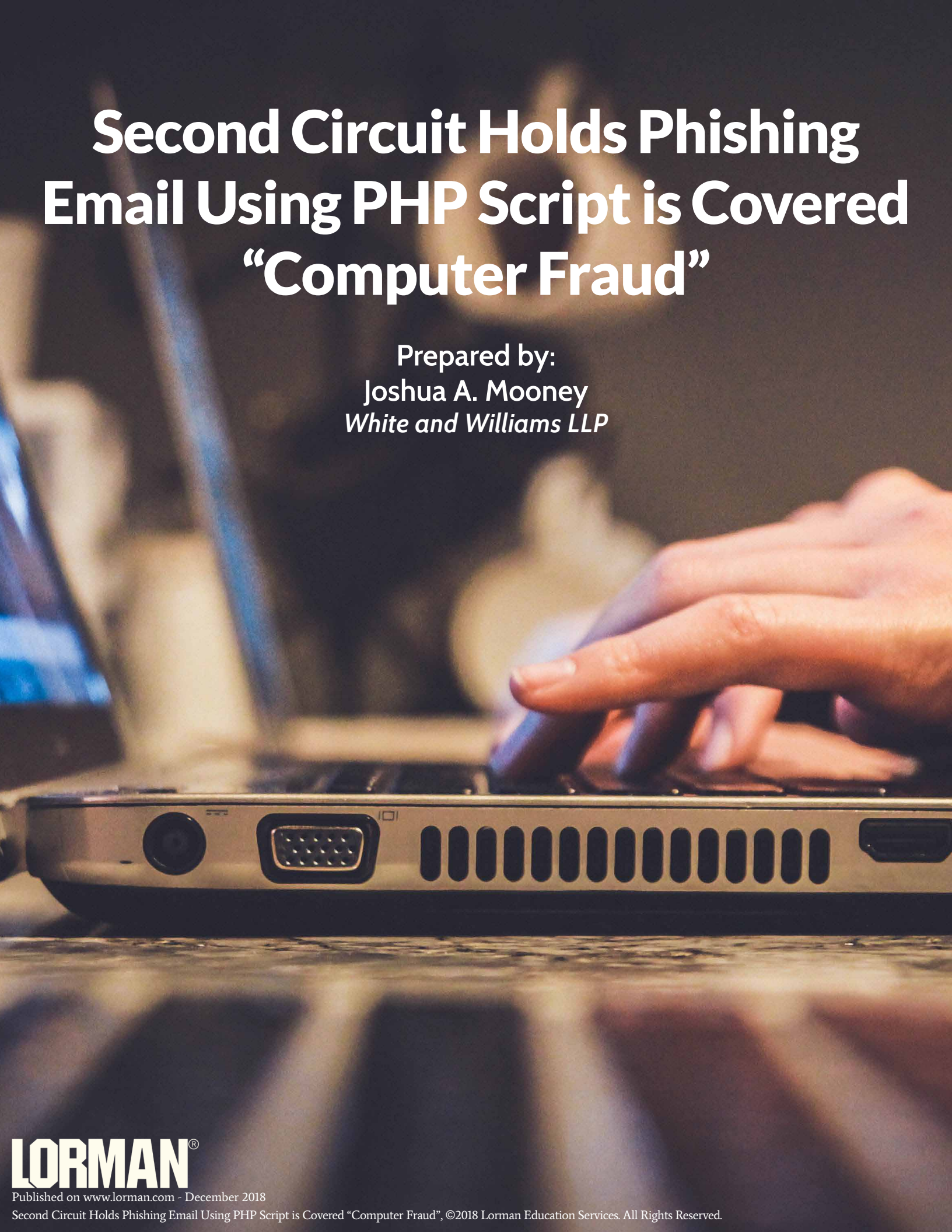

Second Circuit Holds Phishing Email Using PHP Script is Covered "Computer Fraud"

Prepared by:
Joshua A. Mooney
White and Williams LLP

LORMAN®

Published on www.lorman.com - December 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Second Circuit Holds Phishing Email Using PHP Script is Covered "Computer Fraud"

Written by Joshua A. Mooney – 7/6/18

Scams from business compromise emails (BECs) have been labeled by the FBI as a "$5 billion" problem. Sometimes known as "CEO Fraud," BECs are where an email, purportedly coming from a high-ranking company official or vendor, instructs an employee to wire a sum of money to a bank account, or instructs the employee to wire money owed to a new bank account. The company thereafter authorizes and wires the money to the new account, which is controlled by fraudsters. The fraudsters then withdraw the money before the fraud is discovered.

On July 6, 2018, the United States Court of Appeals for the Second Circuit, in *Medidata Solutions, Inc. v. Federal Ins. Co.*, 17-2492 (July 6, 2018), became the first U.S. Court of Appeals to determine that a BEC perpetrated using a PHP script as a spoofing tool implicates "computer fraud" coverage under a crime policy.

In *Medidata*, a phishing email purportedly coming from Medidata's president, instructed a lower-level employee to wire roughly $4.7 million to a bank account as part of a secret corporate transaction. The email used a PHP script which made the address of the sender in the text of the email appear as if it had come from the company president's company email, when in fact the real sender (and recipient of any replies) was a third-party fraudster. PHP scripts are a common tool used to spoof emails; the tool may be employed through third-

party websites. The money was transferred pursuant to the fraudulent instructions and was withdrawn.

Medidata sought coverage for its loss under a crime policy for "computer fraud," which covered "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." *Medidata,* 268 F. Supp. 3d 471, 474 (S.D.N.Y. 2017). The policy defined "Computer Fraud" as "[T]he unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." *Id.* The Policy defined "Computer Violation" as "the fraudulent: (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against an Organization." *Id.*

The Second Circuit held that the policy covered the loss. The parties agreed that use of email satisfied the definition for "computer system" within the meaning of the policy. Equating the PHP script as malicious code, the Second Circuit concluded that spoofed email, which the court labeled as an "attack," was both a fraudulent entry of data into a computer system as well as a fraudulent change to Data elements. The court explained:

> While Medidata concedes that no hacking occurred, the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system, which the parties do not dispute constitutes a "computer system" within the meaning of the policy. The spoofing code enabled the fraudsters to send messages that inaccurately appeared, in all respects, to come from a high-ranking member of Medidata's organization. Thus, the attack represented a fraudulent entry of data into the

> computer system, as the spoofing code was introduced into the email system. The attack also made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender. Accordingly, Medidata's losses were covered by the terms of the computer fraud provision.

According to the court, the fraudulent email involved a compromise of the insured's computer system. The court stated that the "spoofing attack quite clearly amounted to a 'violation of the integrity of the computer system through deceitful and dishonest access,' since the fraudsters were able to alter the appearance of their emails so as to falsely indicate that the emails were sent by a high-ranking member of the company."

The Second Circuit also held that because the spoofed email had set off a chain of events resulting in the mis-wiring of funds, the loss at issue constituted a "direct loss of Money … resulting from Computer Fraud[.]" The court explained:

It is clear to us that the spoofing attack was the proximate cause of Medidata's losses. The chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred. The employees were acting, they believed, at the behest of a high-ranking member of Medidata.

Critically, this decision contradicts decisions rendered by other U.S. Courts of Appeals in the context of BEC claims. Most courts, including

the Fifth, Ninth, and Eleventh Circuits, have held that intervening events, such as the insured's failure to verify properly the legitimacy of the instructions or its own subsequent instruction to its bank to transfer the funds, constitute intervening acts that break the "direct" casual requirement. In *Medidata*, the Second Circuit rejected such reasoning – although, it did not cite or distinguish the other appellate court decisions – stating that New York does not require "so strict" a rule about intervening acts.

Other courts have yet to address coverage for BEC claims. This decision may have a dramatic impact on coverage analysis for a significant fraud perpetrated every day in the U.S. economy.

If you have questions or would like additional information, contact Josh Mooney (mooneyj@whiteandwilliams.com; 215.864.6345) or another member of the Cyber Law and Data Protection Group.