SULLIVAN & CROMWELL LLP

April 16, 2015

Cybersecurity: Sophisticated Scams Target Corporate Transactions and Confidential Information

Cyber Criminals Are Reportedly Pairing Falsified Wire Instructions with Seemingly Credible Justifications in Attempts to Misdirect Funds to Third-Party Accounts and Tricking Executives and Advisers into Compromising Sensitive Non-Public Information

SUMMARY

Recent reports indicate that sophisticated cyber criminals are increasingly targeting company executives and their outside counsel, advisers, and consultants in connection with corporate transactions in fraudulent efforts to obtain funds or inside information. These schemes involve hacked systems or forged emails that appear legitimate to redirect funds transfers or obtain confidential information. To avoid loss of funds or confidential information, companies should consider implementing heightened verification procedures with respect to significant financial transactions or sensitive information requests.

DISCUSSION

With cyber intrusions and attacks increasing in both prevalence and sophistication, cybersecurity is a pressing concern for all businesses. While high-profile thefts of consumer and commercial data draw the most public attention, recent reports indicate that sophisticated cyber scam artists are deploying fraudulent schemes to target company executives and their counsel, advisers, and consultants, as well as company vendors, in connection with corporate transactions, including financing transactions and mergers and acquisitions.

Of particular concern are reports that cyber scammers have hacked systems to create false emails to provide seemingly legitimate wire transfer instructions that misdirect funds transfers to third-party

accounts, including by providing a credible justification for the transfers, such as a closing or a litigation settlement. For example, in connection with a recent closing of one corporate transaction, hackers reportedly infiltrated the seller's systems and caused a fraudulent email to be sent to the buyer's lawyers, including modified wire transfer instructions that would have sent funds to a third-party account controlled by the hackers. In another sophisticated scheme that has reportedly been attempted on numerous occasions, scammers have utilized falsified emails that appeared to come from a corporate acquirer's lawyers or its finance executives instructing that funds be wired to a particular account, sometimes directing that the transfer be made according to instructions contained in an also-falsified email earlier in the chain that appeared to be from the company's CEO.

In addition, cybersecurity experts have reported the existence of a group that has been seeking to gain access to email accounts of company executives and their counsel, advisers, and consultants so as to gain access to material non-public information about nascent M&A deals and other announcements expected to affect securities trading.[1] Unlike widely publicized "phishing" attacks that are broadly disseminated and designed primarily to dupe the gullible, these targeted and more sophisticated "spear phishing" efforts appear to be written by native English speakers, employ credible investment terminology, and suggest familiarity with the internal operations of public companies. The group focuses on tricking targets into disclosing their network sign-on information, enabling the group to view email correspondence containing actionable non-public information.

In light of these reports, companies and their attorneys must exercise particular vigilance with regard to electronic communications that direct funds transfers, discuss sensitive information, or relate to user sign-on information. Companies should consider implementing heightened verification procedures before performing wire or other funds transfers according to electronically transmitted instructions, including where appropriate verifying transfer instructions orally. Similar caution should be taken with respect to requests or instructions to transmit sensitive information. Companies should also ensure that their outside counsel, advisers, consultants, and vendors observe similar safeguards.

* * *

[1] FireEye, Hacking the Street: FIN4 Likely Playing the Market (Dec. 1, 2014), available at https://www2.fireeye.com/fin4.html.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 800 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Stefanie S. Trilling (+1-212-558-4752; trillings@sullcrom.com) in our New York office.

CONTACTS

New York		
Jay Clayton	+1-212-558-3445	claytonwj@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Washington, D.C.		
Eric J. Kadel Jr.	+1-202-956-7640	kadelej@sullcrom.com
Brent J. McIntosh	+1-202-956-6930	mcintoshb@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com