WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

OCIE Reminds SEC Firms About Cybersecurity Following Global Ransomware Attack

May 22, 2017

AUTHORS

Elizabeth P. Gray | James E. Anderson | James R. Burns | Marc J. Lederer

On May 17, 2017, the SEC's Office of Compliance Inspections and Examinations ("OCIE") strongly encouraged investment management firms and broker-dealers to review their cybersecurity programs in light of the recent ransomware cyberattack that affected thousands of computers of businesses in over 100 countries around the world ("Ransomware Alert").[1] The ransomware, known as WannaCry, WCry, or Wanna Decryptor, exploited a vulnerability in Microsoft Windows, encrypting computer files and threatening to delete all data unless a ransom was paid. The SEC's Ransomware Alert is one of the first actions that the agency has taken under its new chairman, Jay Clayton, who was sworn into office on May 4, 2017. The action signals that Chairman Clayton will act on the concerns he has expressed regarding cybersecurity risk in the financial markets.[2] It also indicates OCIE's continued interest in requiring firms to test the sufficiency of their cybersecurity programs.

1 https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf.

2 At his Senate confirmation hearing, Chairman Clayton called for better cybersecurity disclosure by public companies and voiced his support for legislation that would require companies to disclose whether their boards of directors have cybersecurity experts. https://www.gpo.gov/fdsys/pkg/CHRG-115shrg24998/pdf/CHRG-115shrg24998.pdf. Chairman Clayton also wrote an article in 2015 calling for the

OCIE recommended that firms protect themselves against this ransomware by (1) reviewing the alert published by the United States Department of Homeland Security's Computer Emergency Readiness Team — U.S. Cert Alert TA17-132A[3] and (2) evaluating whether applicable Microsoft patches for Windows XP, Windows 8, and Windows Server 2003 operating systems are properly and timely installed.

OCIE noted that it recently conducted a cybersecurity examination of 75 SEC registered broker-dealers, investment advisers, and investment companies and found deficiencies in their cybersecurity practices. OCIE made a number of observations following those examinations that are relevant to this recent ransomware cyberattack:

- Five percent of broker-dealers and 26 percent of advisers and investment companies (collectively, "investment management firms") did not conduct periodic **cyber-risk assessments.**
- Five percent of broker-dealers and 57 percent of investment management firms did not conduct **penetration tests** and **vulnerability scans** on systems that the firms considered to be critical.
- Ten percent of broker-dealers and four percent of investment management firms had a significant number of critical and high-risk **security patches** that were missing important updates.

OCIE also reminded firms that the Division of Investment Management, OCIE, and FINRA have all provided guidance and information that firms may wish to consider when addressing cybersecurity risks and response capabilities.[4] The Ransomware Alert in particular noted the importance of firms' having incident response plans in place, including rapid response capability.

---

public and private sectors to work together to combat cyber threats. http://knowledge.wharton.upenn.edu/article/we-dont-need-a-crisis-to-act-unitedly-against-cyber-threats/.

[3] *See* U.S. Department of Homeland Security/U.S. Computer Emergency Readiness Team (US-CERT), Alert (TA17-132A), Indicators Associated with WannaCry Ransomware (May 12, 2017, last revised May 15, 2017) ("U.S. Cert Alert TA-132A"). This Homeland Security notice provides tips for prevention and remediation for this specific ransomware cyberattack as well as tips for preventing ransomware cyberattacks in general.

[4] *See* Division of Investment Management, IM Guidance Update: Cybersecurity Guidance (April 2015); OCIE, National Exam Program Risk Alert, OCIE's 2014 Cybersecurity Initiative (April 15, 2014), National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary (Feb. 3, 2015), National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015); and FINRA, Topic Page: Cybersecurity (last visited May 16, 2017).

If you have any questions regarding this memorandum, please contact Elizabeth P. Gray (202-303-1207, egray@willkie.com), James E. Anderson (202-303-1114, janderson@willkie.com), James R. Burns (202-303-1241, jburns@willkie.com), Marc J. Lederer (212-728-8624; mlederer@willkie.com) or the Willkie attorney with whom you regularly work.

May 22, 2017