WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

FINRA Fines Broker-Dealer $650,000 for Cybersecurity Lapses

November 21, 2016

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower | James R. Burns | Elizabeth P. Gray | Katherine Doty Hanniford | Marc J. Lederer

In the latest example of the increasing attention being paid to cybersecurity issues by regulators and other oversight officials, the Financial Industry Regulatory Authority ("FINRA") fined Lincoln Financial Securities Corporation ("LFS") $650,000 for its failure to adequately supervise third-party vendors tasked with electronic storage of customer records and electronic preservation and retention of customer consolidated reports, and other cyber risk compliance lapses, following a cyber attack in 2012 (the "2012 Cyberattack") where foreign hackers accessed 5,400 customers' confidential records and information.[1] In addition to the monetary penalty, LFS also agreed to undertake a review of its written supervisory procedures ("WSPs") and to implement necessary revisions to such procedures and systems that are reasonably designed to achieve compliance with the Safeguards Rule.

FINRA based its action upon certain alleged procedural, administrative and information technology data security deficiencies that occurred both before and after the attack. FINRA also took note of LFS' previous experience as the

[1] FINRA Letter of Acceptance, Waiver and Consent No. 2013035036601, November 14, 2016. It appears that FINRA levied this penalty despite the fact that LFS self-reported the underlying cyber attack to FINRA around August 2012, notified the affected individuals in writing, engaged an outside law firm and electronic forensic investigation firm to respond to the incident, and fully cooperated with FINRA in its investigation.

subject of a 2011 Letter of Acceptance, Waiver, and Consent ("AWC") for cybersecurity failures related to the safeguarding of customer records and information under Rule 30 of Regulation S-P of the Securities Exchange Act of 1934 (the "Safeguards Rule").[2] Specifically, FINRA found that LFS failed to reasonably safeguard confidential customer data and failed to reasonably supervise and retain consolidated reports, and that this conduct constituted violations of Section 17(a) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 17a-4 thereunder, in addition to NASD Rules 3010 and 3110, and FINRA rules 3110, 4511, and 2010.[3]

Overview of Alleged Violations

Failure to Reasonably Safeguard Confidential Customer Data

In June 2011, a branch office of LFS began storing sensitive customer records on a cloud-based computer server. According to FINRA's findings, LFS failed to ensure that the third-party vendor that configured the cloud-based server properly installed anti-virus software or data encryption for the stored documents. The data therefore were susceptible to cyber attack and indeed, hackers traced to foreign Internet Protocol addresses accessed the server and exposed the confidential records and information of approximately 4,500 LFS customers.

Accordingly, FINRA found that LFS failed to establish, maintain, and enforce a supervisory system, including WSPs, that were reasonably designed to ensure the security of customer records stored on electronic systems at LFS' branch offices. Specifically, FINRA found that prior to the 2012 Cyberattack, LFS failed to adopt WSPs regarding the storage of customer data on cloud-based systems. Furthermore, while LFS instituted a revised data security policy following the attack to provide some guidance to representatives regarding the storage of customer data on cloud servers, FINRA found that the revised policy was insufficient because it lacked specific guidance or instructions on data security, such as what type of firewalls were sufficient and the instructions needed for their implementation. FINRA noted that LFS representatives did not have the technical expertise to adequately interpret and apply the LFS general data security recommendations. In addition, FINRA found that, following the 2012 Cyberattack, LFS failed to ensure that its representatives or the third-party vendors retained by its representatives adequately applied its revised data security policy. Additionally, FINRA found that LFS did not adequately test and verify the security of information that continued to be stored on cloud-based servers, and could not tell whether a computer server was breached. FINRA cited its Notice to Members 05-48, where it states that: "[a]fter the member has selected a third-party service provider, the member has a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities."

---

[2] 17 C.F.R. § 248.30(a). The Safeguards Rule requires registered broker-dealers and investment advisers to adopt written policies and procedures reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

[3] NASD Rule 3010 was superseded by FINRA Rule 3110, and in this context applied to LFS' conduct prior to FINRA Rule 3110 becoming effective. NASD Rule 3110 was superseded by FINRA Rule 4511, and in this context applied to LFS' conduct prior to FINRA Rule 4511 becoming effective.

Failure to Reasonably Supervise and Retain Consolidated Reports

FINRA also concluded that LFS violated NASD Rule 3010(a) and FINRA Rule 2010 by failing to reasonably supervise and retain consolidated reports. According to FINRA, LFS used a software program developed by a third-party vendor to create customers' consolidated reports, which contain consolidated account information regarding most or all of a customer's assets. The software program permitted LFS representatives to enter assets and asset values manually into the reports if certain criteria were met. However, FINRA found that LFS failed to develop and implement any WSPs regarding the criteria, to ascertain whether the criteria were in fact met prior to a manual entry, or to review the criteria and actual use of manual entry in a consolidated report. FINRA also found that the software program would overwrite a consolidated report if it was updated or modified, which made LFS unable to reproduce such consolidated reports. This resulted in lost consolidated reports that could not be recovered, and LFS did not otherwise retain or centrally store copies of previous consolidated reports.

Conclusion

As the FINRA AWC makes clear, financial regulators continue to focus enforcement efforts on the Safeguards Rule, which has been in effect for more than 15 years but has become more critical given the proliferation of attempted and successful cyber attacks on financial institutions.[4] This case further emphasizes the importance of well-implemented WSPs, the role of compliance and risk management in identifying and mitigating cyber risk, and broker-dealers' obligations to oversee, supervise, and monitor third-party service providers' activities. Firms should periodically and sufficiently test and verify the security of information stored by third-party service providers, including the use of data encryption for data at rest and in transit, and other multi-layer defense mechanisms instituted to defend against cyber-events. Moreover, firms should ensure that personnel tasked with supervising cyber risk management and personnel responsible for implementing cyber-related policies possess the expertise and capabilities to effectively implement and monitor such cyber-related measures.

[4] *See* Willkie Farr Client Memorandum, "New SEC Enforcement Action Gives Force to Ongoing Safeguards Requirements," June 20, 2016, *available* here.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Elizabeth J. Bower (202-303-1252, ebower@willkie.com), James R. Burns (202-303-1241, jburns@willkie.com), Elizabeth P. Gray (202-303-1207, egray@willkie.com), Katherine Doty Hanniford (202-303-1157, khanniford@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

November 21, 2016