BRACEWELL

INSIGHTS

FINRA Fines Lincoln Financial Sub $650,000 For Cybersecurity Shortcomings

November 22, 2016

A Lincoln Financial Group subsidiary agreed to pay $650,000 to the Financial Industry Regulatory Authority (FINRA) to resolve allegations that it failed to implement sufficient security policies to protect confidential customer information after its web-based customer account database was hacked in 2012. The 2012 breach came on the heels of a $600,000 fine, imposed by FINRA in 2011, for lax security measures relating to its customer database.

Conduct

From 2002 to 2009, employees of Lincoln Financial Securities, Inc. ("LFS") and affiliated firm Lincoln Financial Advisors Corporation (collectively, "the firms") were able to access customer account details by means of shared user names and passwords. More than one million customer account records were accessed using the shared credentials during this time period. The firms did not track who had access to the login credentials so they had no way of knowing how many or which employees accessed customer data. No policies were in place to change the shared credentials when an employee left the firm or was terminated. In February 2011, FINRA imposed a $450,000 fine on LFS to resolve these shortcomings; Lincoln Financial Advisors was fined $150,000.

In June 2011, LFS migrated many of its records – including those containing customer non-public personal information such as social security numbers – to a cloud-based server. LFS failed, however, to ensure that the third-party cloud host had sufficient antivirus software or data encryption in place. The information of approximately 5,400 customers was exposed in January 2012. LFS reported the breach to FINRA in August 2012.

In November 2012, LFS adopted written supervisory procedures ("WSPs") regarding the storage of customer data on the cloud-based server. LFS's WSPs fell short in providing adequate guidance to the firm's employees in implementing and enforcing the new policies. For example, the data security policy required that "[f]irewalls must be used to prevent unauthorized access." Yet the policies offered no help in how to install such a firewall. Similarly, the WSPs required written authorization by the customer before a firm employee could manually make changes to the customer's consolidated asset reports. The WSPs, however, did not offer any acceptable forms of written authorization, or any supervisory systems to ensure that the required authorization was secured.

LFS also failed to adequately preserve some consolidated reports. From December 2010 to December 2013, the firm relied on third-party vendor software to produce current reports as well as maintain past data for report generation. Unfortunately, LFS discovered that when certain information on a report was modified or updated, the report was overwritten and past data could no longer be reproduced.

LFS has agreed to a monetary fine of $650,000 to resolve the issues that arose since its last settlement.

Takeaways

The best approach to cybersecurity is that a firm have effective WSPs and oversight in place before it becomes subject to regulatory scrutiny. In the event that a firm has settled cybersecurity allegations with a regulator, it is critical that the firm undertake demonstrable improvements in policies and protocols to avoid becoming a repeat offender. While no company enjoys a regulatory review, it can identify concrete areas in which a firm can strengthen its WSPs as well as create an opportunity to recommit to upholding security policies.

Moreover, the facts from the LFS settlement illustrate a real issue that many member firms face – the reliability of third-party vendors. As companies from a cross-section of industries are increasingly migrating their business systems to the cloud, member firms are sometimes blindly putting their trust, and by extension that of their customers, into the hands of outside vendors who may or may not fully appreciate the security requirements imposed on regulated entities. The proper vetting and supervision of vendor cybersecurity practices are just as critical as maintaining one's own WSPs.

* * *

Rule 30(a) of Regulation S-P, the Safeguards Rule, requires brokers and dealers to adopt written policies and procedures reasonably designed to maintain the confidentiality and security of customer information, anticipate and defend against threats to the security of such information, and protect customers from harm or inconvenience as a result of unauthorized access to customer information.

NASD Rule 3010 and FINRA Rule 3110 require that member firms maintain a system, including WSPs, to supervise the activities of each registered person that is reasonable designed to achieve compliance with applicable securities laws and regulations.

NASD Rule 3010(a) and FINRA Rule 2010 require reasonable supervision of consolidated reports.

*The full text of the Lincoln Financial Securities settlement is available **here**.*