CARLTON FIELDS

FINRA Focus on Cybersecurity Continues

December 22, 2016

On November 14, the Financial Industry Regulatory Authority (FINRA) imposed a $650,000 fine against Lincoln Financial Securities Corporation (Lincoln Financial) for its failure to implement adequate data security measures to protect confidential customer information. Specifically, FINRA found that, between 2011 and 2015, Lincoln Financial failed to adopt and maintain supervisory procedures, including written policies, to ensure the security of customer information stored electronically at its branch offices. FINRA took issue with both the firm's policy regarding the use of cloud-based systems as well as its failure to ensure its registered representatives and third party vendors were appropriately applying these procedures. This action follows a February 2011 FINRA action that resulted in the imposition of a $450,000 fine for similar data security failures, including enabling employees to access customer data online using shared login credentials without instituting procedures to safeguard the information or monitoring access to the accounts. The data, which included personal and financial information such as names, birthdates, addresses, Social Security numbers, email addresses, account numbers and balances, and transaction information, could be accessed from any Internet browser using the shared credentials. In total, the firm's failure to adequately secure its login details placed more than 260,000 customer records at risk. Moreover, because the firm did not institute procedures to monitor the distribution of the login information or access to the website, it had no way to determine who was accessing the information and when. The firm further failed to require brokers to install security software on their personal computers that would protect customer data when they worked remotely on firm business. FINRA alleged Lincoln Financial's conduct violated Rule 30 of Regulation S-P, requiring broker-dealers to adopt written policies to safeguard customer records and protect against unauthorized access; NASD Rule 3010, requiring supervision of registered persons to ensure compliance with applicable regulations; as well as NASD Rule 2110 and FINRA Rule 2010, requiring firms to maintain high standards in business. Lincoln Financial's failure to implement sufficient cybersecurity procedures contributed to a 2012 data breach in which foreign hackers stole the records of more than 5,000 customers. The breach occurred after Lincoln Financial began using a cloud-based server to store customer information without requiring the third party vendor involved in the set-up to install security software on its

computers. FINRA specifically stated that the security policy adopted post-breach was inadequate, as it provided insufficient guidance regarding what security measures were required or how to implement them, instead leaving it up to the representatives themselves. Moreover, FINRA found the firm had failed to supervise both its registered representatives and their third party vendors to ensure they were following the proper guidelines and protecting customer information, including by not monitoring or auditing the third parties to ensure compliance. Lincoln Financial consented to the $650,000 fine pursuant to a Letter of Acceptance, Waiver, and Consent without admitting or denying FINRA's findings. A Corrective Action Statement submitted by the firm stated it had taken measures to improve. These included hiring additional data security personnel and enhancing its training for representatives, hiring experts to evaluate its cybersecurity policies, implementing improved audit procedures at its branch locations, and holding regular meetings to assess the security of its data. **Takeaways** Though the landscape has changed significantly since 2011, increased regulation related to data security and the threat of breaches are now the norm. Adopting advanced security measures is no longer optional. In particular, both FINRA and the Securities and Exchange Commission require broker-dealers to adopt written data security policies and procedures. Firms must take steps to not only implement but continuously monitor and maintain adequate procedures to stay ahead of cybersecurity threats and business developments. Because technology and procedures change—for example, a firm may adopt cloud-based storage—the policies must be reviewed and revised as appropriate to maintain effective security.

1. Details Matter In adopting these policies and procedures, general guidance is not enough. Even after a firm adopts written procedures, FINRA may determine those procedures lack specificity and fall short of what applicable regulations require. For example, a firm's written policy should not simply state that representatives must use security measures like firewalls and anti-virus software to prevent unauthorized access to customer records. Instead, it should include specifics, such as what type of firewall should be used and how it should be installed. Firms can no longer rely on representatives to interpret and implement specific policies based on general best practices, as they may not have the requisite technical knowledge to do so. Rather, firms are required to develop specific and adequate security plans and ensure their representatives are able to properly implement them. Where firms lack the ability to do so themselves, they must bring in experts to advise on potential risks and appropriate procedures. **2. Branch Supervision is Vital** More generally, firms are responsible for the information security practices of branch offices, and ongoing supervision is essential to ensure data protection. In addition to adopting written procedures and overseeing their implementation, firms must take an active role in monitoring branches for compliance. Firms should engage in regular audits of these locations to ensure security measures are effective and up to date. In addition, firms must implement procedures to monitor the security of the systems used at branch offices on an ongoing basis. In this way, firms will be able to act quickly if necessary to avert a threat or respond in case of unauthorized access. Ultimately, ongoing supervision is not only required by applicable laws and regulations, it can significantly help minimize a data breach's effects. **3. Security Does Not Stop at the Door** Firms are not just responsible for their employees and registered representatives, but for third party vendors—even where those

vendors are retained by the representatives. NASD Rule 3010 (effective prior to December 1, 2014) and FINRA Rule 3110 (effective December 1, 2014), both require firms to maintain supervisory systems, including written policies, that enable them to oversee the activities of registered representatives and ensure they are in compliance with relevant laws and regulations. Information is placed at risk whenever it is shared, and firms are responsible for safeguarding customer information at each point of access. In essence, it is not the security of a firm's own system, but the security of the information generally that matters. Thus, firms must take an active role in guiding representatives and third parties and ensuring such policies are properly implemented. **4. Security is Ongoing** Moreover, it is not enough to simply institute such systems and mandate compliance by third parties; firms have a continuing obligation to ensure information is being protected. This involves ongoing testing and supervision. Also, firms must implement procedures that would enable them to track access to data and determine whether a server at any of their branches was breached. Personnel training can help keep data secure, but it is not enough. Regular meetings by those involved with data security and compliance, as well as the adoption of audit procedures to ensure the continued security of hardware and software are necessary. **5. Communication is Key** When information is placed at risk or a breach occurs, firms must be prepared to respond. In particular, communications with customers matter. Having proper procedures in place to deal with a security breach and assist affected customers will not only help minimize the damage but can affect the way in which regulators view a firm. Ultimately, given increased enforcement of cybersecurity regulations, and a rise in data breaches themselves, firms must take their responsibility to safeguard customer data seriously. This obligation includes not only implementing proper procedures, but supervising third parties and engaging in ongoing monitoring to ensure these security measures are effective and up to date.

Related Practices

Cybersecurity and Privacy
Securities Litigation and Enforcement
FINRA Enforcement, Arbitration, and Appeals

Related Industries

Life, Annuity, and Retirement Solutions