BNA's

BROKER/DEALER COMPLIANCE REPORT

BNA Employee-Owned Since 1947

CYBERSECURITY

Cybersecurity and the SEC Recent Developments in Compliance and Enforcement

BY KATHY DELANEY WINGER

If you're a registered investment advisor or broker-dealer, there is yet another reason to pay close attention to cybersecurity. The two recent developments discussed below make it abundantly clear that the Securities and Exchange Commission ("SEC") will likely be focusing even more intensely on the cybersecurity practices of the companies it regulates.

On the compliance front, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert on September 15, 2015. The Alert identifies the areas that the OCIE will focus on in its second round of cybersecurity examinations. Those areas and the questions you should be asking yourself with respect to those areas:

1. Governance and risk assessment: Are you periodically evaluating cybersecurity risks? Are your controls and risk assessment processes tailored to your business? Do you have adequate governance and risk assessment processes and policies in place to address the focus areas discussed in #2 through #6, below? What is the board of directors' and the senior management team's level of involvement in these five focus areas?

2. Access rights and control: Have you implemented basic controls to prevent unauthorized access to systems or information (e.g. multifactor authentication, updating access rights based on personnel or system changes)? How do you control access to various systems and data via management of user credentials, authentication, and authorization methods (e.g., controls associated with remote access, customer login, passwords, and firm protocols to address customer login problems, network segmentation and tiered access)?

3. Data Loss Prevention: How do you monitor the volume of content transferred outside of the firm by its employees or third parties (e.g., by email attachments or uploads)? How do you monitor for potentially unauthorized data transfers? How do you verify the authenticity of a customer request to transfer funds?

4. Vendor Management: What are your practices and controls related to vendor management (e.g., due diligence with regard to vendor selection, monitoring and

oversight of vendors, contract terms)? How are vendor relationships considered as part of your ongoing risk assessment process? How do you determine the appropriate level of due diligence to conduct on a vendor?

5. Training: How is your training tailored to specific job functions? How is your training designed to encourage responsible employee and vendor behavior? How are procedures for responding to cyber incidents under an incident response plan integrated into regular personnel and vendor training?

6. Incident Response: Have you established policies and assigned roles? Have you assessed system vulnerabilities and developed plans to address possible future events? Have you determined which firm data, assets and services warrant the most protection to help prevent attacks from causing significant harm?

On the enforcement front, the SEC brought and settled charges against a registered investment advisor on September 23, 2015. The following circumstances led to the charges:

The advisor required prospective customers to submit their names, dates of birth and social security numbers to its website to verify that they were eligible participants of the retirement plan for which the advisor provided managed account services. The website was hosted on a third-party server and contained customers' personally identifiable information. All data was stored in unencrypted formats and the advisor had not adopted written policies and procedures regarding the security and confidentiality of the information and the protection of the information from anticipated threats or unauthorized access. The server operated from 9/09 to 7/12. In July 2013, the advisor discovered that unknown hackers had obtained access to the data on the server.

The SEC found that the advisor has failed to adopt policies and procedures to protect its clients' information including, among other things, failing to conduct periodic risk assessments, failing to implement a firewall, failing to encrypt personally identifiable information on its server; and failing to maintain a response plan for cybersecurity. The SEC ordered the advisor to cease and desist from these practices (which, in its view, violated Reg. S-P[1]) and fined the advisor $75,000.00.

Both of the above events make it crystal clear that the SEC (like many other regulatory agencies) is focusing and will continue to focus very closely on cybersecurity from both a compliance and an enforcement perspective. Thus, you should focus on it too by taking the necessary steps to ensure that your customers' personal information and other confidential information is protected. A sample list of information that the OCIE would likely request and use in conducting its examinations of registered entities regarding cybersecurity matters is attached to the Security Alert.. At a minimum, you should review that list and use it to evaluate your cybersecurity practices, procedures and policies.

* * * * *

Kathy Delaney Winger is a banking and business attorney who represents banks, credit unions, financial services companies and businesses in commercial and corporate transactions. She has more than 15 years of experience as an attorney in the private sector practicing banking, regulatory, compliance, business, consumer and commercial lending law. Prior to entering private practice, Kathy served as in-house counsel to the credit card division of a national bank and financial services company for more than 5 years. Kathy's experience as both in-house and outside counsel provides a unique perspective for her clients. Kathy is a partner at Munger Chadwick, P.L.C., a full service law firm in Tucson, Arizona, that operates in virtually every practice area important for businesses. You can contact Kathy at kdwinger@mungerchadwick.com.

[1] Implementing the Gramm-Leach-Billey Act and codified at 17 C.F.R. § 248.30(a).

  BDC ISSN 0000-0000