CARLTON FIELDS

Continuing Data Security Lessons from the SEC

May 05, 2016

In September, we reported that the Securities and Exchange Commission (SEC) settled charges against a registered investment adviser for a violation of Rule 30(a) of Regulation S-P (17 C.F.R. 248.30(a))("Safeguards Rule") for failing to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records and information. In January, the SEC reaffirmed its intent to enforce such violations in its release, *Examination Priorities for 2016,* which details this year's examination focus for the Office of Compliance Inspections and Examinations (OCIE). Most recently, in April, the SEC charged a broker-dealer and principals with violating the Safeguards Rule as well as failure to preserve email and eFax business communications. This Administrative Proceeding highlights the SEC's continued determination to ensure the security and confidentiality of customer information and records, and its intent to pursue any breach in internal procedures regarding the protection of such information. According to the SEC Order resulting from the above Administrative Proceeding, Craig Scott Capital, LLC (CSC), its chief executive officer and president, who also served as chief compliance officer (CCO), and its chief operating officer (COO) routinely failed to adopt and enforce CSC's own policies and procedures regarding the use of company email and eFax for sensitive customer information. Upon registering in 2012, CSC provided firm email addresses for all employees. Shortly thereafter, an eFax system was created that automatically converted the contents of all email messages sent to CSC's fax number into an electronic file. The eFax files were subsequently routed by email to designated email addresses, two of which did not contain the

@craigscottcapital.com domain name. CSC concurrently established written supervisory procedures (WSPs), which prohibited using personal email accounts for business communications. Throughout this period, however, CSC employees routinely used eFaxes and personal email accounts to effect business transactions on behalf CSC, including receiving clients' sensitive and confidential information. Records such as opening documents, asset transfer forms, and other agreements between CSC and its customers containing social security numbers, birthdates, and account numbers were shared outside of CSC's internal controls. Furthermore, an administrative assistant's personal email was routinely used to receive eFaxes sent to CSC containing customer information and records. The SEC found that during this period, the WSPs implemented by CSC were deficient due to the lack of a "designated supervisor," failure to identify a "designated information officer," failure to ensure compliance with the CSC's own safeguards policy, that CSC's safeguards policies were inadequately tailored to the systems the broker used to collect sensitive and confidential information, and that CSC's policies and systems were inadequate to protect the information collected. The SEC ordered that CSC cease and desist from committing or causing these violations and imposed a civil money penalty of $100,000 against CSC and $25,000 against both of CSC's individual corporate officers named in the Administrative Proceeding. Takeaways from this Administrative Proceeding and our September article include:

- Both firms and individual officers could be sanctioned even if no one is financially harmed.
- Written supervisory procedures (WSPs) should not be boilerplate. Policies and procedures should reflect significant thought to ensure they are actually tailored to the firm.
- Never use personal email to conduct business.
- Domain names should clearly relate the firm to its email address.
- Designated personnel responsible for ensuring data compliance and managing information security must be identified by name in firm policies.
- Personally identifiable information (PII) should be encrypted.
- Develop, implement, and maintain a written security information plan (WISP).
- Systems should be put in place to prevent and detect breaches.
- Ongoing systems monitoring and regular reporting to management on the effectiveness of security systems should be instituted.
- Know what information your outside vendors and suppliers are collecting and maintaining, and what they are doing to protect it.
- Collect the minimum amount of PII needed for your business purposes.

This is not an exhaustive list of all steps registered broker-dealers should take, but serves as a reminder that the SEC is serious about ensuring broker-dealers act to mitigate cyber risks.

Related Practices

Cybersecurity and Privacy
Securities Litigation and Enforcement
Securities Transactions and Compliance
Technology

Related Industries

Technology