Akin®

SEC Brings Enforcement Action Against a Broker-Dealer for Weak Cybersecurity Controls

Apr 21, 2016

Reading Time : **2 min**

By: Jenny M. Walters, Jason Daniel, Jo-Ellyn Sakowitz Klein, Natasha G. Kohne, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

The broker-dealer, Craig Scott Capital, LLC (CSC), used email addresses other than those within its domain name to electronically receive more than 4,000 faxes from customers and other third parties, which routinely included sensitive customer records and information, such as customer names, addresses, social security numbers, bank brokerage account numbers, copies of driver's licenses and passports, and other customer financial information. The two settling principals of CSC also used their personal, non-CSC email addresses for matters relating to the business of CSC. The SEC also found that CSC did not maintain and preserve either these faxes or this email correspondence as required by Section 17(a) of the Exchange Act.

Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30 (a)), otherwise known as the "Safeguards Rule," requires that every broker-dealer registered with the SEC adopt 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. The SEC adopted amendments to the Safeguards Rule in 2005 that require that policies and procedures adopted thereunder be in writing. Though CSC had written supervisory procedures (WSPs) during the relevant period, the SEC found that these WSPs were not reasonably designed to protect customer records and information, as

required by the Safeguards Rule, since they (i) failed to designate the responsible supervisor, (ii) failed to address how customer records and information transmitted through the fax system were to be handled, (iii) contained blanks as to how CSC was to comply with the Safeguards Rule, and (iv) were not tailored to the actual practices at CSC.

This enforcement action against CSC is a warning and reminder for registered firms to:

- carefully construct cybersecurity and other written policies and procedures
- make sure these policies and procedures are complete and tailored to the companies' business and practices
- review cybersecurity practices to ensure that information security measures are consistent with the emerging standard of care to be enforced by regulators;
- never use non-domain emails or fax accounts for business purposes, especially relating to personally identifiable customer information.

It is also a reminder that off-the-shelf compliance manuals that are not effectively implemented remain a target for SEC enforcement.

Categories

Cybersecurity, Privacy & Data Protection | Compliance