PUBLICATION

SEC Issues Risk Alert on Regulation S-P

Authors: Matthew George White, Alexander Frank Koskey, III
May 2019

It should not be surprising to anyone that cybersecurity and data protection remain top priorities for regulators of the financial services industry. Indeed, cybersecurity has been regularly identified as a key priority by both FINRA and the SEC for several years. In addition to issuing guidance, both FINRA and the SEC have instituted several high profile actions against companies for their failure to protect customer information.

Recently, the SEC's Office of Compliance Inspections and Examinations (OCIE) again highlighted their focus on these issues. On April 16, the OCIE published a Risk Alert highlighting the most common compliance issues under Regulation S-P, which governs privacy notices and safeguard procedures for investment advisers and broker-dealers. The Risk Alert noted specific deficiencies with (1) privacy and opt-out notices and (2) implementing effective policies and procedures to safeguard customer information. While prior risk alerts have focused on general practices and requirements, the specificity of this most recent alert by the OCIE emphasizes the need for firms to review their privacy and security policies and procedures to assess compliance with Regulation S-P. In particular, the OCIE has stressed a clear requirement for firms to have written policies and procedures implementing specific safeguards for customer information.

Privacy and Opt-Out Notices

Under Regulation S-P, advisers and broker-dealers are required to provide three core notices to customers: (a) an Initial Privacy Notice describing its policies and procedures; (b) an Annual Privacy Notice describing policies and procedures during the continuation of the customer relationship, and (c) an Opt-Out Notice explaining to customers the right to opt-out of certain disclosures of non-public personal information to nonaffiliated third parties.

In its Risk Alert, the OCIE noted situations where advisers and broker-dealers either did not provide the required privacy notices to customers or, when such notices were provided, the notices did not accurately reflect the policies and procedures of the company. In addition to not providing the required privacy notices, the OCIE noted situations where companies failed to identify opt-out rights to customers within their privacy notices.

Safeguard Policies and Procedures

The OCIE also noted that firms failed to comply with the Safeguards Rule under Regulation S-P by not having written policies and procedures addressing the security and confidentiality of customer records and information. There were also occurrences where some firms had policies and procedures simply restating the Safeguards Rule, but failed to have specific policies and procedures addressing administrative, technical, and physical safeguards required under the rule.

The three most common problems noted by the OCIE under the Safeguards Rule were the failure to implement or reasonably design policies and procedures that (1) ensured the security and confidentiality of customer information; (2) protect against anticipated threats or hazards regarding the integrity of customer information; and (3) protect against unauthorized access to customer information which could result in substantial harm. The following are a few of the specific issues the OCIE noted:

- **Personal Devices:** Policies and procedures did not address safeguards for customer information on personal devices. The OCIE observed firm employees who regularly stored customer information on personal laptops without policies and procedures addressing how these devices were to be safeguarded.

- **Electronic Communications:** Policies and procedures did not address the inclusion of personally identifiable information in electronic communications. This included the lack of procedures to prevent employees from sending unencrypted emails containing personally identifiable information.

- **Training / Monitoring:** Policies and procedures that failed to provide adequate training to employees on certain procedures including requiring customer information to be encrypted, password-protected, and transmitted using only firm-approved methods.

- **Unsecure Networks:** Policies and procedures which did not address or prohibit employees from sending customer information to unsecure locations.

- **Outside Vendors:** Firms failing to follow and monitor outside vendors for compliance with contractual agreements which required vendors to keep customer information confidential.

- **Inventory of Customer Information:** Failure of firms to identify a complete inventory of all systems where customer information was held, including the categories of customer information maintained and adopting policies and procedures to adequately safeguard such information.

- **Incident Response Plans:** Firms not adopting comprehensive incident response plans addressing specific role assignments for implementing such plans, actions required to address security incidents, and procedures for assessing system vulnerabilities.

- **Former Employee Access:** Allowing former employees to retain access rights to customer information after departure from company (i.e., failure to have proper termination procedures).

As noted above, this Risk Alert follows several actions against companies for violations of Regulation S-P. Several of these actions over the past few years have included:

- On September 26, 2018, the SEC announced that a broker-dealer and investment adviser agreed to pay $1,000,000 to settle charges related to failures in cybersecurity policies and procedures surrounding a cyber intrusion that compromised personal information of thousands of customers. The SEC charged the firm with violating the Safeguards Rule (Rule 30(a) of Regulation S-P) and the Identity Theft Red Flags Rule, which are designed to protect confidential customer information and protect customers from the risk of identity theft. The SEC found that cyber intruders managed to bypass the firm's cybersecurity protocol by impersonating firm contractors and calling the firm's technical support hotline, requesting that the passwords be reset, then using the reset passwords to access 5,600 customers' personal information. The key cybersecurity protocol failure, according to the SEC, centered on the firm's "failure to terminate the intruders' access" and its failure "to apply its procedures to the systems used by its independent contractors."

- On June 8, 2016 – The SEC fined another firm $1,000,000 for failing to protect customer information, some of which was hacked and offered for sale online. The firm used web "portals" for employees to access customer information; however, they did not have effective authorization modules to restrict access solely to employees with legitimate business needs, and did not audit or test the relevant authorization modules. The SEC found that as a result of these failures, from 2011 to 2014, a then-

employee impermissibly accessed and transferred the data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties. Following the hack of the personal server, portions of the confidential data was posted on the Internet with offers to sell larger quantities.

- September 22, 2015 – The SEC settled with a firm for $75,000 for failing to establish adequate cybersecurity policies and procedures in advance of a breach that made PII of approximately 100,000 individuals, including thousands of the firm's clients vulnerable to theft. The firm's web server was attacked in July 2013 by an unknown hacker who gained access and copyright to the data on the server, rendering the PII of more than 100,000 individuals, including thousands of the firm's clients, vulnerable to theft. The SEC found that the firm failed to adopt written policies and procedures reasonably designed to safeguard customer information. For example, the firm failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents. Notably, there were no indications of financial harm to any customers as a result of the attack, and the firm provided notice of the breach and offered free identity monitoring to every affected individual.

These actions are representative of the SEC's continued focus on cybersecurity and data protection, and its willingness to bring actions against companies it believes have failed to protect customer information. We expect more enforcement actions; in fact, the SEC has created a "Cyber Unit" within its enforcement division.

The SEC's focus has not been limited to broker-dealers and investment advisers. The SEC has also recently issued guidance for public companies regarding how and when to disclose actual and potential cybersecurity-related risks, breaches, or incidents. Shortly after issuing this guidance, the SEC fined a company $35 million for failing to disclose a substantial data breach and cyberattack.

One thing is for sure: the SEC's focus on cybersecurity-related matters is not going away. Firms need to ensure that they have sufficient policies and procedures in place to address cyber-related concerns and that those policies and procedures are being followed, and must regularly train their employees and test their systems to reduce the likelihood of a data incident.

If you have any questions regarding these issues, your data protection program, policies, or procedures, or any other cybersecurity or data privacy-related matters, please contact Matt White, Alex Koskey, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.