The SEC Charges Investment Adviser with Violating Regulation S-P by Failing to Adopt Cybersecurity Policies and Procedures

Written by Catherine M. Anderson

September 25, 2015

In recent years, the SEC has been focused on cybersecurity. It has issued risk alerts, conducted examinations and provided guidance about what the agency sees as widespread weaknesses in many policies and procedures to protect against cyberthreats. The SEC has now taken the next step: a few days ago, the SEC brought its first-ever enforcement action for a violation of Regulation S-P, 17 C.F.R. § 248.30(a) – known as the "Safeguards Rule" – against an investment adviser that was itself the victim of a security breach in which hackers stole customer information. *See* In re Matter of R.T. Jones Capital Management Equities, Inc., AP No. 3-16827 (Sept. 22, 2015). This recent action makes clear that advisers cannot afford to wait until after a potential data breach to deal with cybersecurity.

Cybersecurity Examination Activity

By way of recap, in March 2014, the SEC hosted a Cybersecurity Roundtable that addressed cybersecurity, the challenges that it raises for market participants, and how these issues might be addressed. Shortly thereafter, in April 2014, the Office of Compliance Inspections and Examinations issued a Risk Alert regarding an initiative to assess cybersecurity preparedness and threats in the securities industry. That initiative included examinations of a sample of SEC-registered investment advisers and broker-dealers.

In February 2015, the SEC released its report of observations from these examinations. That report reflected some serious concerns: for example, the SEC found that most advisers had adopted cybersecurity policies and procedures, but only about half of them periodically audited compliance, even though three-quarters reported suffering cyberattacks. It also found that fewer than one-quarter of the examined advisers had considered cybersecurity as it relates to third-party vendors. In April 2015, based largely on the same report, the Investment Management Division released additional cybersecurity guidance.

Earlier this month, the Office of Investor Education and Advocacy issued an alert titled, "Identity Theft, Data Breaches and Your Investment Accounts." The OCIE also issued yet another Risk Alert; this latest initiative features a second round of examinations with a focus on more testing of cybersecurity policies and procedures to assess implementation of firms' controls.

Further information on these initiatives can be found in our previous Foley Advisers:

- SEC Issues Risk Alert on Cybersecurity Initiative for Investment Advisers
- SEC Office of Compliance Inspections and Examinations Releases Cybersecurity Examination Sweep Summary of Investment Advisers and Broker-Dealers
- OCIE's 2015 Cybersecurity Examination Initiative

First-of-its-kind Enforcement Action

The continued focus on cybersecurity at the SEC has now expanded to include enforcement. On September 22, 2015, the Enforcement Division announced a novel case arising from a violation of Regulation S-P, which requires investment advisers, investment companies, and broker-dealers to adopt written policies and procedures that are "reasonably designed" to protect customer records and information. The SEC charged a St. Louis-based investment adviser, R.T. Jones Capital Equities Management, Inc., with failing to establish required cybersecurity policies and procedures in advance of a data breach that compromised the personally identifiable information ("PII") of approximately 100,000 individuals, including thousands of the firm's clients.

To settle the matter, the SEC and R.T. Jones agreed to the following sanctions: the SEC issued a cease-and-desist order and censured the firm, and R.T. Jones agreed to pay a civil monetary penalty of $75,000. Notably, prior to the enforcement action, R.T. Jones had already taken a number of remedial steps, including adopting written policies and procedures, appointing an information security manager, encrypting PII on its internal network, installing new firewalls and logging systems, and retaining an independent cybersecurity firm to provide reports and advice. In its order, the SEC acknowledged these efforts.

The SEC brought this enforcement action against R.T. Jones despite the fact that the firm has not received any indications that any of its clients had suffered financial harm as a result of the cyberattack. That decision was likely intended to send an important signal. Commenting on the case, Marshall Sprung, Co-Chief of the Enforcement Division's Asset Management Unit, emphasized the importance of enforcing the Safeguards Rule, given the "increasing barrage of cyberattacks on financial firms." Cybersecurity is an enforcement priority, said Sprung, "even in cases like this one when there is no apparent financial harm to clients." In other words, the SEC wants advisers to be proactive, not reactive, when it comes to cyberthreats.

Next Steps for Advisers and the SEC

The recent enforcement action offers investment advisers important lessons about what they need to do to comply with the Safeguards Rule and ensure adequate cybersecurity. It would be a mistake to dismiss R.T. Jones as an "outlier" because, as the SEC press release notes, the firm "failed to establish *any* written policies and procedures" to address cybersecurity.

Firms that have already adopted written policies and procedures regarding cybersecurity should, at a minimum, ensure that they have taken the following steps:

- review policies and procedures to ensure that they are reasonably designed to safeguard client information in light of evolving threats from hackers,
- conduct periodic risk assessments,
- implement firewalls,
- encrypt PII stored on its servers, and
- maintain an appropriate response plan for responding to cybersecurity incidents and mitigating any damage.

Of course, it goes without saying that if a firm has not yet adopted any written policies and procedures, it should immediately do so.

The action against R.T. Jones also offers hints about what the SEC might do next, particularly on the enforcement front. First, the Safeguards Rule requires written policies and procedures that are "reasonably designed" to prevent damaging cyberattacks. Simply having some written guidance on cybersecurity will not suffice. Firms must take approaches that are appropriately tailored to their business models, operational practices and the particular cyberthreats that they face. Firms must also adapt as their circumstances change (e.g., the types of customer information that they collect).

Moreover, the Safeguards Rule broadly protects customer information, not only account information or financial data. R.T. Jones, for example, ran afoul of the rule by exposing to hacking certain "personal identifiable information" – known as PII – including names, dates of birth and social security numbers. It did "not control or maintain client accounts or client account information." Firms should not assume, therefore, that they face no risk under the Safeguards Rule if they possess only limited customer PII as opposed to account information. Similarly, Regulation S-P is about information, not assets. R.T. Jones did not, as the SEC order recognized, have custody of client assets. It would also be a mistake for firms to conflate complying with the Custody Rule (or not falling under it, like R.T. Jones) with satisfying the Safeguards Rule.

Finally, one thing that this recent action makes clear is that, according to the SEC, "no harm, no foul" is not a defense to charges that a firm failed to protect customer information. As noted above, the SEC acknowledged that R.T. Jones has "not learned any information indicating that any client had suffered any financial harm as a result of the cyberattack," and the SEC itself pointed to no such harm. Nevertheless, the SEC brought an enforcement action, issued a cease-and-desist order, censured R.T. Jones and imposed a penalty of $75,000. This case shows that potential liability under the Safeguards Rule does not turn on the intent of the adviser or the harm to its investors.

RELATED INDUSTRIES

- Investment Advisers & Private Funds

- Professional Services

RELATED PRACTICES

- Business Counseling
- White Collar Crime & Government Investigations
