The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 23, NO. 9 • SEPTEMBER 2016

REGULATORY MONITOR

SEC Update

By Timothy C. Blank, D. Brett Kohlhofer, and Hilary Bonaccorsi

Tailored Cybersecurity Programs Remain a Policy and Enforcement Focus for Financial Regulators

Recent pronouncements from US government officials, as well as regulatory actions, have made it clear that ensuring financial institutions' cybersecurity will be a major priority for the Securities and Exchange Commission (SEC) and other regulators charged with safeguarding financial markets.

Market Regulators Recognize and Respond to the Growing Cybersecurity Threat

In recent weeks, the SEC Chair Mary Jo White, and the Chairman of the Commodity Futures Trading Commission (CFTC), Timothy Massad, each identified cybersecurity as a critical risk for the financial industry and a priority for their respective agencies. Most recently, on June 2, 2016, the SEC appointed a new Senior Advisor to the Chair for Cybersecurity Policy. In commenting on the appointment, Chair White yet again reiterated the SEC's cybersecurity focus. Earlier, in a May 2016 address to the Investment Company Institute's (ICI) General Membership Meeting, Chair White explained that "[c]ybersecurity is … one of the greatest risks facing the financial services industry." Chair White also identified cybersecurity as a "key element" of the "evolution of regulation for the asset management industry" and an area in which industry participants "have major responsibilities."

Similarly, in a May 2016 interview at the Reuters Financial Regulation Summit, Chairman Massad underscored the importance of cybersecurity when he commented that "[c]yber is the biggest threat facing financial markets today." In a further parallel to Chair White's commentary, Chairman Massad emphasized cybersecurity-related regulatory obligations, noting that the CFTC has undertaken its own review of the industry's cybersecurity. He added that the CFTC plans to finalize new cybersecurity rules before year-end;[1] the CFTC proposed rule would apply only to markets, not asset managers.

The Importance of Tailored Cybersecurity Policies for Asset Managers

For asset managers, a central responsibility is to ensure that the firm maintains written policies and procedures related to cybersecurity.[2] Chair White indicated, in her May 2016 address, "[the SEC's] regulatory efforts are focused primarily on ensuring that our registered entities have policies and procedures to address the risks posed to systems and data by cyberattacks." Further, she warned that "[c]yber risks can produce far-reaching impacts, and robust and responsible safeguards for funds and for their investors must be maintained."

Over the last year, the SEC and its Staff have made clear that firms need not only maintain written cybersecurity policies and procedures, but that they must also tailor those policies and procedures to their own business practices and risks. Indeed, in her comments to the ICI, Chair White instructed firms to "consider the full range of cybersecurity risks to their funds and consider appropriate tools and procedures to prevent breaches, detect attacks and limit harm."

Consistent with the Chair White's admonition, the SEC's Division of Investment Management's April 2015 Cybersecurity Guidance explained that "[b]ecause funds and advisers are varied in their operations, they should tailor their compliance programs based on the nature and scope of their businesses."[3]

Despite the SEC's continued focus on tailored policies and procedures, last month Chair White candidly assessed that "so far, [the Commission has found] a lot of preparedness, a lot of awareness but also [that] policies and procedures are not tailored to their particular risks[.]"[4] As a result, the SEC Staff continues to demonstrate its commitment to policing this issue.

By way of background, in 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) announced a Cybersecurity Initiative – an initiative to examine the cybersecurity practices at registered broker-dealers and registered investment advisers.[5] In late 2015, OCIE launched its second Cybersecurity Examination Initiative – focusing on cybersecurity compliance and controls.[6] In announcing the sweep's renewal, OCIE noted that it would focus on firm governance and risk assessments – including whether firms' "[cybersecurity] controls and risk assessment processes are tailored to their businesses." Continuing the trend, earlier this year, OCIE again announced a cybersecurity focus. Specifically, OCIE previewed that its 2016 examinations would include "testing and assessments of firms' implementation of procedures and controls."

Recent SEC Enforcement Activity Underscores the Risk of Template Cybersecurity Policies

Consistent with the regulatory focus on tailored cybersecurity policies and procedures, the SEC Staff has pursued penalties where it finds an industry participant's policies and procedures inadequate. Recently, in *In the Matter of Craig Scott Capital LLC* (Order), the SEC Staff alleged that an SEC-registered broker-dealer (CSC) failed to adopt written policies and procedures reasonably designed to ensure the security and confidentiality of customer records and information, in violation of Rule 30(a) of Regulation S-P (Safeguards Rule).[7]

According to the Order, from January 2012 until approximately June 2014, CSC's staff "used email addresses other than those with the Firm's domain name … to electronically receive more than 4,000 faxes from customers and other third parties." The faxes "routinely included sensitive customer records and information, such as customer names, addresses, social security numbers, bank and brokerage account numbers, copies of driver's licenses and passports, and other customer financial information." Further, the Order alleged that a number of the firm's employees, including its principals, used non-firm email accounts for matters relating to firm business.

Importantly, the Order notes that *the broker-dealer had written policies and procedures, which included a section directly addressing the Safeguards Rule*. But, critically, the SEC Staff concluded and charged that the existing policies "were not reasonably designed to protect customer records and information[.]"

As the Order describes, many of the written policies and procedures did not actually match CSC's business practices. For example, CSC utilized an eFax system, but its "Safeguards Rule Policy did not address either the eFax System or how to handle customer records and information contained in eFaxes[.]" In addition, CSC's policy provided that "customer records and information, including customer social

security numbers, may only be accessed outside of [the firm's] office by employees who received approval from CSC's 'designated information officer,' and who have installed appropriate firewalls on their devices." But the firm's policies failed to identify the "designated information officer," and "employees who accessed customer records and information remotely through personal email accounts did not install appropriate firewalls" as CSC's policies required. Similarly, while the firm's policy "required the encryption of customer records and information transmitted to laptops or other remote devices," CSC personnel failed to actually encrypt customer records and information.

The SEC Staff also cited portions of the firm's policy that lacked sufficient detail or were incomplete. For instance, the "Safeguards Rule Policy stated that the 'Designated Supervisor' was responsible for ensuring compliance with the policy [but] did not identify th[is] 'Designated Supervisor[.]'" The policy also "contained blanks" where methods for complying with the Safeguards Rule had not yet been completed.

Ultimately, the SEC Staff concluded and charged that the policies "were not tailored to the actual practices at [the firm]." The Order indicates that CSC agreed to a $100,000 penalty and to cease and desist from committing or causing any violations and any future violations of the Safeguards Rule.[8]

Conclusion

The SEC, the CFTC, and other financial regulators are devoting significant attention and resources to cyber threats. Recently, the SEC's approach to cyber regulation has given the industry real insight into regulator expectations. Registered broker-dealers and investment advisers should regularly review their cybersecurity-related risks, and the risk assessment should include a review of how the firm actually collects, transmits, stores and uses non-public personal information. Firms should then update their policies and procedures accordingly. The *Craig Scott Capital* Order highlights a regulatory risk that firms could face if they rely on "form" or outdated policies to comply with the Safeguards Rule, rather than building a program contoured to the specifics each firm may face in the course of its business.

Timothy C. Blank is a partner, and **D. Brett Kohlhofer**, and **Hilary Bonaccorsi** are associates at Dechert LLP

NOTES

1 The National Futures Association (NFA), the US derivatives industry's self-regulatory organization, adopted cybersecurity guidance for its members in late 2015. For more information, please refer to *Dechert OnPoint*, NFA Adopts Cybersecurity Guidance.

2 *See* 17 C.F.R. § 248.30(a) (Regulation S-P). The CFTC has adopted a similar general rule, which requires covered entities to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." 17 CFR § 160.30.

3 For further information, please refer to *Dechert OnPoint*, U.S. SEC Division of Investment Management Issues Cybersecurity Guidance.

4 "SEC says cyber security biggest risk to financial system," Reuters.com.

5 For further information, please refer to *Dechert OnPoint*, SEC Staff to Conduct Broker-Dealer and Investment Adviser Examinations Focused on Cybersecurity.

6 For further information, please refer to *Dechert OnPoint*, SEC Cybersecurity Examinations and Enforcement: What Broker-Dealers and Investment Advisers Need to Know.

7 *In the Matter of Craig Scott Capital LLC, Craig S. Taddonio, and Brent M. Porges*, Rel. No. EA-77595 (Apr. 12, 2016). For information regarding a similar settled SEC enforcement proceeding, *In the Matter of R.T. Jones Capital Equities Mgmt., Inc.*, Rel. No. IA-4204 (Sept. 22, 2015), please refer to *Dechert OnPoint, supra* n.6.

8 The Order also charged CSC and two of its principals individually for violations of Section 17(a) of the Securities Exchange Act of 1934.