JONES DAY

APRIL 2014

COMMENTARY

CFTC and SEC Announce Focus on Cybersecurity

Recent steps by the Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC") show that both agencies will increase their focus on cybersecurity issues going forward. The CFTC's Division of Swap Dealer and Intermediary Oversight ("DSIO") recently issued recommended best practices for securing financial information in compliance with Title V of the Gramm-Leach-Bliley Act ("GLBA").[1] Staff-Advisory 14-21 provides covered financial institutions with guidance for required administrative, technical, and physical safeguards and establishes the CFTC as an emerging player in the regulation of data security. In addition, the SEC's Office of Compliance Inspections and Examinations ("OCIE") recently announced that its 2014 Examination Priorities included a focus on cybersecurity and that it intends to examine the cybersecurity practices of more than 50 registered broker-dealers and investment advisors as part of an overall assessment of the cybersecurity preparedness of the securities industry.[2] Entities subject to the jurisdiction of the SEC or the CFTC should, in turn, expect to devote increased time and resources to cybersecurity matters.

CFTC's DSIO Best Practices

Congress enacted Title V of the GLBA in 1999 to ensure that financial institutions protect the security and confidentiality of their customers' nonpublic personal information. The CFTC was deemed a federal financial regulator with responsibility for implementing Title V with the passage of the Commodity Futures Modernization Act of 2000. Under Part 160, issued in 2001, the CFTC promulgated its first Title V privacy rules, mandating that covered entities "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." Today, covered entities include futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants.

Not surprisingly, given the daily barrage of news coverage concerning data breaches and hackings, the CFTC's DSIO wrote that "at this time … it [is] important to outline recommended best practices for covered financial institutions to comply with Title V and Part 160 of the Commission's regulations concerning security safeguards." The CFTC's DSIO advised that each covered entity develop, implement, and maintain a written

information security and privacy program that is appropriate to its size, complexity, and scope of activities. According to the CFTC's DSIO, covered entities should, "at a minimum," abide by the following best practices:

Designate an employee with privacy and security management oversight responsibilities to (i) develop strategic organizational plans for implementing controls, (ii) report directly to senior management or the board of directors, and (iii) designate employees to implement and assess the effectiveness of the program.

Identify all reasonably foreseeable risks to security, confidentiality, and integrity of personal information and related systems, both internal and external, that could result in the compromise of such information or systems; identify such risks; and establish processes and controls to assess and mitigate risks.

Design and implement safeguards to control the identified risks.

Train staff to implement the program.

Regularly test or monitor the safeguards and maintain written records of the effectiveness of the controls, including the effectiveness of:

- Controls on personal information;
- Appropriate encryption of electronic information in storage and transit;
- Controls to detect, prevent, and respond to incidents of unauthorized access to or use of personal information; and
- Employee training and supervision relating to the program.

Arrange for an independent party to test and monitor the safeguards' controls, systems, policies, and procedures at least once every two years.

Oversee third-party service providers with access to customer information to ensure they maintain safeguards.

Regularly evaluate and adjust the program in light of:

- The results of the risk assessment process;
- Relevant changes in technology and business processes;
- Any material changes to operations or business arrangements; and
- Any other circumstances that may have a material impact on the program.

Design and implement policies and procedures for responding to an incident involving unauthorized access, disclosure, or use of personal information, including policies and procedures to:

- Assess the nature and scope of any such incident;
- Take appropriate steps to contain and control the incident to prevent further unauthorized access, disclosure, or use;
- Promptly conduct a reasonable investigation to determine the likelihood that personal information has or will be misused;
- If the covered entity determines that misuse of information has occurred or is reasonably possible, then as soon as possible notify individuals whose information was or may be misused and notify the Commission (unless law enforcement requests otherwise); and
- Keep appropriate written records.

Provide the board of directors with an annual assessment of the program, including a report on any material cyber incidents.

SEC's OCIE Cybersecurity Initiative

In March, the SEC hosted a roundtable to discuss cybersecurity and the challenges facing market participants and public companies. At the roundtable, SEC Chair Mary Jo White described cyber threats as a "global threat … of extraordinary and long-term seriousness."[3]

After the roundtable, the SEC's OCIE launched a cybersecurity initiative to assess preparedness and obtain information about cyber threats from market participants. The OCIE announced that it would examine more than 50 registered broker-dealers and registered investment advisors. As part of its cybersecurity initiative, the SEC's OCIE published a detailed list of information

requests that the OCIE may use in its examinations of cybersecurity matters. Those questions borrow in part from the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity," voluntary standards for managing cyber risk to critical infrastructure released on February 12. The OCIE's sample questions cover a range of topics, including cybersecurity governance, protecting firm information, risks associated with remote customer access and funds transfer request, risk stemming from third parties, and detection of data breaches.

The OCIE's initiative is the most recent manifestation of the SEC's continued focus on cybersecurity-related issues since at least October 2011, when the SEC Division of Corporation Finance issued guidance on existing disclosure obligations related to cyber risks and data breaches to assist public companies with the disclosure of cybersecurity issues.

Takeaways

Both the CFTC and SEC exam staffs are focusing their efforts on cybersecurity. Consequently, CFTC-covered entities should begin devoting sufficient resources, including revising policies and procedures where needed, to comply with the CFTC's DSIO's best practices, including the more onerous requirements of arranging for an independent party to test and monitor safeguard controls, systems, policies, and procedures. Similarly, those facing an examination by the SEC's OCIE will need to devote substantial time and effort to respond to the wide breadth of information outlined in the sample request as part of the office's cybersecurity initiative.

Ironically, days after the announcement of the Cybersecurity Initiative, the Government Accountability Office ("GAO"), the investigative arm of Congress, found in a report that the SEC had failed to protect its own data network from intrusion, to encrypt highly sensitive data, to use strong enough passwords, or to properly monitor a contractor. While the GAO does not have the power to assess penalties against the SEC, firms dealing with the CFTC or SEC might not be so fortunate if they fail to focus on cybersecurity.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Robert W. Gaffey
New York
+1.212.326.7838
rwgaffey@jonesday.com

Joan E. McKown
Washington
+1.202.879.3647
jemckown@jonesday.com

Stephen J. Obie
New York
+1.212.326.3773
sobie@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Bart Green and Zachary M. Werner of the New York Office assisted in the preparation of this Commentary.

Endnotes

1 Division of Swap Dealer and Intermediary Oversight, "Gramm-Leach-Bliley Act Security Safeguards" (Feb. 26, 2014), *available at* www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

2 Office of Compliance Inspections and Examinations, "OCIE Cybersecurity Initiative" (April 15, 2014), *available at* www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

3 Chair Mary Jo White, "Opening Statement at SEC Roundtable on Cybersecurity" (March 26, 2014), *available at* www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.