STRADLEY RONON ATTORNEYS AT LAW

Adviser Alert

A Publication of the Stradley Ronon
Investment Management Group

WWW.STRADLEY.COM

APRIL 2014

Stradley Ronon Stevens & Young, LLP
2005 Market Street, Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
Malvern, Pa.
Harrisburg, Pa.
Wilmington, Del.
Cherry Hill, N.J.
New York, N.Y.

LAW FIRMS WORLDWIDE MERITAS

www.meritas.org

Our firm is a member of Meritas – a worldwide business alliance of more than 210 law offices in 70 countries, offering high-quality legal services through a closely integrated group of independent, full-service law firms.

Takeaways From the Recent SEC Cybersecurity Roundtable

By Kenneth L. Greenberg

In our first cybersecurity alert (see http://www.stradley.com/newsletters.php?action=view&id=911), we discussed the focus for 2014 on cybersecurity by the Securities and Exchange Commission's National Exam Program and how investment advisers and investment companies can prepare for that regulatory focus. In this cybersecurity update, we discuss some interesting points that were made at the cybersecurity roundtable hosted by the SEC on March 26.

The cybersecurity roundtable's agenda consisted of four topics: cybersecurity landscape; public company disclosure; market systems; and broker-dealers, investment advisers and transfer agents.

The roundtable focused on three broad themes: data protection, market integrity and disclosure of risks, and in that regard the SEC noted some of its recent activities regarding each of these themes. With regard to data protection, last year the SEC adopted Regulation S-ID: Identity Theft Red Flags,[1] which built upon existing regulations for protecting customer data. With regard to market integrity, the SEC in 2013 proposed Regulation SCI, which would require certain self-regulatory organizations (including registered clearing agencies), alternative trading systems, plan processors and exempt clearing agencies subject to the SEC's automation review policy to establish written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and that they operate in the manner intended.[2] With regard to disclosure of risks, in October 2011, the SEC's Division of Corporation Finance published guidance regarding disclosure obligations relating to cybersecurity risks and incidents.[3] The SEC commissioners and staff were particularly interested in gaining input regarding the SEC's role in combating cybersecurity threats.

The following are some of the more interesting discussion points of the cybersecurity roundtable:

Cybersecurity Threats to Financial Services Companies:

- Compared to other industries, financial services companies are relatively advanced in addressing cybersecurity issues and have sophisticated defenses. Unfortunately, they are also prime targets of cybersecurity bad actors because, as bank robber Willie Sutton used to say, "That's where the money is."

- Threat vectors of financial services companies include (1) nation-states or terrorists seeking ways to disrupt the United States market system (e.g., denial-of-service attacks or destruction of data); (2) espionage by state or nonstate actors seeking ways to steal proprietary information; (3) organized crime seeking ways to steal

Information contained in this publication should not be construed as legal advice or opinion or as a substitute for the advice of counsel. The enclosed materials may have been abridged from other sources. They are provided for educational and informational purposes for the use of clients and others who may be interested in the subject matter.

Copyright © 2014
Stradley Ronon Stevens & Young, LLP
All rights reserved.

financial information in order to steal money from an account holder through identity theft or account takeover; (4) hacktivists seeking to promote an ideological agenda by disrupting computer systems; and (5) insiders – rogue employees who steal information for personal benefit or careless employees who leave security systems vulnerable (e.g., due to weak passwords or lost laptops).

- Cybersecurity threats include the following:
  - **Malware/Spyware** – Installation of malicious code using removable media (e.g., USB flash drive) or email.
  - **Ransomware** – Installation of malicious code that encrypts data and is used to extort money from a company that needs to have such data returned unencrypted.
  - **Hacking** – Exploitation of weak computer security systems, especially weak passwords.
  - **Spoofing** – Masquerading a malicious website as a legitimate website in an attempt to steal private information that can be used for identity theft.
  - **Phishing** – Sending an email that falsely claims to be from a legitimate enterprise in an attempt to steal private information that can be used for identity theft.
  - **Denial-of-Service Attacks** – Flooding a computer network with useless traffic to disrupt website operations.
  - **Loss/Theft** – The loss or theft of mobile computer devices, such as laptops and smartphones, or compact disks or flash drives that contain personally identifiable information of customers or company proprietary data.
  - Cybersecurity threats are constantly changing, which makes it difficult to monitor potential patterns of threats.
- Bad actors are constantly looking for computer system vulnerabilities. Some attacks are opportunistic, "drive by" attacks where a firm may not have been specifically targeted, but a vulnerability was discovered and immediately exploited by theft of information. Other attacks involve a firm being specifically targeted and subject to a patient and persistent attack. In some cases, a system may be breached but not immediately exploited by data theft. An in-depth forensic computer investigation may be needed to discover what the hacker is doing in a company's computer system.

Cybersecurity Challenges for Financial Services Companies:

- Determining what information needs to be protected.
- Understanding how information travels and the risks related to that travel, particularly if information leaves your company.
- Managing access to information, including access by both employees and third-party vendors.
- Figuring out what needs to be monitored.
- Sharing information – There is no clear guidance as to what can be shared between companies and between companies and government.
- Dealing with multiple regulators and government agencies. There is a tension between the regulatory desire to notify various parties (e.g., regulators, clients, service providers) and the need to keep information secret to assist law enforcement.
- Timing of investigation versus notification. Investigating a data security breach can be a time-consuming process, but there is pressure to quickly notify victims. Balancing the investigative needs for law enforcement and the need for notifying victims so that they can protect themselves is a challenge.
- Receiving timely and actionable information of potential cyberthreats.
- Improving communication between IT staff and senior management.
- Ensuring that sufficient resources and personnel are devoted to cybersecurity (especially for small and medium-sized companies).

Corporate Governance and Cybersecurity:

- Firms should have a culture of cybersecurity. Cybersecurity is not just a technology issue for IT staff to deal with but starts at every employee's keyboard and ends with senior management and the board.
- Increasingly, boards of directors have also become involved and often consider cybersecurity issues through their audit committee or risk committee.

© 2014 Stradley Ronon Stevens & Young, LLP

However, it is not well-established what, when and how cybersecurity issues should be reported.

- Cybersecurity involves risk management. There is no magic software purchase that will solve all problems. Cybersecurity involves constant monitoring and risk mitigation (e.g., discovering security gaps and closing them). Technology moves faster than security countermeasures.

Disclosure Issues Involving Cybersecurity:

- A tension exists in the Division of Corporation Finance's Cybersecurity Guidance regarding the need to avoid generic boilerplate disclosure and to provide risk disclosure that is meaningful to shareholders and that is tailored to a particular company. Disclosure tends to be more generic, because companies want to avoid providing details that may compromise their own cybersecurity.

- While the Division of Corporation Finance's Cybersecurity Guidance requests disclosure of material cybersecurity incidents, one participant suggested that disclosure was driven more by the requirements of state data breach notification laws and that actual disclosure of incidents relate primarily to those in which state law required disclosure. Other cybersecurity incidents that did not trigger state data breach notification laws because they did not involve personally identifiable information (e.g., proprietary data) may ultimately be considered to be immaterial and therefore require no disclosure.

Best Practices:

- Computer security policies and procedures need to be in place, constantly reviewed for gaps and updated to reflect new developments. Firms need a defense in depth.

- Firms must develop and implement a data breach security response policy and consider holding a data breach exercise.

- Cybersecurity is an enterprisewide concern involving all employees and senior management.

Possible Recommendations Regarding the Role of the SEC:

- Provide clarification about what information can be shared among companies and among regulators and law enforcement agencies and who should receive such information.

If you would like more information, contact Kenneth L. Greenberg at kgreenberg@stradley.com or 215.564.8149.

- Provide legal protection for information sharing.

- Provide information about cybersecurity best practices.

- Coordination among regulators in developing uniform approaches to cybersecurity regulations and review of cybersecurity policies and procedures.

- Provide principle-based guidance instead of prescriptive regulations that may become quickly outdated.

Public Input on Cybersecurity:

Members of the public are welcome to submit comments on the topics that were addressed at the roundtable. Comments may be submitted either electronically or on paper. Any comments submitted will become part of the public record of the roundtable and posted on the SEC's website.

- Electronic submissions: Use the SEC's Internet submissions form or send an email to rule-comments@sec.gov.

- Paper submissions: Send paper submissions in triplicate to the Office of the Secretary, Securities and Exchange Commission, 100 F Street N.E., Washington, D.C. 20549-1090.

All submissions should refer to File Number 4-673, and the file number should be included on the subject line if email is used. ▪

---

[1] *Identity Theft Red Flags Rules*, Release Nos. 34-69359, IA-3582, IC-30456, (April 10, 2013).

[2] *Regulation Systems Compliance and Integrity*, Release No. 34-69077, (March 8, 2013).

[3] *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, SEC Division of Corporation Finance, (Oct. 13, 2011).

Stradley Ronon's Investment Management Group

ATTORNEYS

Bruce G. Leto, Chair .....bleto@stradley.com.....215.564.8115
John M. Baker .....jbaker@stradley.com.....202.419.8413
Fabio Battaglia III .....fbattaglia@stradley.com 215.564.8077
Shanna B. Bayer .....sbayer@stradley.com 202.507.6406
E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Joan E. Boros.....jboros@stradley.com 202.507.6413
Emily Taylor Brody .....ebrody@stradley.com 215.564.8071
Jessica Burt .....jburt@stradley.com.....202.419.8409
Anthony V. Coletta Jr. .....acoletta@stradley.com 215.564.8154
Joel D. Corriero .....jcorriero@stradley.com.....215.564.8528
Jana L. Cresswell.....jcresswell@stradley.com.....215.564.8048
Brian Crowell .....bcrowell@stradley.com.....215.564.8082
Matthew R. DiClemente .....mdiclemente@stradley.com 215.564.8173
Lisa A. Duda .....lduda@stradley.com 215.564.8143
Ruth S. Epstein .....repstein@stradley.com 202.292.4522
J. Stephen Feinour Jr. .....jfeinourjr@stradley.com 215.564.8521
Amy C. Fitzsimmons .....afitzsimmons@stradley.com....215.564.8711
Alison M. Fuller .....afuller@stradley.com 202.419.8412
Robert K. Fulton .....rfulton@stradley.com 215.564.8042
Alan R. Gedrich.....agedrich@stradley.com.....215.564.8050
Jamie M. Gershkow.....jgershkow@stradley.com 215.564.8543
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Cory O. Hippler.....chippler@stradley.com 215.564.8089
Peter M. Hong .....phong@stradley.com.....202.419.8429
Nathan M. Iacovino .....niacovino@stradley.com.....215.564.8164
Kristin H. Ives .....kives@stradley.com 215.564.8037
John Y. Kim .....jkim@stradley.com.....215.564.8020
Lisa M. King .....lking@stradley.com 215.564.8733
Jonathan M. Kopcsik.....jkopcsik@stradley.com.....215.564.8099
Mena Ryley Larmour.....mlarmour@stradley.com.....215.564.8014
Cillian M. Lynch .....clynch@stradley.com 202.419.8416
Michael D. Mabry .....mmabry@stradley.com 215.564.8011
Prufesh R. Modhera.....pmodhera@stradley.com.....202.419.8417
Michael W. Mundt.....mmundt@stradley.com 202.419.8403
Molly O'Brien .....mobrien@stradley.com 202.292.4527
Michael P. O'Hare .....mohare@stradley.com.....215.564.8198
David F. Roeber.....droeber@stradley.com 215.564.8179
Mark A. Sheehan .....msheehan@stradley.com.....215.564.8027
Joshua N. Silverstein .....jsilverstein@stradley.com 856.321.2416
Nicole Simon .....nsimon@stradley.com.....215.564.8001
Amy G. Smith .....asmith@stradley.com 215.564.8104
Lawrence P. Stadulis .....lstadulis@stradley.com 202.419.8407
Merrill R. Steiner.....msteiner@stradley.com.....215.564.8039
John L. Sullivan .....jsullivan@stradley.com.....202.292.4524
Joan Ohlbaum Swirsky .....jswirsky@stradley.com 215.564.8015
Angela N. Velez.....avelez@stradley.com 215.564.8691
Christopher J. Zimmerman ....czimmerman@stradley.com 202.419.8402

IMG PRACTICE GROUP ADMINISTRATOR

Sinclair A. Ziesing.....sziesing@stradley.com 215.564.8055

LEGAL ASSISTANTS

Katherine Bennett .....kbennett@stradley.com.....202.507.6407
Robert Dillon .....rdillon@stradley.com.....215.564.8649
Dawn E. Mac Donald .....dmacdonald@stradley.com 408.241.1770
Kristopher R. Pietrzykowski ....kpietrzykowski@stradley.com..215.564.8114
Maximillian Schultz .....mschultz@stradley.com 202.419.8411

FUND TAXATION

ATTORNEYS

Zachary P. Alexander.....zalexander@stradley.com 215.564.8043
David J. Karasko .....dkarasko@stradley.com 215.564.8542
Kristin M. McKenna .....kmckenna@stradley.com 215.564.8176
William S. Pilling III .....wpilling@stradley.com 215.564.8079
Christopher C. Scarpa .....cscarpa@stradley.com.....215.564.8106

FUND ENFORCEMENT AND LITIGATION

ATTORNEYS

Steven B. Davis .....sdavis@stradley.com.....215.564.8714
Gregory D. DiMeglio .....gdimeglio@stradley.com 202.419.8401
Keith R. Dutill .....kdutill@stradley.com 610.640.5809
Zachary T. Knepper .....zknepper@stradley.com 202.419.8414
David C. Franceski Jr. .....dfranceski@stradley.com 215.564.8062
Paula D. Shaffner.....pshaffner@stradley.com 215.564.8761
Rachel Tausend .....rtausend@stradley.com 202.419.8405

EXCHANGE-TRADED FUNDS (ETFs)

ATTORNEYS

Fabio Battaglia III .....fbattaglia@stradley.com 215.564.8077
E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Matthew R. DiClemente ....mdiclemente@stradley.com 215.564.8173
Lisa A. Duda .....lduda@stradley.com 215.564.8143
J. Stephen Feinour Jr. .....jfeinourjr@stradley.com 215.564.8521
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Bruce G. Leto .....bleto@stradley.com.....215.564.8115
Michael D. Mabry .....mmabry@stradley.com 215.564.8011
Michael W. Mundt .....mmundt@stradley.com 202.419.8403

CFTC ISSUES

ATTORNEYS

Ruth S. Epstein .....repstein@stradley.com 202.292.4522
Kenneth L. Greenberg .....kgreenberg@stradley.com....215.564.8149
Peter M. Hong .....phong@stradley.com.....202.419.8429
Kevin P. Kundra.....kkundra@stradley.com 215.564.8183
Merrill R. Steiner.....msteiner@stradley.com.....215.564.8039

ERISA

ATTORNEY

James F. Podheiser.....jpodheiser@stradley.com 215.564.8111

FUND BANKING ISSUES

ATTORNEY

Christopher S. Connell .....cconnell@stradley.com.....215.564.8138

ISDA/STRUCTURED FINANCE MATTERS

ATTORNEYS

E. Carolan Berkley .....ecberkley@stradley.com 215.564.8018
Deborah Hong .....dhong@stradley.com.....610.640.5818
Kevin P. Kundra.....kkundra@stradley.com 215.564.8183

© 2014 Stradley Ronon Stevens & Young, LLP