The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 26, NO. 9 • SEPTEMBER 2019

The SEC's Regulation S-P in the Age of Cybersecurity

By Jeffrey Taft, Matthew Bisanz, and Leslie Cruz

Cybersecurity worries regularly lead the news and the boardroom agenda as a major part of the zeitgeist of our time. A single cybersecurity incident can move markets, end careers, or prompt litigation. In this age of cybersecurity, financial institutions have rapidly realized the importance of maintaining robust defenses to protect both customers and the institution from bad actors, whether internal or external.

Reflecting the piecemeal nature of financial services regulation in the United States, federal and state regulators have begun jockeying for position by adapting existing regulations to cybersecurity concerns and by breaking ground with new cybersecurity regulations. Each regulator has taken its own path with respect to the institutions it regulates, and no one approach has become dominant.

For investment advisers registered under the Investment Advisers Act of 1940 (RIAs), the US Securities and Exchange Commission (SEC) is the primary functional regulator.[1] So far, the SEC has taken a path of adapting existing requirements in Regulation S-P to address cybersecurity concerns through the issuance of guidance and enforcement actions.[2]

This article provides an overview of Regulation S-P, discusses how the SEC has interpreted Regulation S-P to address cybersecurity and certain SEC and FINRA enforcement activities, reviews cybersecurity initiatives undertaken by other regulators and organizations, and offers concluding remarks that may help RIAs with a path forward.[3] Throughout we discuss considerations and takeaways for developing and evaluating cybersecurity compliance for RIAs.

History of Regulation S-P

The Gramm-Leach-Bliley Act (GLBA) was passed in 1999 to modernize the regulation of financial services.[4] In relevant part, Title V of the GLBA governs how financial institutions may use the nonpublic personal information (NPI) of a customer or consumer.[5] Specifically, the GLBA imposes on financial institutions "an affirmative and continuing obligation … to protect the security and confidentiality of [their] customers' nonpublic personal information" and contains the substantive protection requirements that financial institutions must satisfy.[6]

Multiple regulators were assigned responsibility for implementing the provisions of Title V within their respective areas of functional regulation. Accordingly, the SEC was assigned rulemaking and enforcement responsibility for the information protection and privacy provisions of Title V with respect to RIAs, broker-dealers, and mutual funds (Registered Entities). In 2000, the

SEC adopted Regulation S-P to implement those provisions.[7]

Safeguards Rulemaking

Under the information protection provision of Regulation S-P (Safeguards Rule), a Registered Entity is required to adopt "written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." These written policies and procedures (Safeguarding Procedures) must be reasonably designed to:

1. Ensure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[8]

It is important to note that since the GLBA was enacted in 1999 and Regulation S-P was first adopted in 2000, information privacy and protection concerns have risen in importance, particularly given the increased cybersecurity risks since that time. When Regulation S-P was first adopted, many Safeguarding Procedures focused primarily on administrative and physical safeguards, and to a lesser extent on technical safeguards, reflecting the then-current state of technology used by Registered Entities. Now, the use of technology by Registered Entities has increased not only in scope (with daily operations heavily dependent on technology) but also in complexity. Some Safeguarding Procedures have evolved appropriately over time, but as the SEC's and others' actions discussed below reflect, certainly not all of them have done so, particularly with respect to technical safeguards and breach response.

Unadopted Amendments to the Safeguards Rule

In 2008, the SEC proposed amendments to the Safeguards Rule that would have "set forth more specific requirements for safeguarding information and responding to information security breaches, and broaden[ed] the scope of the information covered by Regulation S-P's safeguarding and disposal provisions."[9] The proposal was driven by concerns regarding information security breaches and the proposed amendments would have broadly required Registered Entities to implement Safeguarding Procedures, including breach notification protocols, similar to those required for banks.

Under the proposed amendments, Registered Entities would have been required to:

1. Designate in writing an employee or employees to coordinate the information security program;
2. Identify in writing reasonably foreseeable security risks that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of personal information or personal information systems;
3. Design and document in writing and implement information safeguards to control the identified risks;
4. Regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of access controls on personal information systems, controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons, and employee training and supervision;
5. Train staff to implement the information security program;
6. Oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain

appropriate safeguards (and document such oversight in writing); and
7. Evaluate and adjust their information security programs to reflect the results of testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the institution knows or reasonably believes may have a material impact on the program.

The proposed amendments were never adopted by the SEC and have not been publicly cited by SEC Staff in subsequent guidance or, indirectly, in enforcement actions.[10] However, some in the investment management industry see the proposed amendments and the safeguarding requirements for banks (on which the proposed amendments were based) as a model for RIAs.

Recent SEC Actions Related to Cybersecurity

In this section, we discuss certain SEC guidance and enforcement actions related to the Safeguards Rule and cybersecurity. As mentioned above, the Safeguards Rule was adopted in 2000. It wasn't until 2007, however, that the SEC first publicly-addressed that rule by initiating enforcement actions against a dual-registered RIA/broker-dealer and another broker-dealer for alleged violations of the Safeguards Rule.[11]

In April 2014, the SEC announced the first cybersecurity sweep examinations initiative, with another following in September 2015 and the third announced in March 2019.[12] The cybersecurity sweeps have resulted in a number of risk alerts and other forms of guidance over the years, with cybersecurity being cited as an SEC examination priority since at least 2013.[13]

These activities, which are discussed in more detail below in reverse chronological order, reflect the SEC's growing concerns over cybersecurity and its use of the Safeguards Rule as the legal basis for imposing cybersecurity standards on RIAs.

SEC Guidance

May 2019 Network Storage Risk Alert

Most recently, on May 23, 2019, the SEC's Office of Compliance Inspections and Examinations (OCIE) published a risk alert describing Safeguards Rule issues that are associated with the storage of electronic customer records and information in network storage solutions (for example, cloud-based storage) that OCIE Staff had identified in recent examinations of RIAs and broker-dealers.[14]

In the May 2019 risk alert, OCIE identified the following three categories of common concerns related to network storage solutions:

1. **Misconfigured Solutions**: OCIE Staff observed registrants that had not adequately configured the security settings on their network storage solution to protect against unauthorized access. In addition, some registrants did not have policies and procedures addressing the security configuration of their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.
2. **Inadequate Oversight**: OCIE Staff observed registrants that had not ensured that the security settings on vendor-provided network storage solutions were configured in accordance with the registrant's standards.
3. **Insufficient Data Classification**: OCIE Staff observed registrants that had policies and procedures that did not identify the different types of data stored electronically by the registrant and the appropriate controls for each type of data.

In light of this alert, RIAs should review their unauthorized access/security configuration controls (including security settings for third-party storage solutions), enhance them as needed, and incorporate the same into their Safeguarding Procedures. RIAs also should consider implementing

information classification programs and/or conducting an inventory of their electronically-stored information.

April 2019 Regulation S-P Risk Alert

On April 16, 2019, OCIE published a risk alert describing customer information safeguarding issues that OCIE Staff had identified in recent examinations of RIAs and broker-dealers.[15] With respect to Safeguarding Procedures, OCIE described the following common exam deficiencies:

1. **Lack of Regulation S-P Policies and Procedures**: OCIE Staff observed registrants that did not have any Safeguarding Procedures as required under the Safeguards Rule or had procedures that merely stated the text of the Safeguards Rule but failed to tailor that document to the firm's actual compliance activities, or consisted of template versions of Regulation S-P policies and procedures that had blank spaces for the firm's terms and practices.
2. **Deficient Policies and Procedures Related to the Safeguards Rule**: In addition, OCIE Staff observed that certain registrants had written policies and procedures that did not appear to be implemented or reasonably designed to satisfy the three main elements of the Safeguards Rule (that is, insuring security and confidentiality, protecting against anticipated threats and hazards, and protecting against unauthorized access or use). For example, OCIE noted that some policies and procedures did not address:
   - Employees' use of personal devices for business purposes (in particular, employees safeguarding customers' personally identifiable information (PII) on their personal devices such as home laptops);
   - Training employees on the firm's safeguarding requirements and monitoring whether such requirements were being followed;
   - The use of outside vendors (such as requiring outside vendors to comply with the firm's safeguarding policies in connection with customer PII);
   - Cataloging firm systems that maintain customer PII;
   - Maintaining incident response plans that address cybersecurity threats and assess firm system vulnerabilities;
   - The security of the storage of customer PII in physical locations (for example, in locked file cabinets);
   - System access (including, but not limited to, the process for granting access rights to appropriate employees and procedures for revoking system access for departing employees); and
   - Other considerations for electronic communications and networks (such as email encryption and securing networks that have customer PII).

RIAs should review their Safeguarding Procedures, and their implementation, to ensure that they are tailored to appropriately comply with the Safeguards Rule as outlined above. Furthermore, RIAs should regularly monitor, evaluate, and adjust their information safeguarding and incident response programs in light of any relevant changes in (i) technology, (ii) the sensitivity of customer information, (iii) internal or external threats to information, and (iv) their own businesses arrangements or practices (for example, new mergers, joint ventures, and outsourcing arrangements and changes to information systems).

2019 OCIE Examination Priorities

On December 20, 2018, OCIE released its 2019 priorities for examinations of RIAs and broker-dealers.[16] As in past years, the 2019 priorities include cybersecurity. The 2019 priorities state that OCIE will focus on how RIAs configure network storage devices, and on information security governance generally, as well as on policies and procedures related to retail trading information security. In addition, OCIE will emphasize cybersecurity practices of RIAs

with multiple branch offices, including those that have recently merged with other investment advisers. Further, OCIE will focus on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. This examination focus is reflected in the above OCIE risk alerts.

In light of this examination priority, RIAs should review their Safeguarding Procedures to evaluate whether they adequately address cybersecurity events (that is, breaches) not only at the RIA's main offices but also at any applicable branch office. RIAs also might consider having a periodic audit of their Safeguarding Procedures, conducting penetration tests and vulnerability scans on critical systems and making sure they have customized and up-to-date response plans in place for addressing cybersecurity incidents and data breaches.

August 2017 Cybersecurity Sweep Examinations Risk Alert

On August 7, 2017, OCIE issued a risk alert which had been announced in September 2015 and provided a summary of its observations from the cybersecurity sweep examinations of 75 RIAs and broker-dealers.[17] OCIE identified the following three areas where compliance and oversight could be improved:

1. **Safeguarding Procedures**: OCIE Staff observed that Safeguarding Procedures were not reasonably tailored because they provided employees with only general guidance and only identified limited examples of safeguards for employees to consider.
2. **Compliance and Enforcement**: OCIE Staff observed that some registrants did not appear to adhere to or enforce their Safeguarding Procedures, or the Safeguarding Procedures did not reflect the firms' actual practices.
3. **Other Related Issues**: OCIE Staff observed that some registrants did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities and other operational safeguards to protect customer records and information.

OCIE also identified six takeaways that RIAs (and broker-dealers) should consider implementing as part of their Safeguarding Procedures:

1. **Maintenance of an inventory of data, information, and vendors**: A complete inventory of data and information and classification of the related risks and vulnerabilities.
2. **Detailed policies and procedures for penetration testing, security monitoring, system auditing, access rights, and data breach reporting**: Specific documentation addressing the scope, methodology, timing and responsible parties for an entity's cybersecurity activities.
3. **Maintenance of schedules and processes for activities such as vulnerability scanning and patch management**: Defined schedules and prioritization for activities related to testing and risk-assessing patches and identifying system vulnerabilities.
4. **Effective access controls and access monitoring**: Implementation of acceptable use and mobile device policies, review of third-party vendor logs, and very prompt termination of former employee systems access.
5. **Mandatory enterprise-wide information security training**: Training covering all employees at on-boarding and periodically thereafter.
6. **Engagement of senior management in the review and approval of cyber-related policies and procedures**.

RIAs should review these takeaways from OCIE and consider where enhancements to their Safeguarding Procedures and related policies and controls may be warranted.

May 2017 Ransomware Risk Alert

On May 17, 2017, OCIE published a risk alert describing cyber preparedness issues that

OCIE Staff had identified in recent examinations of Registered Entities in light of a recent widespread ransomware attack that had disabled numerous organizations' access to their systems.[18] In the risk alert, OCIE identified the following three categories of deficiencies related to cyber preparedness:

1. **Cyber-Risk Assessment:** OCIE Staff observed registrants that did not conduct periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences.
2. **Penetration Tests:** OCIE Staff observed registrants that did not conduct penetration tests and vulnerability scans on systems that the registrants considered to be critical.
3. **System Maintenance:** OCIE Staff observed registrants that had a significant number of critical and high-risk security patches that were missing important updates.

In light of this alert, RIAs should plan to address ransomware and related cybersecurity threats as part of their ongoing compliance activities, including by building risk assessments, penetration testing, and regular systems maintenance into their Safeguarding Procedures.

April 2015 IM Cybersecurity Guidance Update

In April 2015, the SEC's Division of Investment Management (IM) published a guidance update describing a number of measures and strategies that RIAs should consider when addressing cybersecurity risk.[19] Interestingly, IM Staff did not mention the Safeguards Rule in this update. However, it includes recommendations that RIAs should consider incorporating into their Safeguarding Procedures.

The 2015 guidance includes recommendations that RIAs: (i) conduct periodic assessments of their cybersecurity capabilities; (ii) create strategies to detect and respond to cybersecurity threats; and (iii) implement the strategies through written policies, procedures, and training.

Further, in the IM Staff's view, RIAs should conduct a periodic assessment of: (i) the nature, sensitivity, and location of information that the firm collects, processes and/or stores, and the technology systems it uses; (ii) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems; (iii) security controls and processes currently in place; (iv) the impact should the information or technology systems become compromised; and (v) the effectiveness of the governance structure for the management of cybersecurity risk.

After identifying potential cybersecurity threats and vulnerabilities, the IM Staff recommended that RIAs create a strategy designed to prevent, detect, and respond to cybersecurity threats. And finally, RIAs should implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measurers to prevent, detect, and respond to such threats and that monitor compliance with cybersecurity policies and procedures.

February 2015 Cybersecurity Sweep Examinations Risk Alert

On February 3, 2015, OCIE issued a risk alert that provided a summary of its observations from the cybersecurity sweep examinations of 106 RIAs and broker-dealers, which was announced in April 2014.[20] The examinations, which included both review of written policies and procedures regarding cybersecurity and interviews with key personnel, provided Staff with a better understanding of how registrants "address legal, regulatory, and compliance issues associated with cybersecurity." The February 2015 risk alert did not identify deficiencies in cybersecurity practices but, rather, reported statistical information on the prevalence or absence of certain practices at registrants (for example, a majority of registrants had experienced cyber-attacks). The February 2015 alert influenced the development of the 2015 guidance, discussed above.

SEC and FINRA Enforcement Actions

2018 Dual-Registrant Safeguards Rule Enforcement Action

On September 26, 2018, the SEC announced that it had brought and settled charges against a dual-registered RIA and broker-dealer for violations of the Safeguards Rule and Regulation S-ID.[21] The SEC concluded that, although the firm had adopted certain policies and procedures, it failed to (i) ensure the reasonable design and proper operation of its policies and procedures for safeguarding confidential customer information, in violation of Regulation S-P, (ii) reasonably respond to identity theft red flags, in violation of Regulation S-ID and (iii) update and train employees and contractors on its identity theft prevention program, in violation of Regulation S-ID.

As alleged in the SEC's order, weaknesses in the firm's policies and procedures allowed cyber intruders to gain access to the personal information of 5,600 customers. For example, the firm required contractors to establish security questions on a portal as a form of multi-factor authentication. However, the portal wiped, or deleted, previously setup questions when a call center performed a password reset and provided a temporary password to a contractor by phone. This allowed a bad actor to defeat the multi-factor authentication by having the call center perform a password reset on the targeted account. Similarly, while the firm kept a list of phone numbers that were suspected of having been used in connection with fraudulent activity, it did not have a written policy or procedure requiring call center employees to refer to the list when responding to contractor calls, and an informal, unwritten procedure for doing so was not consistently applied. Additionally, while the firm's program required IT security staff to disable potentially compromised accounts, the firm had not trained its IT security staff to understand that changing or resetting a user's password would not terminate existing sessions. After the compromise had been identified, this weakness allowed unknown intruders to continue to access the firm's systems by simply staying logged into the system.

The firm subsequently blocked the unknown intruders' IP addresses, revised its policies to prohibit providing temporary passwords by phone, provided breach notices and free credit monitoring to affected customers, and implemented effective multi-factor authentication for the access portal. However, the incident and related violations were detected by OCIE Staff during a routine exam, and the firm agreed to be censured, pay a $1 million penalty, and retain an independent consultant to evaluate its policies and procedures.

Given the foregoing, RIAs should frequently update their policies and train employees (and independent contractors, if applicable) to ensure that security controls and escalation policies set forth in their Safeguarding Procedures and their overall identity theft prevention program are operating as expected. Employees are often the first line of defense against cybersecurity attacks and need appropriate training and retraining to ensure that they are prepared to properly identify incidents and respond to them.

2017 FINRA Safeguards Rule Action

On September 28, 2017, FINRA sanctioned a dual-registered broker-dealer and state-registered investment adviser (State IA) under Regulation S-P for failing to establish, maintain, and enforce a supervisory system that was reasonably designed to ensure the security of electronically stored confidential customer information and failing to oversee, supervise, and monitor third-party vendors involved with its public Web site.[22] The firm's alleged failures resulted in a seven-day period where the nonpublic information of over 700 customers was accessible to anyone who had access to the firm's Web site. For these violations, the firm was censured and fined in the amount of $50,000.

As discussed above with respect to the May 2019 network storage risk alert, RIAs should implement robust vendor risk management programs to harden virtual services against attacks and prevent

information leaks through improperly configured services.

2016 SEC Safeguards Rule Enforcement Action

On June 8, 2016, the SEC brought and settled charges against a dual-registered RIA and broker-dealer for failure to implement reasonable Safeguarding Procedures as required by the Safeguards Rule.[23] As alleged in the order, the firm maintained hundreds of computer applications to process NPI contained in its customer databases, two of which permitted any employee to access any customer's PII by entering certain number combinations that represented internal business units (other than the employee's own unit). The authorization modules for these two applications remained in place from at least August 2001 until December 2014 and were not audited, tested, or regularly updated during that period. As a result, an employee allegedly was able to run over 5,000 unauthorized searches between 2011 and 2014 and to download PII associated with 730,000 customer accounts. Other controls failed to prevent the employee from establishing a file transfer connection over the Internet between his work computer and his personal server and transferring customer account data to his personal server.

Following the exfiltration of the data, third-party hackers separately compromised the employee's personal server and began to sell the customer account data online. The firm detected these sales during Internet sweeps and identified the employee as the source of the information.

As a result of the settled proceeding, the firm was ordered to cease and desist from further violations of the Safeguards Rule, censured, and fined $1,000,000. Separately, the firm notified customers whose data had been compromised. The employee was banned from the securities industry by the SEC and, in a related criminal case, pled guilty to the felony of exceeding authorized access to a computer and was sentenced to 36 months of probation and ordered to pay $600,000 in restitution to the firm. Moreover, the Federal Reserve Bank of New York notified the employee that, because his conviction involved "dishonesty or breach of trust," he was automatically subject to a statutory ban from the business of banking.

While RIAs can always adopt more robust risk management programs and perform routine auditing, testing, and monitoring, this action highlights that they also should consider adopting effective automated security mechanisms (for example, filters to block "uncategorized" Web sites and effective "authorization modules").

Certain Privacy and Cybersecurity Initiatives by Other Regulators and Organizations

Approach by Federal Banking Regulators

The GLBA assigned the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation (collectively, the federal banking regulators) rulemaking and enforcement responsibility for the information protection provisions of Title V with respect to insured depository institutions and their affiliates that are not regulated by the SEC, CFTC, or state insurance regulators (collectively, banks).

The federal banking regulators adopted guidelines in 2001 to implement the safeguarding provisions of Title V of the GLBA with respect to banks.[24] These guidelines were amended in 2005 to add expectations for incident response and breach notification.[25] The guidelines generally are considered to be the most detailed and comprehensive implementation of the safeguarding provisions of the GLBA.[26]

For RIAs affiliated with banks, it often is efficient for the RIA to adopt and comply with the safeguarding rules for banks. Many financial services organizations (for example, bank holding company groups) have implemented enterprise-wide risk management systems that follow the "lowest common denominator" approach. For RIAs in such groups, the bank requirements described above will often be applied

enterprise-wide because they are the most comprehensive set of US data protection obligations.

Even RIAs that are not affiliated with banks might consider designing their Safeguarding Procedures to comply with the safeguarding rules for banks, particularly with respect to incident response and breach notification. While those rules may be more burdensome than the SEC's Safeguards Rule, they can provide a detailed, comprehensive roadmap to compliance and have been widely adopted in the financial services sector.

Colorado and Vermont Regulations

State regulators in Colorado and Vermont have adopted cybersecurity rules that apply to broker-dealers and investment advisers registered in those states.[27] The Colorado Division of Securities adopted cybersecurity rules under the Colorado Securities Act that require registrants to adopt written procedures that are reasonably designed to ensure cybersecurity and to conduct annual risk assessments of data security practices.[28] The Vermont Securities Division adopted cybersecurity rules (Vermont Regulation) that apply to "securities professionals," which include: broker-dealers, agents, State IAs, investment adviser representatives, solicitors, and third-party portals.[29] Under the Vermont Regulation, securities professionals are required to (i) establish and maintain written procedures reasonably designed to ensure cybersecurity, (ii) include cybersecurity as part of its risk assessment, (iii) maintain evidence of adequate insurance for the risk of a cybersecurity breach, and (iv) provide identity restoration services at no cost to consumers in the occurrence of a breach in the cybersecurity of consumer nonpublic personal information.

RIAs should make sure that cybersecurity is part of the chief compliance officer's overall compliance risk assessment and is evaluated in connection with the annual compliance review. RIAs also may want to consider whether it is appropriate, based on the nature of their businesses, to purchase cyber insurance or acquire prepaid identity restoration services for data breaches.

NYDFS Cybersecurity Regulation (including NAIC Model Law and FTC Proposal)

On February 16, 2017, the New York State Department of Financial Services (NYDFS) finalized regulations (NY Regulations) that mandate cybersecurity standards for all institutions authorized by NYDFS to operate in New York (NY Covered Entities), including many banks, insurance entities, and insurance professionals doing business in New York.[30] The NY Regulations apply to any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the New York Banking, Insurance, or Financial Services Laws. The NY Regulations generally do not apply to RIAs, State IAs, or broker-dealers, which are regulated by the SEC and/or New York Attorney General.

Under the NY Regulations, a NY Covered Entity is required to maintain a written cybersecurity policy or policies and implement a risk-based cybersecurity program. The cybersecurity program must be designed to identify and assess cybersecurity risks; protect information systems and nonpublic information; detect, mitigate and recover from cybersecurity events; and fulfill applicable regulatory reporting obligations. While the NY Regulations are only two years old and apply only to NY Covered Entities, they have inspired similar initiatives in the insurance industry and consumer protection sphere.

On October 24, 2017, the National Association of Insurance Commissioners (NAIC) adopted an Insurance Data Security Model Law (Insurance Model Law).[31] The Insurance Model Law builds on existing data privacy and consumer breach notification obligations by requiring insurance licensees to comply with detailed requirements regarding maintaining an information security program and responding to and giving notification of cybersecurity events.

The Insurance Model Law is similar in many respects to NY Regulations, and the NAIC's drafting notes clearly indicate that it was inspired by those

regulations. For example, both regulations require regular risk assessments to test the adequacy of the information security or cybersecurity program. Further, tracking the NY Regulations, the Insurance Model Law requires every licensee (unless exempted) to maintain a written cybersecurity policy and to implement a risk-based cybersecurity program. The program must be broadly designed to protect its nonpublic information and must be subject to oversight from the licensee's board of directors.

However, unlike the NY Regulations, the Insurance Model Law pertains solely to insurance licensees, and because it is only a model law, it will only apply to licensees in any given state if it is enacted into law by that state. Moreover, each state will have the freedom to modify the wording of the Insurance Model Law as it sees fit.

Separately, on March 5, 2019, the FTC proposed changes to the version of the Safeguards Rule that it enforces.[32] The FTC proposal would add more detailed requirements for what should be included in the comprehensive information security program mandated by its Safeguards Rule. The FTC proposal also would require nonbank financial institutions, not including RIAs, to implement specific information security controls, including with respect to data encryption, multifactor authentication, incident response planning, board reporting, and program accountability. In this regard, the FTC proposal draws heavily from the NY Regulations and imposes very similar requirements, although the FTC proposal will not impose an annual certification requirement on financial institutions.

RIAs should critically evaluate the NY Regulations and variants put forward by the NAIC and the FTC. The NY Regulations have been scaled to financial institutions of all sizes, from major global banks to small check cashers, and many lawyers and consultants are comfortable applying the NY Regulations. For some RIAs, the NY Regulations may provide a current, comprehensive framework that can be efficiently applied to a small to medium-sized firm.

In particular, standalone RIAs may find the NY Regulations to be a comprehensive approach to cybersecurity that is less burdensome than the bank requirements, but still is tailored to the financial services industry and addresses incident response and breach notification. While the NY Regulations do not explicitly address the requirements in the Safeguards Rule, there is intuitive appeal to adopting something that has worked well for similarly situated entities and provides more specific guidance than what the SEC has provided to date.

NASAA Information Security Model Rule Proposal

On September 23, 2018, the North American Securities Administrators Association, Inc. (NASAA) released a proposed model rule for State IAs that would impose new information security and privacy requirements (NASAA Proposal).[33] The NASAA Proposal is intended to provide State IAs with a basic structure for implementing information security policies, procedures, and practices and to create uniformity in state regulation of investment adviser cybersecurity.

However, the NASAA Proposal is not binding on any State IA unless and until state securities administrators formally adopt it through state administrative rulemakings. Additionally, the NASAA Proposal applies to State IAs and generally would not apply to RIAs, which are exempt from state registration under the National Securities Markets Improvement Act of 1996's amendments to the Investment Advisers Act of 1940. (However, the NASAA Proposal would amend the model rules for unethical business practices and prohibited conduct (the UBP Model Rules), which would apply to State IAs and RIAs.) RIAs also may find that the NASAA Proposal provides a more comprehensive framework that can inform a Regulation S-P compliance program.

There are three components to the NASAA Proposal: (i) a new model information security and privacy rule that would require State IAs to adopt policies and procedures, (ii) an amendment to the

existing model recordkeeping rule, and (iii) an amendment to the UBP Model Rules.

The proposed model information security and privacy rule would address the implementation of physical security and cybersecurity policies and procedures. These policies and procedures would need to cover the following functions:

- **Identify**. Develop the organizational understanding to manage information security risk to systems, assets, data, and capabilities;
- **Protect**. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;
- **Detect**. Develop and implement the appropriate activities to identify the occurrence of an information security event;
- **Respond**. Develop and implement the appropriate activities to take action regarding a detected information security event; and
- **Recover**. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information security event.

In addition, the proposed amendment to the UBP Model Rules would clarify that a failure to establish, maintain, and enforce a required policy or procedure would be an unethical business practice and prohibited conduct.

RIAs may find the pending NASAA Proposal helpful in evaluating their Safeguarding Procedures and related policies. Unlike Regulation S-P, the NASAA Proposal was drafted in the cyber age and with cybersecurity concerns in mind.

NFA Action

On January 7, 2019, the National Futures Association (NFA) announced amendments to its information security requirements for the futures industry that include a cybersecurity incident notification obligation.[34] In 2015, the NFA had adopted Interpretive Notice 9070, which established extensive information security standards for futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants (collectively, NFA members).[35] However, in its original form, Interpretive Notice 9070 did not require NFA members to report cybersecurity incidents.

The 2019 amendments include a cybersecurity incident notification requirement that establishes an explicit, uniform reporting regime for NFA members.[36] Specifically, the 2019 amendments require all NFA members, except for FCMs for which the NFA is not the designated self-regulatory organization, to notify the NFA of (i) "cybersecurity incidents related to their commodity interest business that result in a loss of customer or counterparty funds or loss of a Member firm's capital" and (ii) "any cybersecurity incident related to its commodity interest business if the Member notifies its customers or counterparties of the incident pursuant to state or federal law."

Along with the cybersecurity incident notification requirement, the NFA's 2019 amendments also clarified other aspects of Interpretive Notice 9070 related to (i) the approval of a member's information security program, (ii) suspicious activity report filing procedures, (iii) training, and (iv) the resources available to members.

RIAs already must comply with state data breach notification laws, and RIAs that are dual-registered commodity trading advisors must comply with the NFA's 2019 amendments. All RIAs, however, should look closely at the NFA's 2019 amendments as a model for how they might handle breach notification.

Conclusions

The SEC has used the Safeguards Rule to address cybersecurity concerns for RIAs, but arguably that rule is a dated and imperfect fit. In particular, the Safeguards Rule alone does not provide a comprehensive framework for RIAs to identify, assess, mitigate, and manage cybersecurity risks or include incident

response planning and notification elements and was adopted before the onslaught of today's cyber risks. While the SEC has set some expectations through guidance (much of which was the result of OCIE's cybersecurity sweep examinations) and enforcement actions, they were provided in piecemeal fashion and, notably, with the benefit of hindsight. The SEC's most recent agenda of regulatory actions does not indicate that the agency plans to amend Regulation S-P or adopt a cyber/information security rule in the near-term or long-term. [37] This implies that the SEC and its Staff intend to continue the practice of establishing a cybersecurity framework for RIAs by issuing informal guidance and bringing enforcement actions under Regulation S-P and related rules.

Accordingly, RIAs might need more specific guidance to better define the scope and content of their Safeguarding Procedures and to understand the risks they should be designed to mitigate. As a result, RIAs might look to the more recent steps taken by others in the financial services sector as a way to inform their Safeguarding Procedures and related protocols (for example, incident response). These efforts include the comprehensive frameworks established by the banking regulators and the recent frameworks put forward by NYDFS and NASAA that reflect current thinking in cybersecurity.

Overall, it is important for RIAs to carefully consider each piece of guidance issued by the SEC and other regulators, consistently amend their Safeguarding Procedures and related cyber/ information security policies, procedures, and controls, and continually educate their supervised persons, based on the most recent regulatory activity, developing industry practices, and the ever-changing cybersecurity landscape. This ever-shifting goalpost can make it difficult for RIAs to assess risks, identify priorities, and allocate capital. While somewhat counterintuitive, governmental agencies sometimes can reduce the compliance burden on the private sector by codifying collections of guidance and supervisory expectations in comprehensive, principles-based regulations. Cybersecurity is the largest risk of our time, particularly for the investment management industry, and RIAs, for regulatory and reputational purposes, should navigate this arena cautiously and with vigilance.

Mr. Taft, partner, and **Mr. Bisanz**, associate, are members of the Financial Services Regulatory and Enforcement practice group at Mayer Brown LLP. **Ms. Cruz**, counsel, is a member of the Corporate and Securities practice group at Mayer Brown LLP. The authors wish to thank Sheya Jabouin, a summer associate, who assisted in drafting this article.

NOTES

1 The Financial Industry Regulatory Authority (FINRA) is a self-regulatory organization that oversees broker-dealers, certain of which might also be RIAs or affiliates of an RIA. This article includes cybersecurity actions taken by FINRA where they may be relevant to the investment management industry.

2 Since 2013, the SEC has administered and enforced the Identity Theft Red Flags Rules (Regulation S-ID) that require RIAs and broker-dealers to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. *Identity Theft Red Flags Rules*, Rel. No. IA-3582, 78 Fed. Reg. 23,638 (Apr. 19, 2013) (codified at 17 C.F.R. § 248.201). While Regulation S-ID can relate to cybersecurity, it applies across a registrant's operations and is beyond the scope of this article. *See also*, Mayer Brown, "SEC Brings First Enforcement Action Under the Identity Theft Red Flags Rule" (Oct. 23, 2018).

3 Because this article is focused on cybersecurity issues for RIAs under the information protection provisions of Regulation S-P, it does not address the privacy provisions of Regulation S-P or other analogous

privacy laws (*e.g.*, California Consumer Privacy Act, EU General Data Protection Regulation).

4 *See* Pub. L. 106–102, 113 Stat. 1338 (1999). In 2003, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which directed the SEC to adopt regulations requiring the secure disposal of consumer information derived from consumer reports. Pub. L. 108-159, 117 Stat. 1952, 1985-86 (2003). The SEC implemented the FACT Act by amending the regulations implementing GLBA.

5 *See* Pub. L. 106–102, tit. V, 113 Stat. 1338, 1436-50 (1999).

6 15 U.S.C. § 6801(a).

7 *Privacy of Consumer Financial Information (Regulation S-P)*, 65 Fed. Reg. 40,334 (June 29, 2000) (codified at 17 C.F.R. § 248.30). The SEC amended Regulation S-P in 2004 to add a sub-section to the Safeguards Rule that requires Registered Entities that maintain or possess "consumer report information" for a business person to take "reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." *Disposal of Consumer Report Information*, Rel. No. IA-2332 (69 Fed. Reg. 71,322) (Dec. 8, 2004) (amending 17 C.F.R. § 248.30).

8 17 C.F.R. § 248.30(a).

9 *Part 248-Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, 73 Fed. Reg. 13,692 (Mar. 13, 2008). The proposed amendments also would have extended the application of the Safeguards Rule to registered transfer agents and would have extended the application of its disposal provisions to natural persons associated with broker-dealers, RIAs, and registered transfer agents.

10 Aspects of the proposed amendments, however, have been adopted by staff of the Commodity Futures Trading Commission (CFTC) as an expectation for CFTC-regulated entities. CFTC Staff Adv. No. 14-21 (Feb. 26, 2014).

11 Since those initial actions in 2007 and in addition to the actions discussed below, the SEC has brought at least ten other enforcement actions against Registered Entities and their associated persons for violations of the Safeguards Rule. SEC, Rel. No. IA-4834 (Dec. 22, 2017); SEC, Rel. No. 34-77,595 (Apr. 12, 2016); SEC, Rel. No. IA-4204 (Sept. 22, 2015); SEC, Rel. No. 34-66,113 (Jan. 6, 2012); SEC, Rel. No. 34-64,220 (Apr. 7, 2011); SEC, Rel. No. 34-64,221 (Apr. 7, 2011); SEC, Rel. No. 34-64,222 (Apr. 7, 2011); SEC, Rel. No. 34-62,313 (June 17, 2010); SEC, Rel. No. IA-2929 (Sept. 20, 2009); SEC, Rel. No. 34-60,326 (July 17, 2009); SEC, Rel. No. IA-2775 (Sept. 11, 2008); SEC, Rel. No. 34-58,192 (July 18, 2008).

12 *Third OCIE Cybersecurity Exam Sweep Underway*, ACA Insight (Apr. 1, 2019).

13 OCIE, *Examination Priorities for 2013* (Feb. 21, 2013). OCIE's examination priorities are released annually and are designed to provide a preview of key areas where OCIE intends to focus its resources.

14 OCIE, *Risk Alert: Safeguarding Customer Records and Information in Network Storage–Use of Third Party Security Features* (May 23, 2019).

15 OCIE, *Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P - Privacy Notices and Safeguard Policies* (Apr. 16, 2019). *See also,* Mayer Brown, "SEC's OCIE Issues Risk Alert for Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P" (Apr. 30, 2019). OCIE also published a risk alert in February 2019 relating to safeguarding of securities and funds held by transfer agents. OCIE, *Transfer Agent Safeguarding of Funds and Securities* (Feb. 13, 2019). This alert does not relate to the Safeguards Rule and therefore is not addressed in this article.

16 OCIE, *2019 Examination Priorities* (Dec. 20, 2018). See also, Mayer Brown, *OCIE's 2019 Examination Priorities and 2018 Enforcement Actions: Practice Points for Advisers to Consider* (Feb. 19, 2019). On January 22, 2019, FINRA released its 2019 priorities for its examinations of member broker-dealers, including some dual-registered RIAs. FINRA, *2019 Annual Risk Monitoring and Examination Priorities*

Letter (Jan. 22, 2019). FINRA's 2019 priorities state that it will continue to review the adequacy of members' cybersecurity programs to protect sensitive information, including personally identifiable information, in part by using the measures it identified in its 2018 update to its report on effective cybersecurity practices at broker-dealers.

17 OCIE, *Risk Alert: Observations From Cybersecurity Examinations* (Aug. 7, 2017). *See also*, OCIE, *2015 Cybersecurity Examination Initiative* (Sept. 15, 2015); Mayer Brown, "US Securities and Exchange Commission's Office of Compliance Inspections and Examinations Announces Results of Cybersecurity Examination Initiative" (Aug. 15, 2017).

18 OCIE, *Cybersecurity: Ransomware Alert* (May 17, 2017).

19 *See* SEC IM, *Guidance Update: Cybersecurity Guidance*, No. 2015-02 (Apr. 2015). *See also*, Mayer Brown, "US Securities and Exchange Commission Division of Investment Management Issues Guidance on Cybersecurity" (May 29, 2015).

20 OCIE, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015). *See also*, OCIE*, Cybersecurity Initiative* (Apr. 15, 2014) (announcing the sweep); Mayer Brown, "OCIE and FINRA Announce the Results of Cybersecurity Initiatives" (Mar. 25, 2015).

21 SEC, Rel. No. IA-5048 (Sept. 26, 2018). *See also,* Mayer Brown, "SEC Brings First Enforcement Action Under the Identity Theft Red Flags Rule" (Oct. 23, 2018).

22 *See* FINRA, AWC No. 2015043455201 (Sept. 28, 2017).

23 *See*, Mayer Brown, "US SEC Highlights Focus on Cybersecurity in Enforcement Action for Safeguards Rule Violations" (June 13, 2016).

24 *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 66 Fed. Reg. 8616 (Feb. 1, 2001). While styled as "guidelines," the documents impose detailed obligations on banks and carry the same force as an obligation set forth in a regulation or statute. Federal banking regulators examine banks to ensure that they are complying with the guidelines and may bring enforcement actions against deficient banks.

25 *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 59 Fed. Reg. 15,736 (Mar. 29, 2005).

26 As discussed below, the Federal Trade Commission (FTC) has proposed changes to the version of the Safeguards Rule that it enforces that would establish a more comprehensive framework for nonbank financial institutions.

27 *See* Colo. Code Regs. §§ 704-1:51-4.8, 4.14; 4-4 Vt. Code R. § 8:8-4.

28 Colo. Code Regs. §§ 704-1:51-4.8, 4.14.

29 4-4 Vt. Code R. § 8:8-4.

30 NYDFS, Press Release (Feb. 16, 2017); Cybersecurity Requirements for Financial Services Companies, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (codified at N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500). *See also*, Mayer Brown, "Cybersecurity: NY Adopts Final Regulations for Banks, Insurance Businesses and Other Financial Services Institutions" (Mar. 21, 2017).

31 *See* NAIC, *NAIC Passes Insurance Data Security Model Law* (Oct. 24, 2017). *See also*, Mayer Brown, "NAIC Adopts Insurance Data Security Model Law" (Nov. 10, 2017).

32 *Standards for Safeguarding Customer Information,* 84 Fed. Reg. 13,158 (proposed Apr. 4, 2019); *Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act*, 84 Fed. Reg. 13,150 (proposed Apr. 4, 2019). *See also*, Mayer Brown, "US Federal Trade Commission Proposes Prescriptive Data Security Requirements and Other Updates to Its Gramm-Leach-Bliley Act Regulations" (Mar. 22, 2019).

33 NASAA, *Request for Public Comment Regarding a Proposed IA Model Rule for Information Security and Privacy Under the Uniform Securities Acts of 1956 and 2002* (Sept. 23, 2018). *See also*, Mayer Brown, "NASAA Proposes Investment Adviser Model Cybersecurity Rule" (Jan. 4, 2019).

[34] *See* NFA, Notice I-19-01 (Jan. 7, 2019). *See also*, Mayer Brown, "US National Futures Association Adopts Notification Requirement for Certain Cybersecurity Incidents" (Jan. 18, 2019).

[35] *See* NFA, Notice I-15-23 (Oct. 23, 2015).

[36] NFA members, and others including RIAs, should be cognizant that cybersecurity incident notification may be imposed through other applicable regulatory requirements, state data breach laws, or contracts with other parties. Many Registered Entities may have committed to notifying counterparties or other business partners of cybersecurity incidents by signing agreements containing broad notification language.

[37] The SEC publishes an agenda of regulatory actions it expects to take in the near-term and long-term. OMB, *Spring 2019 Unified Agenda of Regulatory and Deregulatory Actions* (May 13, 2019). The agenda covers only planned rulemaking activities (*e.g.*, not planned guidance or interpretations), and an agency may engage in rulemaking activities that are not disclosed on the agenda.