SECURITY BASECAMP

SBC Alert - Summary of Cybersecurity Guidance from Financial Services Regulators

CYBERSECURITY GUIDANCE

NASD (n/k/a FINRA) Rules of Fair Practice have always required confidential treatment of customer information. Regulation S-P further strengthened this requirement. Brokers, dealers, investment companies, and investment advisers registered with the SEC are required to:

1. *Adopt reasonably designed written policies and procedures addressing administrative, technical, and physical safeguards for the protection of customer information and records; and*
2. *Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.*

Business practices have evolved significantly since the time that FINRA and the SEC originally issued guidance regarding the protection of customer information. This alert summarizes such cybersecurity guidance.

JANUARY 2021

Security Basecamp
(949) 330-0899

Table of Contents

NOTABLE REGULATORY GUIDANCE REGARDING CYBERSECURITY

NASD (n/k/a FINRA) Rules of Fair Practice have always required confidential treatment of customer information. Regulation S-P[1] further strengthened this requirement. Brokers, dealers, investment companies, and investment advisers registered with the SEC are required to:

1. Adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.

Business practices have evolved significantly since the time that FINRA and the SEC originally issued guidance regarding the protection of customer information. Each, as summarized below, has issued detailed cybersecurity reports to regulated institutions that provide guidance regarding vendor management. States, most notably New York (effective now) and California (to be effective in early 2020), have enacted legislation and those of the New York Department of Financial Services (NY-DFS) are highlighted below.

FINRA

FINRA published a Report on Cybersecurity Practices[2] in the broker dealer industry to highlight effective practices that firms should consider to strengthen their cybersecurity programs. FINRA stated that the report "does not create any new legal requirements or change any existing regulatory obligations. Our expectation is that firms will use the report to assess and strengthen their cybersecurity practices."

The report has a section dedicated to Vendor Management. FINRA stated, "Broker dealers typically use vendors for services that provide the vendor with access to sensitive firm or client information or access to firm systems. Firms should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of their vendor relationships."[3] Key points of the section on Vendor Management include the following.

- Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:
    - performing pre-contract due diligence on prospective service providers. This due diligence provides a basis for the firm to evaluate whether the prospective vendor's cybersecurity measures meet the firm's cybersecurity standards;
    - establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access, and which govern both the ongoing relationship with the vendor and the vendor's obligations after the relationship ends;
    - performing ongoing due diligence on existing vendors;
    - including vendor relationships and outsourced systems as part of the firm's ongoing risk assessment process;
    - establishing and implementing procedures to terminate vendor access to firm systems immediately upon contract termination; and
    - establishing, maintaining and monitoring vendor entitlements to align with firm risk appetite and information security standards.
- Analyzing FINRA's requirements makes it essential that vendor risk management be an on-going activity and that it involves the application of cybersecurity standards. Key problems facing our industry include the

[1] Morrison & Foerster LLP, Broker Dealer Cybersecurity: Protect Yourself or Pay the Price, January 10, 2014: Regulation S-P became effective in November 2000, and compliance with the rules and regulations has been mandatory since July 1, 2001.
[2] FINRA, *Report on Cybersecurity Practices* (February 3, 2015).
[3] Ibid, page 2.

reality that first, most firms (in particular, small financial advisory firms), do not have the resources required to effectively perform cybersecurity due diligence of their vendors and second, often do not know the standards that should be applied.

- Firms across many industry sectors rely on third-party vendors for a range of services. As recent incidents have shown, these same vendors can also be a significant source of cybersecurity risk. These risks can arise in different ways, for example, if a vendor or one of its employees misuses firm data or systems, if the vendor itself is subject to a cyberattack that compromises vendor systems or firm data, or if an attack on a vendor becomes a vector for an attack on a firm's systems. Firms need an effective vendor management program in place to help guard against these risks.[4]
- The Notice to Members footnoted in this statement relates to "outsourcing" and in summary, broker dealers or regulated entities FINRA wished to "remind members that, in general, any parties conducting activities or functions that require registration under NASD rules will be considered associated persons of the member, absent the service provider separately being registered as a broker dealer and such arrangements being contemplated by NASD rules (such as in the case of clearing arrangements)" and that "in addition, outsourcing an activity or function to a third-party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and NASD and MSRB rules regarding the outsourced activity or function." In other words, it is the regulated institution that is being held accountable (not necessarily the third-party to which an important business function is being outsourced).

Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC)

OCIE stated in its 2019 Examination Priorities letter that it "will continue to prioritize cybersecurity in each of its five examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and policies and procedures. Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response."[5]

As it relates to vendor management, areas that the OCIE has stated it will review include:

- Vendor Management Policies and Procedures: Maintain firm policies and procedures related to third-party vendors, such as those addressing the following:
    - Due diligence regarding vendor selection;
    - Contracts, agreements, and the related approval process;
    - Supervision, monitoring, tracking, and access control; and
    - Any risk assessments, risk management, and performance measurements and reports required of vendors.
- Third-party Access: Maintain information regarding third-party vendors with access to the firm's network or data, including the services provided and contractual terms related to accessing your firm networks or data.
- Third-party Risk Contingency Planning: Maintain information regarding written contingency plans the firm has with its vendors concerning, for instance, conflicts of interest, bankruptcy, or other issues that might put the vendor out of business or in financial difficulty.

On September 26, 2018, the U.S. Securities and Exchange Commission ("SEC") announced that Voya Financial Advisors Inc. ("VFA"), a Des Moines-based broker dealer and investment advisor, agreed to pay $1 million to settle charges related to an April 2016 data breach that gave unauthorized access to the personally identifiable information of at least 5,600 VFA customers. Even though this is the first SEC enforcement action under the Identity Theft Red Flags Rule, and just the third involving the Safeguards Rule (the previous two actions were brought in 2014 and 2016,

[4] *See* Notice to Members 05-48 for further information about firms' obligations in outsourcing arrangements.
[5] See OCIE 2019 Examinations Letter

respectively[6]), SEC scrutiny of broker dealer and investment advisor cybersecurity has long been on the horizon. In September 2017, the SEC announced the creation of a Cyber Unit within the Enforcement Division in order to police cyber-related misconduct. In February of 2018, the SEC issued new guidance to public companies on how to disclose cybersecurity risks and incidents to investors. In April 2018, the SEC settled claims with Altaba Inc. (formerly Yahoo! Inc.) in the amount of $35 million in connection with Yahoo's failure to timely disclose a 2014 data breach of hundreds of millions of user accounts. This action is consistent with the SEC's increased focus on cybersecurity and serves as a reminder to companies that the SEC will likely continue to pursue actions under the Safeguards Rule and Identity Theft Red Flags Rule[7]. Additionally, it is possible that the SEC will find software firms held more accountable for the mishandling of a breach.

New York Department of Financial Services (NY-DFS)

The NY-DFS Cybersecurity Regulation (23 NYCRR 500) is a set of regulations from the New York Department of Financial Services that places new cybersecurity requirements on financial institutions. It is generally viewed as one of the most prescriptive sets of law in the area of cybersecurity. The NY-DFS Cybersecurity Regulation applies to all entities (aka, a Covered Entity) operating under NY-DFS licensure, registration, charter, or those that are otherwise DFS regulated. Some broker dealers have chosen to follow it, while others have not. The regulation also applies to unregulated third-party service providers working with those regulated entities.

Section 500.11, Third-Party Service Provider Security Policy, of the law states:

a. Third-party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:
    (1) the identification and risk assessment of Third-Party Service Providers;
    (2) minimum cybersecurity practices required to be met by such Third-Party Service Providers for them to do business with the Covered Entity;
    (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers; and
    (4) periodic assessment of such Third-Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.
b. Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third-Party Service Providers including to the extent applicable guidelines addressing:
    (1) the Third-Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part[8], to limit access to relevant Information Systems and Nonpublic Information;

[6] Source: SEC, The SEC levied a $75,000 penalty against St. Louis-based broker dealer R.T. Jones Capital Equities Inc. after hackers stole 100,000 individuals' details from its webserver, and subsequently fined Morgan Stanley $1 million after hackers stole client information; September 2015

[7] Source: Alto Litigation, Broker Dealer and Investment Advisor Settles Charges with SEC Related to 2016 Data Breach, October 10, 2018

[8] Section 500.12 Multi-Factor Authentication states, "Multi-Factor Authentication. (a) Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls."

(2) the Third-Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part[9] to protect Nonpublic Information in transit and at rest;
(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third-Party Service Provider; and
(4) representations and warranties addressing the Third-Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

c. Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third-party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

[9] Section 500.15 Encryption of Nonpublic Information states, "(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. (1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO. (2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

ADDITIONAL LEGAL AND REGULATORY RESOURCES

FINRA's Report on Cybersecurity Practices (February 2015)

FINRA published a Report on Cybersecurity Practices in the broker dealer industry to highlight effective practices that firms should consider in strengthening their cybersecurity programs. Given the evolving nature, increasing frequency and sophistication of cybersecurity attacks, as well as the potential for harm to investors, firms and the markets, cybersecurity practices remain a key focus for FINRA. FINRA's goal in publishing the report was to focus firms on a risk management-based approach to cybersecurity that is adaptable and capable of addressing evolving threats.

FINRA Report on Selected Cybersecurity Practices (December 2018)

This report continues FINRA's efforts to share information that can help broker dealer firms further develop their cybersecurity programs. Firms routinely identify cybersecurity as one of their primary operational risks. Similarly, FINRA continues to see problematic cybersecurity practices in its examination and risk monitoring program. This report presents FINRA's observations regarding effective practices that firms have implemented to address selected cybersecurity risks while recognizing that there is no one-size-fits-all approach to cybersecurity

OCIE Cybersecurity Examination Sweep Summary (February 2015)

This Risk Alert provides summary observations from OCIE's examinations of registered broker dealers and investment advisers, conducted under the Cybersecurity Examination Initiative, announced April 15, 2014.

New York State Department of Financial Services - Cybersecurity Requirements for Financial Services Companies

The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a set of regulations from the New York Department of Financial Services that places new cybersecurity requirements on financial institutions. This regulation imposes strict cybersecurity rules on covered organizations, such as banks, mortgage companies, and insurance firms. The regulation requires financial companies to install a detailed cybersecurity plan, enact a comprehensive cybersecurity policy, and initiate and maintain an ongoing reporting system for cybersecurity events. The NYDFS Cybersecurity Regulation applies to all entities operating under DFS licensure, registration, charter, or those that are otherwise DFS regulated. The regulation also applies to unregulated third-party service providers working with regulated entities.

California Consumer Privacy Act of 2018

The intentions of the Act are to provide California residents with the right to: 1) Know what personal data is being collected about them; 2) Know whether their personal data is sold or disclosed and to whom; 3) Say no to the sale of personal data; 4) Access their personal data; 5) Equal service and price, even if they exercise their privacy rights.

The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds: 1) Has annual gross revenues in excess of $25 million; 2) Possesses the personal information of 50,000 or more consumers, households, or devices; or 3) Earns more than half of its annual revenue from selling consumers' personal information

2018 Reform of EU Data Protection Rules

As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based. Stronger rules on data protection mean: 1) people have more control over their personal data and 2) businesses benefit from a level playing field.

ABOUT SECURITY BASECAMP

Security Basecamp is a consulting firm focused exclusively in the financial services industry. We partner with executives and managers to facilitate effective business planning and help you competitively leverage technology for profitable growth. Our mission is to help financial services firms solve their most challenging strategic business issues through critical thinking, rigorous project management, and/or the savvy use of practical technologies.

Collectively, our consultants have managed more than 100 strategy, operations, technology, compliance, and business development projects over the past 25 years. We bring a business-oriented approach to completing cybersecurity projects and the technical acumen to work effectively with your internal IT staff. We help you manage cybersecurity analysis, action planning, and execution that your busy management team doesn't have the time or resources to lead. We offer three primary cybersecurity services: 1) Risk Assessments, 2) a vCISO Service, and 3) Vendor Cybersecurity Due Diligence. To learn more, visit our website www.securitybasecamp.com or call (949) 330-0899.

AUTHOR INFORMATION

Paul Osterberg
Managing Director, Security Basecamp
(949) 330-0899
posterberg@securitybasecamp.com