Overview of Data Privacy and Cybersecurity Regulatory Landscape for Investment Advisers and Other Financial Services Companies

Numerous regulatory authorities and self-regulatory organizations are now focusing intently on cybersecurity and privacy practices of investment advisers and other financial services companies. These regulators include:

- the Securities and Exchange Commission ("SEC");
- the Financial Industry Regulatory Authority ("FINRA");
- the Commodity Futures Trading Commission ("CFTC");
- the Federal Trade Commission ("FTC");
- the Consumer Financial Protection Bureau ("CFPB");
- the National Futures Association ("NFA");
- state regulatory agencies, such as the New York State Department of Financial Services; and
- state attorneys general.

SEC: The SEC has identified cybersecurity as a very important issue facing investment advisers and broker-dealers. For example, cybersecurity has been included in the list of examination priorities issued by the SEC's Office of Compliance Inspections and Examinations (the "OCIE") during the last few years. In connection with its two cybersecurity initiatives in 2014 and 2015, the OCIE conducted examinations of SEC-registered investment advisers and broker-dealers to identify cybersecurity risks and to assess cybersecurity preparedness in the securities industry. These examinations primarily focused on the following general areas:

a. governance and risk assessment;
b. access rights and controls;
c. data loss prevention;
d. vendor management;
e. training; and
f. incident response.

In conducting these examinations, the OCIE obtained various documents and other information from registered investment advisers and broker-dealers, regarding the cybersecurity-related areas. Some of the questions the OCIE asked of its examinees tracked information that was outlined in the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology.

In 2016 and 2017, the OCIE advanced its examination efforts relating to cybersecurity, which included testing and assessments of firms' implementation of data security procedures and controls. Additionally, the OCIE recently placed cybersecurity at the top of its list of market-wide risks on which it would focus.

FINRA: FINRA is a self-regulatory organization that oversees brokerage firms, branch offices and registered securities representatives. In the cybersecurity space, FINRA reviews broker-dealers' ability to protect the confidentiality, integrity and availability of sensitive customer information. This includes reviewing each firm's compliance with SEC regulations, such as Regulations S-P and S-ID, which are discussed later.

Not long ago, FINRA conducted an examination "sweep" of a cross-section of firms. That sweep

focused on the types of cyber threats that firms face, areas of vulnerabilities in their systems and firms' approaches to managing these threats. FINRA has announced that during 2017, it plans to continue to assess its regulated firms' programs to mitigate those cyber risks.

FTC: The FTC is a primary federal regulator in charge of policing corporate cybersecurity practices. Since 2002, the FTC has commenced dozens of cases and administrative proceedings against companies for allegedly unfair or deceptive practices that endanger the sensitive personal data of consumers.

CFPB: The CFPB is a new entrant into the world of cybersecurity enforcement. Although it has brought few cybersecurity-related enforcement actions so far, it may have broad authority to do so under its power to prohibit unfair, deceptive or abusive acts or practices (which are also known as the CFPB's "UDAAP" authority).

This article provides a high-level overview of the cybersecurity laws and regulations that apply to investment advisers and other financial services companies. It also describes recent enforcement actions that regulators have pursued in the cybersecurity field.

Federal Laws and Regulations

A. The Gramm-Leach-Bliley Act and Safeguards Rules

1. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (the "GLB Act") is a 1999 federal law that broadly reformed the banking industry by eliminating certain barriers between banking and commerce. The GLB Act also requires financial institutions under the jurisdiction of various regulators to provide their customers with notice of their privacy policies and practices, and prohibits them from disclosing non-public personal information about a consumer to non-affiliated third parties unless the institutions provide certain information to the consumer and the consumer has not elected to opt out of the disclosure.

In addition, Section 501 of the GLB Act provides that each financial institution must protect the security and confidentiality of its customers' non-public personal information.[1] Section 501 requires regulatory agencies to establish standards for financial institutions relating to administrative, technical and physical safeguards:

1. to insure the security and confidentiality of customer records and information;
2. to protect against any anticipated threats or hazards to the security or integrity of such records; and
3. to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Section 505(b) of the GLB Act specifies the regulatory agencies that are responsible for implementing the standards prescribed under Section 501, by type of financial institution.[2] For example, the SEC is responsible for establishing safeguards rules for investment advisers, investment companies and broker-dealers. The Office of the Comptroller of the Currency, the Federal Reserve and the CFTC are responsible for establishing safeguards rules for financial institutions under their jurisdiction. The FTC is responsible for establishing safeguards rules for financial institutions that are not subject to the jurisdiction of any of the other agencies specified under Section 505(a) of the GLB Act.

These privacy and data security provisions of the GLB Act do not pre-empt or supersede state laws or regulations, to the extent those state laws or regulations are not inconsistent with the GLB Act.[3] A state law or regulation is not considered "inconsistent" with the GLB Act if it affords any person protection greater than the protection provided under the GLB Act. Thus,

[1] 15 U.S.C. § 6801.
[2] 15 U.S.C. § 6805.
[3] 15 U.S.C. § 6807.

financial institutions may be subject to stricter state privacy and data security laws and regulations.

2. The SEC Safeguards Rule (Regulation S-P)

Regulation S-P is the SEC's privacy and safeguards rule promulgated under the GLB Act.[4] That regulation covers investment advisers registered with the SEC, brokers, dealers and investment companies. Section 248.30 of Regulation S-P provides that every broker, dealer, investment company and investment adviser registered with the SEC must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.

These policies and procedures must be reasonably designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Regulation S-P does not specify what data security policies and procedures must be adopted. Rather, it just provides that those policies and procedures must be "reasonably designed" to achieve the three goals listed above. However, recent SEC enforcement actions and settlements, some of which are described in Section III. below, illustrate some types of policies and procedures that the SEC does not consider reasonable.

3. The CFTC's Safeguards Rule

The CFTC's safeguards rule is similar to Regulation S-P.[5] Section 160.30 of the CFTC's rule requires futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, swap dealers and major swap participants to adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.

4. The FTC Safeguards Rule

The FTC is authorized to enforce the data security provisions of the GLB Act with respect to financial institutions that are not covered by the federal banking agencies, the SEC, the CFTC or state insurance authorities. Among the institutions that fall under FTC jurisdiction are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services and debt collectors.

As directed by the GLB Act, the FTC promulgated a safeguards rule that applies to the handling of "customer information" by financial institutions under the FTC's jurisdiction.[6] That rule requires financial institutions under its jurisdiction to develop, implement and maintain a comprehensive information security program, consisting of the administrative, technical or physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit or otherwise handle customer information, including information about the customers of other financial institutions.[7]

---

[4] *The text of Regulation S-P can be found at* https://www.sec.gov/rules/final/34-42974.htm.

[5] The CFTC's safeguards rule can be found at http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2011-17710a.pdf.

[6] The FTC's safeguards rule can be found at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.

[7] "Customer information" is defined as "any record containing nonpublic personal information … about a customer of a financial institution, whether in paper, electronic, or other form" that is "handled or maintained by or on behalf of" a financial institution or

The safeguards must also be reasonably designed to insure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Financial institutions under the FTC's jurisdiction must designate employees responsible for coordinating their information security programs. They also must identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, the risk assessment should include consideration of risks in each relevant area of the financial institution's operations, including:

- employee training and management;
- information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- detecting, preventing and responding to attacks, intrusions or other system failures.

Financial institutions must then design and implement information safeguards to control the risks they identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures.

its affiliates. The FTC's safeguards rule does not apply to all consumer information handled by a financial institution. Rather, it applies only to the information of "customers," which are consumers that have a continuing relationship with a financial institution that provides one or more financial products or services to be used primarily for personal, family or household purposes.

Financial institutions must oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and by requiring service providers by contract to implement and maintain such safeguards.

Finally, financial institutions must evaluate and adjust their information security programs in light of the results of the testing and monitoring, any material changes to the financial institution's operations or business arrangements, or any other circumstances that the financial institution knows or have reason to know may have a material impact on its information security program.

The FTC considers violations of the Safeguards Rule to be "an unfair or deceptive act or practice," which is prohibited by Section 5(a) of the FTC Act. Section 5(a) of the FTC Act is described below.

B. Other Securities and Exchange Commission Rules and Guidance

1. SEC and CFTC Joint "Red Flags" Identity Theft Rules (SEC Regulation S-ID)

The SEC and the CFTC jointly issued rules requiring certain regulated entities to establish programs to address risks of identity theft.[8] The rules (commonly known as the "red flags" rules) implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act that directed the SEC and CFTC to adopt rules requiring entities that are subject to their respective enforcement authorities to address identity theft.

The red flags rules apply to SEC-registered investment advisers and CFTC-registered commodity trading advisors and commodity pool operators that qualify as "financial institutions" or "creditors" and that offer or maintain "covered accounts." These entities must establish

[8] The rules can be found at https://www.sec.gov/rules/final/2013/34-69359.pdf.

programs to address risks of identity theft. Investment advisers may be able to avoid the rules by not coming within the definition of either a "financial institution" or a "creditor." However, these terms are interpreted broadly.

The rules define the term "financial institution" as any entity that, directly or indirectly, holds a transaction account belonging to a consumer. For example, an investment adviser may be deemed a financial institution if:

- it is permitted to direct transfers or payments from accounts belonging to individuals to third parties upon the individuals' instructions;
- it acts as an agent on behalf of clients that are individuals; or
- it manages private funds in which an individual invests money, and the adviser has authority to direct such individual's investment proceeds (such as redemptions, distributions or dividends) to third parties according to the individual's instructions.

The rules define a "creditor" as an entity that regularly and in the ordinary course of business advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person. For example, an investment adviser that regularly lends money, such as by recognizing investments before receiving a wire transfer or clearance of a check from the investor, may be considered a creditor.

Financial institutions and creditors must periodically assess whether they offer or maintain "covered accounts," which are accounts for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks. Covered accounts include brokerage accounts with a broker-dealer and accounts maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties.

The red flags rules require "financial institutions" and "creditors" under their jurisdiction to develop and implement a written identity theft prevention program designed to detect, prevent and mitigate identity theft in connection with the "covered accounts." The rules include guidelines that are designed assist these financial institutions and creditors formulate and maintain programs that satisfy the rules' requirements.

For all "covered accounts," the financial institution or creditor must establish and implement a written identity theft detection program that is appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Such programs must include at least the following elements:

- identifying relevant red flags indicating a risk of identity theft for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into its program;
- detecting red flags that have been incorporated into the program of the financial institution or creditor;
- responding appropriately to any red flags that are detected, to prevent and mitigate identity theft; and
- ensure that the program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

Each financial institution or creditor that is required to implement an identity theft mitigation program under these rules must provide for the continued administration of its program and must:

a. obtain approval of the initial program from either its board of directors or an appropriate committee of the board of directors;

b. involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the program;

c. train staff to effectively implement the program; and

d. exercise appropriate and effective oversight of service provider arrangements.

In establishing and implementing its identity theft mitigation program, each financial institution or creditor must consider the guidelines that the SEC and the CFTC included in the rules, and to include in its program those guidelines that are appropriate.

The rules also establish special requirements for any credit and debit card issuers that are subject to the SEC's and the CFTC's respective enforcement authorities, to assess the validity of notifications of changes of address under certain circumstances.

2. Investment Advisers Act Rule 206(4)-7

Under Rule 206(4)-7 under the Investment Advisers Act of 1940, it is unlawful for an investment adviser registered with the SEC to provide investment advice unless it has adopted and implemented written policies and procedures that are reasonably designed to prevent violation of the Investment Advisers Act by the adviser or its supervised persons. The rule requires advisers to consider their fiduciary and regulatory obligations under the Investment Advisers Act, and to formalize policies and procedures to address them.

The SEC's adopting release for this rule provides information about issues that funds and advisers should consider, certain of which are related to data privacy and security. For example, the SEC expects that each adviser's policies and procedures would address the following issues, to the extent that they are relevant to that adviser:

- the accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction;
- safeguards for the privacy protection of client records and information; and
- business continuity plans.

3. SEC's 2015 Cybersecurity Guidance

In 2015, the SEC's Division of Investment Management issued guidance that identified cybersecurity as a critical issue. That guidance highlighted the following measures that funds and advisers should consider in addressing cybersecurity risks:[9]

- conducting a periodic assessment of (a) the nature, sensitivity and location of information that the firm collects, and the technology systems it uses, (b) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems, (c) security controls and processes currently in place, (d) the impact of any compromise of the firm's information or technology systems, and (e) the effectiveness of the governance structure for the management of cybersecurity risk;
- creating a strategy that is designed to prevent, detect and respond to cybersecurity threats, including (a) controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation and system hardening, (b) data encryption, (c) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized

[9] The guidance can be found at https://www.sec.gov/investment/im-guidance-2015-02.pdf.

intrusions, the loss or exfiltration of sensitive data, or other unusual events, (d) data backup and retrieval, and (e) the development of an incident response plan; and

- implementing that strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

The SEC suggested that funds and advisers consider reviewing their operations and compliance programs, and assess whether they have measures in place that are designed to mitigate their exposure to cybersecurity risk. The SEC also suggested that funds and advisors assess whether protective cybersecurity measures are in place at their relevant third-party service providers.

4. SEC's 2016 Proposed Rule Regarding Business Continuity Plans

In 2016, the SEC proposed a rule under the Investment Advisers Act that would require registered investment advisers to adopt and implement written business continuity and transition plans.[10] The proposed rule is designed to ensure that investment advisers have plans in place to address operational and other risks related to a significant disruption in the adviser's operations in order to minimize client and investor harm.

The proposed rule would require an adviser's business continuity plan to include policies and procedures addressing the following components:

- maintenance of systems and protection of data;
- pre-arranged alternative physical locations;
- communication plans;
- review of third-party service providers; and
- a plan of transition in the event the adviser is winding down or is unable to continue providing advisory services.

In proposing the new rule, the SEC noted the following with regard to cybersecurity in particular:

- investment advisers generally should consider and address as relevant the operational and other risks related to cyber attacks;
- exposure to compliance and operational risks that may be caused by cybersecurity incidents can be mitigated by addressing such risks in the context of business continuity planning; and
- business continuity plans should address both hard copy and electronic backup, as appropriate.

The business continuity plan must be reviewed at least annually.

The SEC has indicated that a violation of the rule, as proposed, would constitute fraud. In that regard, the SEC reasons that an investment adviser's fiduciary duty obligates it to take steps to protect client interests from being placed at risk as a result of the adviser's inability to provide advisory services and, thus, it would be fraudulent and deceptive for an investment adviser to hold itself out as providing advisory services unless it has taken such steps.

C. THE FTC ACT

Section 5(a) of the FTC Act prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[11] Further, Section 5(n) of the FTC Act provides that, for the FTC to prohibit an act or practice on the grounds that it is "unfair," such act or practice must cause (or must be likely to cause) substantial injury to

[10] The proposed rule can be found at https://www.sec.gov/rules/proposed/2016/ia-4439.pdf.

[11] 15 U.S.C. § 45.

consumers that is (a) not reasonably avoidable by consumers themselves and (b) not outweighed by countervailing benefits to consumers or to competition. As noted above, a violation of the Safeguards Rule constitutes an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act. Section 5(a) is enforced by the FTC.

In the absence of comprehensive federal data security legislation that covers all industries, the FTC has assumed a leading role in policing corporate cybersecurity practices. So far, the FTC has pursued and negotiated dozens of consent agreements with companies for "unfair" or "deceptive" practices, where the company allegedly had inadequate cybersecurity practices or overstated how comprehensive its cybersecurity practices were. In its cybersecurity enforcement actions, the FTC has often claimed that the company violated the "unfair" or "deceptive" prong of Section 5 by failing to employ reasonable and appropriate measures to protect personal information against unauthorized access.

In determining whether to bring an enforcement action, the FTC often evaluates data security practices based on "reasonableness." Specifically, the FTC has indicated that it believes a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.

D. National Futures Association

The NFA requires its member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems.[12] In accordance with the NFA's interpretive notice, all NFA member firms, including futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers, should adopt and enforce written policies and procedures to secure customer data and access to their electronic systems.

The interpretive notice provides guidance regarding information systems security practices that NFA member firms should adopt and tailor to their particular business activities and risks. These practices include:

- Written Information Security Programs. Each NFA member firm should establish and implement a governance framework that supports informed decision making and escalation within the firm to identify and manage information security risks. Each NFA member firm is required to adopt and enforce a written information security program reasonably designed to provide safeguards, appropriate to the member firm's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities, to protect against security threats or hazards to their technology systems. The program should be approved, in writing, by the member firm's Chief Executive Officer, Chief Technology Officer, or other executive level official. Additionally, if applicable, the member firm's senior management should periodically provide sufficient information about its information security program to the member's board of directors or similar governing body, the board's or governing body's delegate or a committee of the board or body to enable it to monitor information security efforts.
- Security and Risk Analysis. Each NFA member firm should maintain an inventory of critical information technology hardware with network connectivity, data transmission or data storage capability and an inventory of critical software with applicable versions. Member firms should identify the significant internal and external threats and vulnerabilities to at-risk data that are collected, maintained and disseminated, including customer and counterparty

[12] The NFA's interpretive notice is available at http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9%20.

personally identifiable information, corporate records and financial information; assess the threats to and the vulnerability of their electronic infrastructure including any systems used to initiate, authorize, record, process and report transactions relating to customer funds, capital compliance, risk management and trading; assess the threats posed through any applicable third-party service providers or software; and know the devices connected to their network and network structure.

- Deployment of Protective Measures Against the Identified Threats and Vulnerabilities. NFA member firms should document and describe in their information security programs the safeguards deployed in light of the identified and prioritized threats and vulnerabilities.
- Response and Recovery from Events that Threaten the Security of the Electronic Systems. NFA member firms should create an incident response plan to provide a framework to manage detected security events or incidents, analyze their potential impact and take appropriate measures to contain and mitigate their threat. Member firms should also consider in appropriate circumstances forming an incident response team responsible for investigating an incident, assessing its damage and coordinating the internal and external response.
- Employee Training. The information security program should contain a description of the Member's ongoing education and training relating to information security for all appropriate personnel. This training program should be conducted for employees upon hiring and periodically during their employment and be appropriate to the security risks the member firm faces as well as the composition of its workforce.

STATE LAWS AND REGULATIONS

A. NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY REGULATION

The New York State Department of Financial Services ("DFS") recently issued an extraordinarily prescriptive cybersecurity regulation, which requires banks and trust companies, insurance companies, licensed consumer lenders, check cashers, licensed mortgage lenders and brokers, and other institutions that are regulated by the DFS (collectively, "Covered Entities") to establish and maintain a rigorous cybersecurity program.[13] Notably, Covered Entities that are regulated by the DFS but operate outside of New York State are also subject to this regulation.

The DFS regulation does not directly apply to entities that are not regulated by the DFS (such as hedge funds, broker-dealers and national banks). However, because the DFS regulation is very comprehensive, regulators that do have jurisdiction over hedge funds could decide to adopt rules that are very similar to the DFS regulation. In addition, the DFS regulation obligates Covered Entities to assess the cybersecurity risks posed by certain of their third party service providers. Thus, as a result of the DFS regulation, non-Covered Entities that lack adequate cybersecurity policies and procedures may be unable to continue doing business with Covered Entities.

The principal purpose of the DFS regulation is to protect the security of Covered Entities' "Information Systems" and "Nonpublic Information" from "Cybersecurity Events." Under the DFS regulation, "Nonpublic Information" is defined as electronic information consisting of:

[13] The DFS regulation, 23 NYCRR 500, can be found at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf. The DFS regulation became effective on March 1, 2017, and Covered Entities have 180 days from that date to comply with most of the regulation's requirements.

- business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the Covered Entity's business, operations or security;
- any information concerning an individual which because of name, number, personal mark or other identifier can be used to identify such individual, together with any one or more of the following: (i) social security number, (ii) driver's license number or non-driver identification card number, (iii) account number, credit card number or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; and
- any information (except age or gender) created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or family member, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

The DFS regulation defines a Cybersecurity Event as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on the Information System.

Under the DFS regulation, Covered Entities must abide by the following requirements, among others:

- Cybersecurity Program. Covered Entities must establish and maintain a cybersecurity program that is designed to protect the confidentiality, integrity and availability of their Information Systems, and to perform certain other core cybersecurity functions, such as (a) identifying internal and external cyber risks that may threaten the security or integrity of Nonpublic Information stored on Information Systems, (b) using defensive infrastructure and implementing policies and procedures to protect Information Systems and the Nonpublic Information stored on the Information Systems, (c) detecting and responding to cybersecurity events, and (d) responding to and recovering from cybersecurity events.
- Written Cybersecurity Policy. Covered Entities must implement and maintain a written cybersecurity policy to address the protection of their Information Systems and the Nonpublic Information that is stored on those systems. The written cybersecurity policy must be based on the Covered Entity's own risk assessment, and the policy be approved by a senior officer of the Covered Entity or by the Board of Directors or equivalent governing body.
- Incident Response Plan. Each Covered Entity must establish a written incident response plan that is designed to respond promptly to, and recover from, a cybersecurity event.
- Chief Information Security Officer. Each Covered Entity must designate a qualified individual to serve as its Chief Information Security Officer (known as a CISO), who is responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy. The CISO must report in writing at least annually to the Covered Entity's Board of Directors or equivalent governing body. While Covered Entities may satisfy the CISO requirement by engaging third-party service providers, a senior member of the Covered Entity must oversee the service provider and retain responsibility for compliance with the DFS regulation.
- Cybersecurity Personnel. Each Covered Entity must also engage sufficiently trained and competent cybersecurity personnel to manage its cybersecurity risks and implement security measures. Covered Entities may utilize an affiliate or a qualified third party service provider to comply with this requirement.

- Controls to Secure Nonpublic Information. Covered Entities must implement controls to secure Nonpublic Information (which may include encryption) that are appropriate based on their risk assessments. The DFS prefers that Covered Entities encrypt Nonpublic Information, but encryption is not absolutely required. However, Covered Entities that use controls other than encryption must review the effectiveness of those controls (and review the feasibility of encryption) at least annually.
- Monitoring and Testing. The cybersecurity program for each Covered Entity must include monitoring and testing that is designed to assess the effectiveness of the cybersecurity program. Covered Entities must conduct annual penetration testing and bi-annual vulnerability assessments, absent effective continuous monitoring or other systems to detect changes that may indicate vulnerabilities.
- Notification of DFS Regarding Cybersecurity Events. Certain Cybersecurity Events require notice to the DFS within 72 hours of their detection. Cybersecurity Events that require such notice to the Superintendent are (a) Cybersecurity Events for which notice must be provided to any supervisory body (including supervisory bodies under the laws of other states or countries), and (b) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. Moreover, if a Covered Entity identifies areas that require material improvement, updating or design, the Covered Entity must document its identification of the problem and its remedial efforts. The DFS Superintendent may inspect the Covered Entity's documentation.
- Third Party Service Providers. Each Covered Entity must implement written policies and procedures to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third party service providers who do business with the Covered Entity. These procedures are expected to address the following issues, to the extent they are applicable to the Covered Entity:
  - identification and risk assessment of third party service providers;
  - minimum cybersecurity practices required to be met by third party service providers for them to do business with the Covered Entity;
  - due diligence processes used to evaluate the adequacy of cybersecurity practices of third party service providers; and
  - periodic assessment of third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.
- Annual Certification Requirement. Each Covered Entity must submit an annual written certification to the superintendent of the DFS, certifying that it is in compliance with the requirements of the regulation. All records and data supporting these annual certifications must be retained for five years, and such records and data may be examined by the DFS.

Certain small Covered Entities are exempt from some of the requirements of the proposed regulation, but still are required to comply with most of the general requirements such adopting a cybersecurity program, and naming a CISO. To qualify for this limited exemption, Covered Entities must have fewer than 10 employees and independent contractors located in New York State or responsible for the Covered Entity's business, less than $5 million in gross annual revenue from New York business operations for each of the last three fiscal years, and less than $10 million in year-end total assets (including the assets of all affiliates). The DFS regulation includes a handful of other exemptions, as well.

B. State Breach Notification Laws

At least 47 states, the District of Columbia, and some U.S. territories have their own data breach

notification laws, which generally require businesses to notify affected individuals and regulatory authorities if the businesses suffer a data breach in which personally identifiable information is compromised. Importantly, if a business has customers in multiple states and suffers a data breach, it may be required to comply with the breach notification requirements of each state in which it has customers.

In New York State, Section 899-aa of the General Business Law provides that parties conducting business in New York State that own or license computerized data which includes "private information" must disclose any breach of that data to any New York State residents whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.[14] Such notification must be made in "the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." However, the notification may be delayed if a law enforcement agency determines that the notification would impede a criminal investigation. If more than 5,000 New York State residents must be notified at one time, then the business must also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.

Moreover, these businesses must notify three regulatory authorities: (a) the New York State Attorney General, (b) the New York State Division of State Police, and (c) the New York Department of State's Division of Consumer Protection. Notifications to these regulators must describe the timing, content and distribution of the notices, as well as the approximate number of affected persons. Such notice must be made without delaying notice to the affected New York State residents.

The New York data breach notification statute defines "private information" as "personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or when it is encrypted with an encryption key that has also been compromised:

- Social Security number;
- driver's license number or non-driver identification number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Private information" does not include publicly available information which is lawfully made available to the general public from government records.

If the New York State Attorney General believes that a business has violated Section 899-aa of the General Business Law, then the Attorney General may seek an injunction to enjoin the continuation of such violation. In addition, the court may award damages (including damages for consequential financial losses) for actual costs or losses incurred by a person entitled to notice under the statute, if notification was not properly provided. If a business knowingly or recklessly violates the statute, the court may impose a civil penalty of up to $10 per instance (and up to $150,000 in the aggregate).

Regulators' Recent Examination Priorities and Enforcement Activity Concerning Cybersecurity

A. SEC

The SEC has recently taken aggressive action against investment advisers and broker-dealers with respect to potential violations of cybersecurity laws and regulations. In many of these actions, the SEC alleged that investment advisers and broker-dealers had violated

[14] The statute is available at http://public.leginfo.state.ny.us/lawssrch.cgi?NVLWO:

Regulation S-P (which is described above). If an investment adviser or broker-dealer suffers a data breach, it appears that the SEC will impose "strict liability," and conclude that the firm failed to implement appropriate cybersecurity policies and procedures.

In light of these actions, SEC-registered entities should make cybersecurity a key priority. SEC-registered entities should prepare and implement written cybersecurity policies and procedures, and update those policies and procedures on a regular basis. Among the cybersecurity "best practices" that the SEC will likely expect each firm to implement include:

- periodic risk assessments;
- firewalls;
- encryption of personally identifiable information;
- incident response plans; and
- monitoring of user activity to identify any suspicious patterns.

1. RT Jones Capital Equities Management

In 2015, R.T. Jones Capital Equities Management, a St. Louis-based investment adviser ("R.T. Jones") settled charges by the SEC that it had failed to establish reasonable cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information ("PII") of approximately 100,000 individuals, including thousands of the firm's clients.[15] The SEC concluded that R.T. Jones violated Regulation S-P by failing to adopt any written policies or procedures to ensure the security and confidentiality of PII. In particular, the SEC made the following findings:

- R.T. Jones stored PII of clients and others on its third party-hosted web server.
- The firm's web server was attacked in July 2013 by an unknown hacker who gained access and copy rights to the data on the server, rendering the PII vulnerable to theft.
- The firm failed to adopt written policies and procedures reasonably designed to safeguard customer information. For example, the firm failed to conduct periodic risk assessments, implement a firewall, encrypt PII that was stored on its server, or maintain a response plan for cybersecurity incidents.
- After the firm discovered the breach, the firm promptly retained more than one cybersecurity consulting firm to confirm the attack, which was traced to China, and determine the scope.
- Shortly after the incident, R.T. Jones provided notice of the breach to every individual whose PII may have been compromised and offered free identity theft monitoring through a third-party provider.

Without admitting or denying the findings, R.T. Jones agreed to cease and desist from committing or causing any future violations of Regulation S-P. R.T. Jones also agreed to be censured and to pay a $75,000 penalty.

Notably, R.T. Jones was censured and paid this penalty, even though it took prompt action to respond to the breach (including by hiring cybersecurity consulting firms), and even though it provided notice to affected individuals. What is more, the SEC conceded that R.T. Jones's violation of Regulation S-P resulted in "no apparent financial harm to clients."

Here, R.T. Jones found itself in trouble with the SEC because it did not have appropriate policies and procedures in place before the breach occurred. In the SEC's press release announcing this settlement, the Co-Chief of the SEC Enforcement Division's Asset Management Unit stated that "[f]irms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures

[15] The SEC's press release announcing this settlement can be found at https://www.sec.gov/news/pressrelease/2015-202.html.

in place rather than waiting to react once a breach occurs."

2. Morgan Stanley

In 2016, Morgan Stanley Smith Barney LLC ("Morgan Stanley") agreed to pay a $1 million civil penalty to settle the SEC's charges related to Morgan Stanley's alleged failures to protect customer information, some of which was hacked and offered for sale online.[16] In particular, the SEC concluded that Morgan Stanley violated Regulation S-P by failing to adopt written policies and procedures reasonably designed to protect customer data. As a result of these failures, a former-employee impermissibly accessed and transferred data relating to approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties. In particular, the SEC made the following findings:

- Morgan Stanley's policies and procedures were not reasonable for two internal web applications or "portals" that allowed its employees to access customers' confidential account information.
- For these portals, Morgan Stanley did not have effective authorization modules for more than 10 years to restrict employees' access to customer data based on each employee's legitimate business need.
- Morgan Stanley also did not audit or test the relevant authorization modules, nor did it monitor or analyze employees' access to and use of the portals.
- Consequently, a former employee of Morgan Stanley downloaded and transferred confidential data to his personal server at home between 2011 and 2014.
- A likely third-party hack of the former employee's personal server resulted in portions of the confidential data being posted on the Internet with offers to sell larger quantities.

Morgan Stanley agreed to settle the SEC's charges without admitting or denying the findings.

3. Craig Scott Capital

In 2016, Craig Scott Capital, LLC, a registered broker-dealer, and its principals agreed to settle charges that they violated requirements that broker-dealers adopt written policies and procedures to protect confidential customer information and records and to keep and maintain copies of all business communications.[17]

The SEC's investigation found that Craig Scott Capital used personal email addresses to receive thousands of faxes from customers and other third parties. These faxes routinely included sensitive customer records and information, such as customer names, addresses, social security numbers, bank and brokerage account numbers, copies of driver's licenses and passports, and other customer financial information. The SEC also found that the firm's written supervisory procedures failed to adequately protect customer information and records because they failed to address how customer records and information transmitted through the electronic fax system were to be handled, and they were not otherwise tailored to the actual practices at the firm.

The SEC concluded that the firm violated Regulation S-P by failing to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records. Without admitting or denying the findings, the firm agreed to pay a $100,000 civil money penalty, and the firm's principals each agreed to pay a $25,000 civil money penalty.

---

[16] The SEC's press release announcing this settlement can be found at https://www.sec.gov/news/pressrelease/2016-112.html.

[17] The SEC's press release announcing this settlement can be found at https://www.sec.gov/litigation/admin/2016/34-77595-s.pdf.

B. FTC

The FTC has commenced numerous court actions and administrative proceedings against companies that have allegedly violated consumers' privacy rights, or that have allegedly misled consumers by promising to maintain the security of sensitive personal information (but failing to actually do so). The FTC Act does not specifically address data security or data breaches. Nonetheless, since 2002 the FTC has brought over 60 cases against companies that had allegedly engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk, on the theory that such practices are "unfair" or "deceptive" in violation of Section 5(a) of the FTC Act, whether or not these practices lead to a breach of PII.

In addition, as noted above, the FTC enforces provisions of the GLB Act, as well as the FTC Safeguards Rule, against financial services companies that are not subject to the jurisdiction of any of the other agencies specified under Section 505(a) of the GLB Act. The FTC does not have enforcement jurisdiction over banks.

In 2012, the FTC commenced an action in federal district court against PLS Financial Services, Inc., a manager of payday loan and check cashing stores, alleging that the company disposed of documents containing PII (including Social Security numbers, employment information, loan applications, bank account information and credit reports) in unsecured dumpsters. The FTC also alleged that the company violated the FTC Safeguards Rule by failing to develop and use safeguards to protect consumer information. Finally, the FTC alleged that the company violated the FTC Act by misrepresenting that it had implemented reasonable measures to protect sensitive consumer information. The company ultimately agreed to pay a $101,500 civil penalty to settle the suit.

C. CFPB

The CFPB, which was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, lacks specific enforcement authority with respect to the data security provisions of the GLB Act. However, the CFPB does have authority to prohibit "unfair, deceptive or abusive acts or practices" in connection with consumer financial products and services (its "UDAAP" authority), and to prohibit other actions that otherwise violate federal consumer financial laws. The CFPB's enforcement jurisdiction covers large banks, as well as non-bank companies that offer consumer financial products and services (such as mortgage lenders, credit card networks, payday lenders, debt collectors, student loan services and automotive finance companies). The FTC and CFPB share enforcement jurisdiction over almost all types of non-bank companies that provide consumer financial products and services.

The CFPB may have authority to impose civil penalties with respect to any type of data security violation, under the CFPB's broad UDAAP authority. The penalties start at up to $5,000 per day for violations, and rise to up to $25,000 per day for "recklessly" engaging in violations and up to $1 million per day for "knowing" violations. In contrast, the FTC only has the ability to impose civil penalties in specific types of data security cases, such as cases involving violations of the Children's Online Privacy Protection Act.

In its first data security enforcement action, which the CFPB brought under its UDAAP authority, the CFPB issued a consent order in 2016 against Dwolla, Inc. (an online payment platform) for deceiving consumers about its data security practices and the safety of its online payment system. In particular, the CFPB alleged that Dwolla deceptively claimed to protect consumer data from unauthorized access with "safe" and "secure" transactions. On its website and in its communications with consumers, Dwolla claimed that its data security practices exceeded industry standards and that it was compliant with the Payment Card Industry Data Security Standards (PCI-DSS). Dwolla also claimed that it encrypted all sensitive

personal information, and that its mobile applications were safe and secure.

However, the CFPB found that Dwolla in fact had failed to:

- adopt and implement data security policies and procedures that were reasonable and appropriate for the organization;
- conduct regular risk assessments, or to assess the safeguards in place to control those risks;
- properly train its employees;
- use encryption technologies to properly safeguard sensitive consumer information; or
- test the security of its applications to ensure that consumers' sensitive information was protected before the apps' public release.

Under the terms of the CFPB's order, Dwolla was required (a) to cease misrepresenting its data security practices, (b) to train employees and improve data security practices, and (c) to pay a $100,000 civil penalty. In addition, even though there was no allegation of an actual data breach, the CFPB required Dwolla and its Board of Directors to abide by stringent requirements going forward.[18]

D. FINRA

1. Sterne, Agee & Leach, Inc.

In 2015, FINRA reached a settlement with brokerage firm Sterne, Agee & Leach, Inc., under which the firm agreed to sanctions, including public censure and a $225,000 fine.[19] The action arose from the loss of a laptop computer that contained unencrypted confidential financial and personal information regarding hundreds of thousands of customers. In particular, an information technology employee of the firm inadvertently left an unencrypted laptop in a restroom and it was lost. The lost laptop was believed to contain files that contained account numbers, client names, client addresses, and tax identification numbers for all accounts opened or closed on the firm's systems.

FINRA concluded that the firm's security policy and standards did not adequately address the security of laptop computers, and that the firm had failed to take appropriate technological precautions to protect customer and highly sensitive information. In particular, the firm's policies and standards did not require encryption of laptop hard drives. As a result, FINRA determined that the firm violated Regulation S-P. FINRA also determined that the firm had violated NASD Conduct Rule 3010 and FINRA Rule 2010.[20]

2. Centaurus Financial, Inc.

FINRA levied a $175,000 fine on Centaurus Financial, Inc. for its failure to protect certain confidential customer information. Centaurus was also ordered to provide notifications to affected customers and their brokers and to offer these customers one year of free credit monitoring.[21]

---

[18] The CFPB's press release announcing the settlement with Dwolla can be found at https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/

[19] The Letter of Acceptance, Waiver and Consent relating to this settlement can be found at http://disciplinaryactions.finra.org/Search/ViewDocument/51064.

[20] NASD Rule 3010(a) was replaced by FINRA Rule 3110(a), which requires a firm to have a supervisory system for the activities of its associated persons that is reasonably designed to achieve compliance with applicable rules and regulations, and sets forth the minimum requirements for a firm's supervisory system. FINRA Rule 2010 provides that a "member, in the conduct of its business, shall observe high standards of commercial honor and just and equitable principles of trade."

[21] FINRA's press release announcing this settlement can be found at http://www.finra.org/newsroom/2009/finra-fines-centaurus-financial-175000-failure-protect-confidential-customer.

FINRA determined that for over a year, the firm had failed to ensure that it safeguarded confidential customer information. Its improperly-configured computer firewall, together with an ineffective username and password on its computer facsimile server, permitted unauthorized persons to access documents that included confidential customer information, such as social security numbers, account numbers, dates of birth and other sensitive data.

The firm's failures also permitted an unknown individual to conduct a phishing scam. When the firm became aware of that scam, it conducted an inadequate investigation and sent a misleading notification letter to approximately 1,400 affected customers and their brokers. As a result, FINRA determined that the firm violated Regulation S-P and FINRA rules.

E. State Attorneys General and Other State Regulators

Federal regulators are not the only ones who have authority to commence enforcement actions and reach settlements with companies regarding cybersecurity. Material data breaches involving theft or unauthorized access of PII will likely draw the attention of state attorneys general. As noted above, almost all states have data protection and breach notification laws, which are enforced at the state level. Some examples of state attorney general enforcement actions are below:

In 2016, Provision Supply, LLC (d/b/a EZcontactsUSA.com) entered into a $100,000 settlement with the New York State attorney general. The settlement arose from a data breach that resulted in the potential exposure of over 25,000 credit card numbers and other cardholder data. EZcontactsUSA.com has agreed to pay $100,000 in penalties and to enhance its data security practices. In particular, the attorney general had alleged that EZcontactsUSA.com did not maintain a written security policy. Moreover, EZContactsUSA.com failed to provide notice to its customers or law enforcement about the breach, in violation of New York State's data breach notification law (which is described above).[22]

TD Bank, N.A. entered into a settlement agreement with the attorneys general of nine states. Under the agreement, TD Bank settled allegations that it had violated state laws in connection with a data breach that involved the loss of two unencrypted backup tapes containing the personal information of approximately 260,000 customers. Under the settlement agreement, TD Bank agreed to pay $850,000 to the attorneys general. It also agreed to maintain reasonable security policies to protect personal information (including a prohibition on transporting unencrypted backup tapes) and to assess its policies regarding the collection, storage and transfer of consumers' personal information at least every two years.[23]

In addition, Adobe Systems Inc. recently entered into a settlement agreement with the attorneys general of fifteen states. The settlement arose from the attorneys generals' investigation of a cyber attack that Adobe suffered in 2013, in which the personal information of millions of customers was stolen. In the attorneys generals' view, the risk of a cyber attack was "reasonably foreseeable," but Adobe failed to employ reasonable security measures to protect its systems. The attorneys general also alleged that Adobe's conduct contravened its representations to consumers that it would take reasonable steps to protect consumers' personal information. Under the terms of the settlement, Adobe was required to pay $1 million and to implement new cybersecurity policies.[24]

---

[22] The New York State attorney general's press release announcing the settlement is available at https://ag.ny.gov/press-release/ag-schneiderman-announces-100k-settlement-e-retailer-after-data-breach-exposes-over

[23] A copy of the settlement is available at http://www.ct.gov/ag/lib/ag/press_releases/2014/20141016_oag_cdp_tdbank_settlement.pdf.

[24] A copy of the settlement is available at http://src.bna.com/j1m.

Conclusion

Federal and state regulators are increasingly focused on financial institutions' data security practices and procedures, and have not hesitated to take enforcement action against firms whose practices they find lacking. Firms that suffer data breaches may also find themselves embroiled in private party litigation. Now is the time for financial institutions to examine their security infrastructure and practices, and to ensure that they comply with applicable regulations.

For more information on the topic discussed or if you have any questions or concerns with respect to your organization's cybersecurity practices, please contact any member of Tannenbaum Helpern's Cybersecurity & Data Privacy practice:

Andre R. Jaglom
212.508.6740 | jaglom@thsh.com

David R. Lallouz
212.702.3142 | lallouz@thsh.com

Michael J. Riela
212.508.6773 | riela@thsh.com

Beth Smigel
212.702.3176 | smigel@thsh.com

Maryann C. Stallone
212.508.6741 | stallone@thsh.com

Vincent J. Syracuse
212.508.6722 | syracuse@thsh.com

About Tannenbaum Helpern Syracuse & Hirschtritt LLP

Since 1978, Tannenbaum Helpern Syracuse & Hirschtritt LLP has combined a powerful mix of insight, creativity, industry knowledge, senior talent and transaction expertise to successfully guide clients through periods of challenge and opportunity. Our mission is to deliver the highest quality legal services in a practical and efficient manner, bringing to bear the judgment, common sense and expertise of well trained, business minded lawyers. Through our commitment to service and successful results, Tannenbaum Helpern continues to earn the loyalty of our clients and a reputation for excellence. For more information, visit www.thsh.com. Follow us on LinkedIn and Twitter: @THSHLAW.