READING MATERIALS

REGULATORY ENFORCEMENT PRIORITIES

Privacy+ Security Academy

Arnold & Porter

March 16, 2021

NYDFS Fines Residential Mortgage Services $1.5 Million for Failures to Comply with New York's Cybersecurity Regulation

Enforcement Edge: Shining Light on Government Enforcement

By Jami Vibbert, Kevin M. Toomey, Michael A. Mancusi, Nancy L. Perkins, Anthony Raglani, Jason T. Raylesberg

On March 3, 2021, the New York Department of Financial Services (NYDFS) announced its execution of a consent order (the Order) with Residential Mortgage Services, Inc. (RMS), a NYDFS-licensed mortgage banker and mortgage loan servicer. The Order fines RMS $1,500,000 for its violations of Cybersecurity Regulation, Part 500 of Title 23 of the New York Codes, Rules, and Regulations (Part 500). According to the Order, RMS failed to meet its Part 500 obligations by inadequately responding to a data security breach and failing to conduct a comprehensive cybersecurity risk assessment. This action is the latest demonstration of the seriousness with which NYDFS is approaching enforcement of Part 500, which became fully effective in March 2019.

The Order serves as a warning to and guide for financial institutions that may prompt them to reevaluate whether their existing cybersecurity safeguards, policies, and procedures are sufficient to meet the requirements of Part 500. Moreover, it reinforces the imperative for covered entities to fully comply with all aspects of Part 500––even where entities believe that their cybersecurity measures meet their level of risk or are consistent with industry standards.

To learn more about the Order and its implications for the financial services industry, read this Advisory.

Arnold & Porter

May 11, 2021

Cybercrime Is on the Rise: Will the Federal Government Require Companies to Report Cyber Attacks?

By Jami Vibbert, Ronald D. Lee

On May 8, 2021, Colonial Pipeline had to shut down a 5,500-mile fuel pipeline from Texas to New Jersey after its network experienced a ransomware attack. This attack follows a long list of other, recent high-profile cyber attacks in recent months. As cyber experts and officials have noted, cybercrime has been dramatically increasing since the SolarWinds attack, targeting critical infrastructure such as hospitals, manufacturers, and government entities. Companies are often hesitant to disclose information about security incidents, frequently making it difficult to gauge the timeframe and scope of a cyberattack and making it even more challenging to keep networks secure.

As a result of the SolarWinds security incident, the US Senate Select Committee on Intelligence is working on a bill that requires a limited form of mandatory reporting for the private sector when they experience a cyber attack. The goal of the legislation is to create an early warning system for foreign cyberattacks on critical organizations. The SolarWinds cyberattack, which compromised several federal agencies, is believed to have been carried out by Russian hackers, and the FBI has confirmed that a Russian cybercrime gang named DarkSide compromised Colonial Pipeline's network. Listen to Privacy, Cybersecurity & Data Strategy partners Ron Lee and Jami Vibbert discuss the pending mandatory reporting legislation and how privacy officers and counsel can prepare for potential new requirements and compliance.

Arnold & Porter

June 11, 2021

Lessons Learned from the SolarWinds Cyberattack, and the Future for the New York Department of Financial Services' Cybersecurity Regulation

Advisory

By Ronald D. Lee, Michael A. Mancusi, Amber A. Hay, Anthony Raglani

In December 2020, a cybersecurity company alerted the world to a major cyberattack against the US software development company, SolarWinds, through the company's Orion software product (SolarWinds Attack). The SolarWinds Attack went undetected for months, as it has been reported that the hackers accessed the source code for Orion as early as March 2020.[1] Orion is widely used by companies to manage information technology resources, and according to SolarWinds Form 8-K filed with the Securities and Exchange Commission, SolarWinds had 33,000 customers that were using Orion as of December 14, 2020.

It is alleged that the SolarWinds Attack was one part of a widespread, sophisticated cyber espionage campaign by Russian Foreign Intelligence Service actors which focused on stealing sensitive information held by US government agencies and companies that use Orion.[2] The hack was perpetuated through SolarWinds sending its customers routine system software updates.[3] SolarWinds unknowingly sent out software updates to its customers that included the hacked code that allowed the hackers to have access to customer's information technology and install malware that helped them to spy on SolarWinds' customers, including private companies and government entities, thereby exposing up to 18,000 of its customers to the cyberattack.

The New York Department of Financial Services (DFS) alerted DFS-regulated entities of the SolarWinds Attack on December 18, 2020 through the "Supply Chain Compromise Alert."[4] The Supply Chain Compromise Alert included guidance from the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, SolarWinds, and other sources, and reminded the regulated entities of their obligations under the New York Cybersecurity Regulation (Cybersecurity Regulation), adopted in 2017, which requires DFS-regulated entities, including New York banks, insurance companies and producers and other financial services firms, to develop a comprehensive cybersecurity program, implement specific cybersecurity controls, assess cybersecurity risks posed by third-party service providers, and notify DFS of "cybersecurity events" (which includes certain *unsuccessful* cyberattacks) that carry a "reasonable likelihood" of causing material harm to the operations of the institution or otherwise require notice to any governmental or supervisory entity.[5]

DFS followed up its Supply Chain Compromise Alert with its *Report on the SolarWinds Cyber Espionage Attack and Institutions' Response* (SolarWinds Report), released in April 2021.[6] In the SolarWinds Report, DFS analyzes the remediation of approximately 100 of its regulated entities to the SolarWinds Attack, and DFS's recommendations for ways that organizations can strengthen their cybersecurity practices to protect against future cyberattacks. In general, DFS found that its regulated entities responded "swiftly and appropriately" with 94% of impacted companies removing the vulnerable systems caused by the SolarWinds hackers from their networks (and or patching them) within three days of being notified of the attack. However, DFS noted gaps in cybersecurity policies of several regulated entities, including irregularities in patching and patch management systems, identifying third-party service providers as critical vendors, and the need for more information sharing and transparency among the regulated entities with respect to cybersecurity breaches.

Interestingly, DFS's observations as detailed in the SolarWinds Report, and specifically those related to the need for enhanced cybersecurity preparedness by companies and their third-party service providers and the need for more transparency and information sharing among companies regarding actual or perceived cyberthreats, align with the principles outlined in President Biden's Executive Order on Improving the Nation's Cybersecurity, released on May 12, 2021, applicable to the federal government and government contractors. This could signal a new wave of state cybersecurity laws and regulations if not a federal regulation in the foreseeable future.

This Advisory provides a brief overview of DFS's findings detailed in the SolarWinds Report, and the outlook for DFS's enforcement of the Cybersecurity Regulation, as well as potential changes to those rules, based on DFS's findings and observations.

DFS-Regulated Entities' Response to the SolarWinds Attack and Weaknesses Identified in Patch Management Systems

As detailed in the SolarWinds Report, DFS found that its supervised companies generally responded to the SolarWinds Attack swiftly and appropriately, by clearing their systems of the infected software within three days of notification by disconnecting, patching, or applying a mitigation script. The remediation steps that were taken by more than half of the regulated companies to mitigate risks associated with the SolarWinds Attack included, but were not limited to:

- Evaluated system integrity and audit logs for indicators of compromise;
- Disconnected affected systems from their networks; and
- Applied security patches to affected systems.

About a quarter or less of DFS-regulated entities took the following remediation steps:

- Isolated affected systems by blocking access to the internet;
- Isolated affected systems by blocking specific external DNS domains, based on guidance by Cybersecurity and Infrastructure Security Agency;
- Decommissioned Orion and replaced it with another monitoring product; and
- Applied mitigation scripts to affected systems, as recommended by SolarWinds.

While these remediation steps allowed DFS-regulated entities to address the risks associated with the SolarWinds Attack once identified, DFS found that several companies could have addressed the risks posed by the SolarWinds Attack (if not preventing it altogether) by implementing a mature patch management system.

According to DFS, several DFS-regulated companies' patch management programs were immature at the time of the cyberattack, and the lack of proper "patching cadence"[7] likely resulted in a delay in the ability of the companies to ensure timely remediation of high-risk cyber vulnerabilities. For example, it is reported that the cyberhackers inserted the malware referred to as "Sunburst" into SolarWinds's software Orion in February 2020, and SolarWinds unknowingly distributed updates of the Orion software with the Sunburst malware to its customers between March and June 2020.[8] DFS found that some of the companies found to be vulnerable to Sunburst malware in December 2020 had not applied patches released by SolarWinds in August and October 2020 that would have eliminated Sunburst, and some companies had not patched since 2018, with two companies having not patched since 2017. Fortunately, there have been no reports that the hackers exploited the vulnerabilities caused by the Sunburst (or Supernova) malware;[9] however, supervised entities need to ensure proper patching cadence to prevent against material harm from vulnerabilities that may result from future cyberattacks.

DFS's Recommendations for Regulated Entities Going-Forward

DFS includes in its reports key observations and recommendations for DFS-regulated entities to prevent against supply chain attacks and reduce supply chain risks, based on industry standards on cybersecurity measures. The key recommendations noted by DFS include that supervised entities should:

- Ensure that third party service provider and other vendor risk management policies and procedures should include processes for due diligence and contractual protections that will ensure the company can monitor the cybersecurity practices and overall cyber hygiene of critical vendors. These policies should include provisions requiring third-party service providers to immediately notify the regulated company when a cyber event occurs that impacts or could potentially impact an organization's information systems or non-personal information that is maintained, processed or accessed by the vendor.
- Adopt a "Zero Trust" approach and assume that any software installation and any third-party service provider could be compromised and used as an attack vector. In this regard, third party service providers' access to a company's network systems or Nonpublic Information (NPI) should be limited to only what is needed and systems should be monitored for anomalous or malicious activity. Regulated entities are also expected to implement multiple layers of security for extra protection for sensitive information to limit compromises.
- Have a vulnerability management program that prioritizes patch testing, validation processes, and deployment, including which systems to patch and the order or priority of patching. In addition, a regulated entity's patch management strategy should include

performing tests of all patches to the internal system environment with defined rollback procedures if the patch creates or exposes additional vulnerabilities.

- Have an effective and tested incident response plan with detailed procedures and playbooks. DFS also notes that cybersecurity fundamentals such as knowing your environment and understanding where assets reside in the environment, including their versions and configuration, should be incorporated into playbooks. To address supply chain compromises or attacks, the incident response plans should include, at a minimum:
    - Procedures to isolate affected systems;
    - Procedures to reset account credentials for users of all affected assets and users of assets controlled by compromised software;
    - Procedures to rebuild from backups created before the compromise;
    - Procedures to archive audit and system logs for forensic purposes; and
    - Procedures to update response plans based on lessons learned.

DFS recommends that regulated entities engage in "table top" exercises to test and refine incident response plans, and notes that incident response plans should be aligned with an organization's business continuity plan.

DFS also notes in the SolarWinds Report that there is a need for more transparency and effective information sharing amongst DFS-regulated entities regarding cybersecurity breaches, which would have allowed organizations that detected the intrusion earlier than December 13, 2020 to alert the others. DFS found that some of its regulated entities publicly revealed that they blocked an intrusion prior to the intrusion becoming widely known by others. Based on this finding, DFS has indicated that it plans to improve information sharing and transparency, which suggests that future changes to the Cybersecurity Regulation may encourage DFS-regulated entities to share information on cyberattacks. Financial institutions are currently able to share information one with another and report to the federal government activities that may involve money laundering or terrorist activity (including those that involve or tied to cyberattacks) under Section 314(b) of the USA PATRIOT Act (Section 314(b)). DFS could adopt a voluntary information sharing approach similar to that under Section 314(b) of the USA PATRIOT Act for cybersecurity breaches that are not covered by Section 314(b).

Outlook for Future Changes to the Cybersecurity Regulation and Enforcement

DFS has been the most active state government functional regulator focused on cybersecurity regulation, and the issuance of the SolarWinds Report is one of the many examples of DFS continuing its efforts.

After adopting the Cybersecurity Regulation in 2017,[10] and releasing several alerts informing its regulated companies of cyber threats and providing reminders of obligations under the Cybersecurity Regulation, in July 2020, DFS commenced its first enforcement action under the Cybersecurity Regulation against the second largest title insurance provider in the US[11] In February of this year, DFS released the US's first Cyber Insurance Risk Framework and alerted DFS-regulated entities of the growing cyber campaign to steal NPI.[12]

With respect to management of supply chain risks, DFS-regulated companies should expect future changes to the Cybersecurity Regulation and related guidance that stresses the importance of:

- Effective third-party risk management and identifying critical vendors that have access to sensitive information and NPI;
- Enhanced information sharing amongst regulated entities regarding cybersecurity breaches;
- Adequate patch management systems, with validation processes, deployment, and priorities, as well as mandated patching and testing of patch management systems on a routine basis; and
- Mandated testing of incident response plans that include cybersecurity fundamentals and "table top" exercises.

Additional Considerations for DFS-Regulated Banks

DFS may look to federal regulations and guidance for developing additional requirements related to incident response plans. DFS-regulated banks and other insured depository institutions are also subject to the regulation and supervision of the federal banking agencies, and in December 2020 the federal banking agencies proposed a computer-security incident notification rule that would require banking organizations to notify their primary regulators upon the occurrence of certain computer-security incidents as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred.[13] Under the proposed rule, bank service providers also would be required to notify the banking organizations for which they provide services of computer-security incidents that the service provider believes in good faith could disrupt, degrade or impair services provided for four or more hours. The

heightened focus of supervisory agencies on real-time information sharing of cybersecurity incidents that may be disruptive and harmful to supervised institutions and the industry likely will require certain institutions to enhance their monitoring, testing, and reporting controls and processes over time. In addition, although it appears that the proposed rule would have a collaborative purpose and is not intended to be used as a means of identifying and scrutinizing supervised institutions perceived to have insufficient cybersecurity risk management controls, institutions must nonetheless be prepared to manage any supervisory or examination scrutiny that may arise from the satisfaction of their current and future obligations to share information with their regulators and other institutions regarding known or suspected cybersecurity incidents (if, for example, a cybersecurity incident exposes a vulnerability or insufficient control that results in greater supervisory or examination scrutiny and/or enforcement action).

Conclusion

All in all, the SolarWinds Attack provided DFS with a real-time opportunity to assess the cybersecurity preparedness of its regulated entities, and identify areas of improvement for its regulated entities in managing risks from third-party service providers as well as areas of improvement for cybersecurity regulation. The SolarWinds Report provides some insight into DFS's expectations of DFS-regulated entities, as well as plans for the future of the Cybersecurity Regulation and related guidance.

[1] See gen., The US is readying sanctions against Russia over the SolarWinds cyberattack and SEC Form 8-K, Solarwinds Corporation.

[2] Business Insider, December 20, 2020, Former US cybersecurity chief Chris Krebs says officials are still tracking 'scope' of the SolarWinds hack.

[3] SolarWinds unknowingly sent out software updates to its customers that included the hacked code that allowed the hackers to have access to customer's information technology and install malware that helped them to spy on SolarWinds' customers, including private companies and government entities, and thereby exposing up to 18,000 of its customers to the cyberattack. See, Press Release - April 27, 2021: DFS Issues Report On the SolarWinds Supply Chain Attack | Department of Financial Services (ny.gov).

[4] See, the Supply Chain Compromise Alert. DFS advised its regulated entities to respond immediately to assess the risk to their systems and consumers, and take steps necessary to address vulnerabilities and customer impact. The alert included several resources for completing such tasks.

[5] In 2017, DFS adopted the Cybersecurity Regulation, 23 NYCRR Part 500, which requires all DFS-regulated financial services entities to implement a risk-based cybersecurity program and to report any unauthorized access (or attempts) to their information systems. DFS was the first in the United States to adopt such a regulation, and in 2019 DFS became the first financial regulator in the nation to establish a division dedicated to cybersecurity. See, Arnold & Porter Advisory, *New York Department of Financial Services Issues Final Cybersecurity Regulations* (February 22, 2017).

[6] *See* SolarWinds Report. It is estimated by DFS that approximately nine federal agencies and approximately 100 companies were compromised.

[7] DFS defined "patching cadence" in the SolarWinds Report to refer to how often an organization reviews systems, networks, and applications for updates that remediate security vulnerabilities.

[8] See, SolarWindsReport.

[9] Id. Following the removal of the Sunburst malware, on December 24, 2020, SolarWinds became aware of another vulnerability, referred to as "Supernova" that was found in the same versions of Orion that had the Sunburst malware as well as other versions of Orion that had been distributed to customers. SolarWinds released additional patches that addressed Supernova, and informed its customers that the patches released on December 14 and 15 also eliminated the vulnerability in the versions of Orion that held the Sunburst malware. SolarWinds released additional patches to address both Sunburst and Supernova on January 25, 2021. The Sunburst and Supernova vulnerabilities in the Orion software allowed the hackers to gain access to the exposed institutions' internal network and nonpublic information, however, as of the date of the SolarWinds Report, no reports or indications that hackers exploited the vulnerabilities resulting from the Sunburst or Supernova in any financial services organization.

[10] See, Arnold & Porter Advisory, *New York Department of Financial Services Issues Final Cybersecurity Regulations* (February 22, 2017).

[11] See, Arnold & Porter blog post, *NY Department of Financial Services Brings Its First Cybersecurity Regulation Enforcement Action* (August 3, 2020). See also, Arnold & Porter Blog post, *NYDFS Fines Residential Mortgage Services $1.5 Million for Failures to Comply with New York's Cybersecurity Regulation* (March 16, 2021).

[12] See Arnold & Porter blog post, *NYDFS Warns of Growing Cyber Campaign to Steal NPI and Reminds Entities of Part 500 Reporting Obligations*.

[13] See,Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2,299 (Jan. 12, 2021); see also,Arnold & Porter Advisory, *Federal Banking Agencies Propose Cybersecurity-Incident Notification Rule for Banks and Their Third-Party Service Providers* (Dec. 23, 2020).

Arnold & Porter

July 8, 2021

Colorado Enacts Broad Data Privacy Law, Following Lead of California and Virginia

Advisory

By Nancy L. Perkins, Jason T. Raylesberg, Suneeta Hazra, Ronald D. Lee, Jami Vibbert

On July 7, 2021, Colorado Governor Jared Polis signed into law the Colorado Privacy Act (CPA or the Act), a far-reaching statute providing Colorado residents new rights to control the collection, use and disclosure of their personal information by businesses active in the state. In so doing, Governor Polis made Colorado the third US state, following California and Virginia, to mandate procedures that will give consumers more insight into and choices regarding processing of their personal information. Most provisions of the Act will take effect on July 1, 2023; others not until July 1, 2024. Depending on their current data privacy practices, businesses that will be subject to the CPA may need to take some significant steps within the next two years to be ready with procedures for compliance.

Many aspects of the CPA resemble provisions of the California Consumer Privacy Act (CCPA) and/or the California Privacy Rights Act (CPRA) adopted by ballot initiative last year, as well as provisions of Virginia's Consumer Data Protection Act (VCDPA) enacted in March of this year.[1] And, like the VCDPA, the Act contains terms and reflects concepts used in the European Union's General Data Protection Regulation (GDPR). Colorado will likely be followed by other states in adopting legislation along the same lines, and although Congress will continue to consider proposals for an overarching federal law, it appears that at least in the near term, the states will be the innovators in this area.

Enforcement of the CPA will be by the state attorney general as well as district attorneys; the Act does not give consumers a private right of action. The attorney general also has broad rulemaking authority under the Act, and may adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for businesses. This guidance should prove helpful to businesses, as will the fact that the attorney general and district attorneys, at least until January 1, 2025, must issue a notice of violation prior to commencing an enforcement action and allow the respondent 60 days to cure.

Who is Subject to the CPA?

Like the GDPR and the VCDPA, the CPA applies to "controllers" and "processors" of "personal data," controllers being those who determine what data to collect and what should be done with it; and processors being those who process personal data on a controller's behalf. These terms roughly correspond to the CCPA's definitions of "businesses" and "service providers."

All processors of regulated controllers are subject to the CPA, regardless of their size, location or other characteristics. The controllers that are regulated under the Act are those that (1) either conduct business in Colorado or (2) produce or deliver commercial products or services that are intentionally targeted to Colorado residents (Consumers) *and* either (A) control or process the personal data of at least 100,000 Consumers during a calendar year, or (B) control or process the personal data of at least 25,000 Consumers and derive revenue or receive a discount on the price of goods or services from the sale of personal data.

A "Consumer" is a Colorado resident, but only in the context of their role as an individual or household, where they are not acting on behalf of any organization or as an employee of an organization. Thus, an individual representing a company in a business-to-business context, or an individual employed by or seeking a job from a company, is not a Consumer whose personal information would be considered in calculating the number of Consumers whose personal information the company is processing for purposes of determining the CPA's application to that company.

This scope of application tracks closely but is in one respect broader than that of the VCDPA, which, with respect to entities that control or process personal data of at least 25,000 Consumers, covers only those that derive more than *50%* of gross revenue from the sale of personal data. The CPA's scope is also similar to that of the CCPA, but is narrower in that the CCPA (subject to statutory exemptions)

applies to businesses with annual revenues above $25,000,000, *regardless of the number of Consumers whose personal data is processed*. Also, while the CCPA and the VCDPA both exempt non-profit companies from their scope, the CPA does not.

What Information Is Covered?

The CPA protects privacy interests in "personal data," which (as under the VDCPA and much like the CCPA and GDPR) is information "linked or reasonably linkable to an identified or identifiable individual," excluding de-identified data and publicly available information.

"De-identified data" under the CPA means "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual," *if the controller possessing the data:* (1) takes reasonable measures to prevent the data from being capable of association with an individual, (2) publicly commits to maintain and use the data only in de-identified form and to not attempt to re-identify the data, and (3) contractually obligates any recipients of the information to take such measures and make such commitments. In effect, the CPA thereby imposes legal obligations on recipients of de-identified data, regardless of whether they are controllers or processors subject to the CPA.

"Publicly available information" is information "lawfully made available from federal, state or local government records and information that a controller has a reasonable basis to believe the [C]onsumer has lawfully made available to the general public." This definition, similar to that in the VDCPA, is notably broader than the CCPA's, which does not cover information relating to a consumer that the consumer has themselves placed in the public domain, such as in an open Facebook profile or on LinkedIn.

What Exemptions Apply?

Like the CCPA and the VCDPA, the CPA has a number of exemptions that materially limit its scope. Most of these exemptions are for individually identifiable information protected under other privacy laws, such as protected health information under the Health Insurance Portability and Accountability Act (HIPAA), nonpublic personal financial information under Title V of the Gramm-Leach-Bliley Act (GLBA), consumer report information under the federal Fair Credit Reporting Act, children's data collected in compliance with the Children's Online Privacy Protection Act (COPPA), and personal data protected by the Family Educational Rights and Privacy Act (FERPA). Notably, the CPA expressly exempts not only personal information protected under the GLBA, but also, "a financial institution or an affiliate of a financial institution as defined by and that is subject to" the GLBA, suggesting that *any* personal information processed by such a financial institution or affiliate thereof is exempt.

What Obligations Does the CPA Impose?

The CPA sets forth a series of obligations on controllers with respect to their processing of personal data, including:

1. Data minimization (limiting their collection of personal data to that which is "adequate, relevant, and limited to what is reasonably necessary" for the relevant purposes).
2. Purpose specification (specifying the "express purposes for which personal data are collected and processed").
3. Secondary use (not processing personal data for purposes "not reasonably necessary to or compatible with the specified purposes for which the personal data are processed" unless the Consumer has consented to such processing).
4. Transparency (providing Consumers with a "reasonably accessible, clear, and meaningful privacy notice" that includes, among other things, the categories of collected data, how [C]onsumers may exercise their rights, and the categories of personal data that the controller shares with third parties).
5. Care (taking "reasonable measures to secure personal data during both storage and use from unauthorized acquisition").
6. Non-discrimination (not processing personal data in violation of laws that "prohibit unlawful discrimination against [C]onsumers").

A controller may not share personal information with a processor until it has executed a contract with the processor that includes (i) instructions governing the nature and purpose of the processing to be performed; (ii) the type of personal data to be processed and the duration of the processing; (iii) the processing obligations listed as (1)-(6) above; (iv) requirements for return or destruction of the personal data upon completion of the processor's services; (v) obligations for the processor to assist the controller in responding to Consumer requests and otherwise complying with the CPA; and (vi) mandates for the processor to undergo audits and inspections to confirm its compliance with the CPA's standards.

With respect to "sensitive data," the Act prohibits *any* processing without first obtaining the consent of the Consumer to whom the data pertains (or, when processing personal data concerning a known child, consent from the child's parent or legal guardian). Such consent must be clear, informed and unambiguous. "Sensitive data" is personal data that reveals racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data that

may be processed to identify an individual, and any personal data of a known child.

In addition, as under the VCDPA, controllers must perform data protection assessments for processing activities that present "a heightened risk of harm to a [C]onsumer." Activities that present such a risk include, among other things, selling personal data, processing sensitive data, and processing personal data for purposes of targeted advertising or for profiling that presents a "reasonably foreseeable risk" of unfair or deceptive treatment of, or disparate impact on, "intrusion upon the solitude or seclusion, or the private affairs or concerns, of [C]onsumers if the intrusion would be offensive to a reasonable person." Data protection assessments must balance the benefits from processing to the controller against the potential risks to the rights of the Consumer associated with such processing and must be made available to the attorney general upon request.

What Rights Can Consumers Exercise Under the CPA?

As do the CCPA, GDPR and VCDPA, the CPA grants Consumers a number of rights with respect to their data, including the right to access their personal data and to have the data corrected, deleted, and/or provided in a portable format for transmission to others. And, also like the CCPA and VCDPA, the CPA gives Consumers the right to opt out of selling of their personal data or the use of their data for targeted advertising or profiling.

The Act provides that on July 1, 2024, controllers that process personal data for the purposes of targeted advertising or the sale of personal data must provide a "universal opt-out mechanism" with which Consumers may opt-out. The attorney general must also adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a Consumer's unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data.

What Does the CPA Portend?

As indicated by the actions of California, Virginia and Colorado, as well as the legislatures in a number of other states including New York and Washington, consumer privacy is a growing concern for legislators and their constituents. Privacy regulation is expanding in scope and detail and this trend is much more likely to accelerate than to abate. Companies that have needs to process personal information beyond that of their employees or representatives of their business partners or vendors should be considering the full scope of those needs and what the legislative trends indicate about the future ability to fulfill them. Is now a time to advocate for or against other states' adoption of laws similar to the CPA? Can a push be made for Congress to step up sooner than later at least to set guideposts for processing of personal information that has social benefits? What practical steps toward compliance with the existing state laws should be taken now, well ahead of applicable compliance deadlines? By examining these questions and considering how business models and industries might need to adapt in response to future legislative developments like the CPA, organizations will be better prepared to navigate a privacy regulatory landscape that continues to grow increasingly more complex.

[1] *See* Arnold &Porter advisories on the CPRA and VCDPA.

Joint Press Release

July 13, 2021

Agencies request comment on proposed risk management guidance for third-party relationships

Board of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation

Office of the Comptroller of the Currency

For release at 2:30 p.m. EDT

Share

The federal bank regulatory agencies today requested public comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships, including relationships with financial technology-focused entities. The proposed guidance is intended to assist banking organizations in identifying and addressing the risks associated with third-party relationships and responds to industry feedback requesting alignment among the agencies with respect to third-party risk management guidance.

Banking organizations that engage third parties to provide products or services or to perform other activities remain responsible for ensuring that such outsourced activities are conducted in a safe and sound manner and in compliance with all applicable laws and regulations, including consumer protection laws.

Comments must be received within 60 days of the proposed guidance's publication in the *Federal Register*.

Proposed Interagency Guidance on Third-Party Relationships: Risk Management (PDF)

Board Memo (PDF)

Media Contacts:

Federal Reserve Board	Chelcee Stearns	202-452-5228
FDIC	LaJuan Williams-Young	202-898-3876
OCC	Stephanie Collins	202-649-6870

Related Content

Board Votes

Last Update: July 13, 2021

Arnold & Porter

July 28, 2021

On CCPA's First Anniversary, California AG Details Enforcement Actions, Consumer Notice Tool

Enforcement Edge: Shining Light on Government Enforcement

By Ryan Tanny Kang, Alex Altman, Nancy L. Perkins, Jami Vibbert

On July 19, 2021, California Attorney General Rob Bonta issued a press release highlighting the first anniversary of the date on which the California Consumer Privacy Act (CCPA) became enforceable.

The CCPA vests the AG with the authority to enforce its provisions, limiting private rights of action to security violations involving particularly sensitive personal information. Before commencing a formal action against a business subject to the CCPA, the AG must give the business notice and 30 days in which to cure the alleged violations. AG Bonta stated that 75 percent of all companies that received notices of alleged CCPA violations in the past year responded with amended practices within the allotted 30-day cure period and that the remaining 25 percent were either currently within their 30-day cure window or under active investigation.

In a press conference that same day, AG Bonta touted the effectiveness of such cure notices, stating that "[w]e've sent quite a few [notices], but the good news is when we send out notices to cure we get a response. . . . We're not seeing resistance, stiff-arming or foot-dragging." Notably, despite early speculation that enforcement would target specific industries or prominent businesses, notices to cure have been sent to a broad spectrum across many industries, including data brokers, marketing companies, businesses handling children's information, media outlets, and online retailers.

AG Bonta also announced the availability of a new Consumer Privacy Tool that allows individual consumers to draft and send notices to businesses regarding their CCPA violations. At the moment, the tool is "limited to drafting notices to businesses that do not post an easy-to-find 'Do Not Sell My Personal Information' link on their website." Although consumers cannot, as noted, take action to enforce the CCPA other than in limited security violation cases, the AG suggested that he may treat a consumer's notice of violation of the "Do Not Sell" link requirement as triggering the 30-day cure period for his own action based on such violation.

Businesses subject to the CCPA, therefore, should take steps to receive and respond to notices issued by consumers using the Consumer Privacy Tool. This tool, and the AG's active issuance of notices of alleged violations, are signs that the statute has teeth that will continue to bite.

Regulatory Notice 21-29

Vendor Management and Outsourcing

FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors

Summary

Member firms are increasingly using third-party vendors to perform a wide range of core business and regulatory oversight functions. FINRA is publishing this *Notice* to remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures (WSPs), for any activities or functions performed by third-party vendors, including any sub-vendors (collectively, Vendors) that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. This *Notice* reiterates applicable regulatory obligations; summarizes recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management.

This *Notice*—including the "Questions for Consideration" below—does not create new legal or regulatory requirements or new interpretations of existing requirements. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their Vendor management practices. FINRA recognizes that there is no one-size-fits-all approach to Vendor management and related compliance obligations, and that firms use risk-based approaches that may involve different levels of supervisory oversight, depending on the activity or function Vendors perform. Firms may consider the information in this *Notice* and employ the practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the firm's size and business model.

FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships. FINRA will monitor this proposed guidance and consider comparable action, where appropriate.

August 13, 2021

Notice Type

- Guidance

Suggested Routing

- Business Senior Management
- Compliance
- Cyber
- Information Technology
- Legal
- Operations
- Risk Management

Key Topics

- Business Continuity Planning (BCP)
- Cybersecurity
- Due Diligence
- Internal Controls
- Supervision
- Vendor Management

Referenced Rules & Notices

- FINRA Rule 1220
- FINRA Rule 3110
- FINRA Rule 4311
- FINRA Rule 4370
- Regulation S-P Rule 30
- Notice to Members 05-48

Questions or comments concerning this *Notice* may be directed to:

- Ursula Clay, Senior Vice President and Chief of Staff, Member Supervision, at 646-315-7375 or Ursula.Clay@finra.org;
- Sarah Kwak, Associate General Counsel, Office of General Counsel, at 202-728-8471 or Sarah.Kwak@finra.org;
- Michael MacPherson, Senior Advisor, Member Supervision, at 646-315-8449 or Michael.MacPherson@finra.org.

Background and Discussion

In 2005, FINRA published *Notice to Members 05-48* (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers), which identified a number of common activities or functions that member firms frequently outsourced to Vendors, including "accounting/finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (*e.g.,* statement production, disaster recovery services, etc.) and administration functions (*e.g.,* human resources, internal audits, etc.)." Since that time, including during the COVID-19 pandemic, member firms have continued to expand the scope and depth of their use of technology and have increasingly leveraged Vendors to perform risk management functions and to assist in supervising sales and trading activity and customer communications.[1]

FINRA encourages firms that use—or are contemplating using—Vendors to review the following obligations and assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Supervision	FINRA Rule 3110 (Supervision) requires member firms to establish and maintain a system to supervise the activities of their associated persons that is reasonably designed to achieve compliance with federal securities laws and regulations, as well as FINRA rules, including maintaining written procedures to supervise the types of business in which it engages and the activities of its associated persons. This supervisory obligation extends to member firms' outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and WSPs pursuant to FINRA Rule 3110.[2] *Notice* 05-48 reminds member firms that "outsourcing an activity or function to ... [a Vendor] does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and [FINRA] and MSRB rules regarding the outsourced activity or function." Further, *Notice* 05-48 states that if a member outsources certain activities, "the member's supervisory system and [WSPs] must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and [FINRA] rules." FINRA expects member firms to develop reasonably designed supervisory systems appropriate to their business model and scale of operations that address technology governance-related risks, such as those inherent in firms' change and problem-management practices. Failure to do so can expose firms to operational failures that may compromise their ability to serve their customers or comply with a range of rules and regulations, including FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and books and records requirements under 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Registration	*Notice* 05-48 reminds firms that, "in the absence of specific [FINRA] rules, MSRB rules, or federal securities laws or regulations that contemplate an arrangement between members and other registered broker-dealers with respect to such activities or functions (*e.g.,* clearing agreements executed pursuant to [FINRA Rule 4311]), any third-party service providers conducting activities or functions that require registration and qualification under [FINRA] rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications." Accordingly, firms must review whether Vendors or their personnel meet any registration requirements under FINRA Rule 1220 (Registration Categories), as well as whether employees of the member firm are "Covered Persons" under the Operations Professional registration category pursuant to FINRA Rule 1220(b)(3), due to their supervision of "Covered Functions" executed by a Vendor or because they are authorized or have the discretion materially to commit the member firm's capital in direct furtherance of a Covered Function or to commit the member firm to any material contract or agreement (written or oral) with a Vendor in furtherance of a Covered Function.
Cybersecurity	SEC Regulation S-P Rule 30 requires broker-dealers to have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are 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. FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations. FINRA reminds member firms to review core principles and effective practices for developing such programs and controls, including Vendor management, from our Report on Cybersecurity Practices (2015 Report) and the Report on Selected Cybersecurity Practices – 2018 (2018 Report), as well as other resources included in the Appendix to this *Notice*.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Business Continuity Planning (BCP)	FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires member firms to create and maintain a written BCP with procedures that are reasonably designed to enable member firms to meet their existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption. The elements of each member firm's BCP—including their use of Vendors—can be "flexible and may be tailored to the size and needs of a member [firm]," provided that minimum enumerated elements are addressed. As a reminder, member firms must review and update their BCPs, if necessary, in light of changes to member firms' operations, structure, business or location.

Exam Findings and Observations

The 2021 Report on FINRA's Exam and Risk Monitoring Program, as well as our 2019, 2018 and 2017 Reports on FINRA Examination Findings, addressed compliance deficiencies (discussed below) arising from firms' Vendor relationships.

Cybersecurity and Technology Governance

- **Vendor Controls** – Firms failed to document or implement procedures to: 1) evaluate prospective and, as appropriate, test existing Vendors' cybersecurity controls, or 2) manage the lifecycle of their engagement with Vendors (*i.e.,* from onboarding, to ongoing monitoring, through off-boarding, including defining how Vendors dispose of customer non-public information).
- **Access Management** – Firms failed to implement effective Vendor access controls, including: limiting and tracking Vendors with administrator access to firm systems; instituting controls, such as a "policy of least privilege," to grant system and data access to Vendors only when required and removing access when no longer needed; or implementing multi-factor authentication for Vendors and contractors.
- **Inadequate Change Management Supervision** – Firms did not perform sufficient supervisory oversight of Vendors' application and technology changes impacting firm business and compliance processes, especially critical systems (including upgrades, modifications to or integration of member firm or Vendor systems). These oversight failures led to violations of regulatory obligations, such as those relating to data integrity, cybersecurity, books and records and confirmations.
- **Limited Testing of System Changes and Capacity** – Firms did not adequately test changes to, or system capacity of, order management, account access and trading algorithm systems, and thus failed to detect underlying malfunctions or capacity constraints.
- **Data Loss Prevention Programs** – Vendors did not encrypt confidential firm and customer data (*e.g.,* Social Security numbers) stored at Vendors or in transit between firms and Vendors.

FINRA Disciplined Firms Whose Vendors Did Not Implement Technical Controls

FINRA disciplined certain firms for violations of Regulation S-P Rule 30 and FINRA Rules 3110 and 2010 for failing to maintain adequate procedures and execute supervisory oversight to protect the confidentiality of their customers' nonpublic personal information, including, for example, where:

- a Vendor exposed to the public internet the firms' purchase and sales blotters, which included customers' nonpublic personal information (*e.g.,* names, account numbers, and social security numbers).
- a Vendor did not configure its cloud-based server correctly, install antivirus software, and implement encryption for the firm's account applications and other brokerage records containing customers' nonpublic personal information. As a result, foreign hackers successfully accessed the cloud-based server and exposed firm customers' nonpublic personal information.

Books and Records

- Firms failed to perform adequate due diligence to verify Vendors' ability to maintain books and records on behalf of member firms in compliance with Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and FINRA Rule Series 4510 (Books and Records Requirements) (collectively, Books and Records Rules).
- Firms failed to confirm that service contracts and agreements comply with requirements to provide notification to FINRA under Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected electronic storage media (ESM) used to maintain firms' books and records meets the conditions of Exchange Act Rule 17a-4(f)(2) and a third-party attestation as set forth in Exchange Act Rule 17a-4(f)(3)(vii) (collectively, ESM Notification Requirements).
- Firms did not confirm that Vendors complied with contractual and regulatory requirements to maintain (and not delete, unless otherwise permitted) firms' books and records.[3]

Consolidated Account Reports (CARs) – Firms did not have processes in place to evaluate how they and registered representatives selected CARs Vendors; set standards for whether and when registered representatives were authorized to use Vendor-provided CARs; determine when and how registered representatives could add manual entries or make changes to CARs; test or otherwise validate data for non-held assets reported in CARs (or clearly and prominently disclose that the information provided for those assets was unverified); and maintain records of CARs.[4]

Fixed Income Mark-up Disclosure – Firms failed to test whether Vendors identified the correct prevailing market price (PMP) from which to calculate mark-ups and mark-downs (for example, instead of using the prices of a member firm's own contemporaneous trades, which were available to be considered, a Vendor's program incorrectly identified PMPs using lower levels of the "waterfall" as described in FINRA Rule 2121.02 (Additional Mark-Up Policy For Transactions in Debt Securities, Except Municipal Securities) or MSRB Rule G-30.06 (Mark-Up Policy).

FINRA Disciplined Firms for Books and Records Violations Resulting from Vendor Deficiencies

FINRA disciplined firms for violations of Books and Records rules and related supervisory obligations involving Vendors, including, but not limited to, failing to preserve and produce business-related electronic communications (including emails, social media, texts, instant messages, app-based messages and video content) due to:

- Vendors' system malfunctions;
- Vendors' data purges after termination of their relationship with firms;
- Vendors failing to correctly configure default retention periods resulting in inadvertent deletions of firm electronic communication for certain time periods;
- Vendors' system configurations making deleted emails unrecoverable after 30 days;
- Vendors failing to provide non-rewriteable, non-erasable storage; and
- Firms failing to establish an audit system to account for Vendors' preservation of emails.

Questions for Consideration

The following questions may help firms evaluate whether their supervisory control system, including WSPs, adequately addresses issues and risks relating to Vendor management. The questions—which address both regulatory requirements and effective practices FINRA has observed firms implement—focus on four phases of a firm's outsourcing activities:

- deciding to outsource an activity or function,
- conducting due diligence on prospective Vendors,
- onboarding Vendors, and
- overseeing or supervising outsourced activities or functions.

As noted above, firms should not infer any new obligations from the questions for consideration. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their vendor management practices. FINRA is sharing this information for firms' consideration only.

Firms may wish to evaluate the questions presented below in the context of a risk-based approach to Vendor management in which the breadth and depth of their due diligence and oversight may vary based on the activity or function outsourced to a Vendor. Factors firms may take into consideration include, but are not limited to:

- Will the Vendor be handling sensitive firm or customer non-public information?
- What would be the extent of the potential damage if there is a security breach (*e.g.,* number of customers or prospective customers impacted)?
- Is the Vendor performing a business-critical role or fulfilling a regulatory requirement for the firm?
- What is the reputation and history of the Vendor, including the representations made and information shared on how the Vendor will secure the firm's information?

I. Decision to Outsource

A decision to outsource an activity or function may depend, in part, on whether the firm has an adequate process to make that determination and then to supervise that outsourced activity or function. The following considerations may help firms address those threshold questions.

- Does your firm have a process for its decision-making on outsourcing, including the selection of Vendors?
- Does your firm's supervisory control system address your firm's outsourcing practices, including your firm's approach to Vendor due diligence?
- Does your firm identify risks that may arise from outsourcing a particular activity or function and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?
- Does your firm engage key internal stakeholders (*e.g.,* Compliance, Legal, IT or Risk Management) relevant to, and with the requisite experience to assess, the outsourcing decision?

II. Due Diligence

Once a member firm decides to outsource an activity or function, it may want to consider some or all of the following questions in evaluating and selecting potential Vendors:

- Due Diligence Approach
  - What factors does your firm consider when conducting due diligence on potential Vendors? These may include, but are not limited to: a Vendors' financial condition, experience and reputation; familiarity with regulatory requirements, fee structure and incentives; the background of Vendors' principals, risk management programs, information security controls, and resilience.

- If a potential Vendor will be performing a function that is subject to regulatory requirements, how does your firm evaluate whether the Vendor has the ability to comply with applicable regulatory requirements and undertakings (*e.g.,* Book and Records rules, including ESM Notification Requirements)?
- Does your firm consider obtaining evaluations of prospective Vendors' SSAE 18, Type II, SOC 2 (System and Organization Control) reports (if available)? If so, who reviews the evaluations and how does your firm follow up on any identified concerns, including, for example, those related to cybersecurity?
- Does your firm take a risk-based approach to vendor due diligence? Does the scope and depth of your firm's due diligence reflect the degree of risk associated with the activities or functions that will be outsourced?
- Does your firm evaluate the impact to your customers or firm if a Vendor fails to perform, for example, by not fulfilling a regulatory obligation? What measures can your firm put in place to mitigate that risk?
- Does your firm assess the BCPs of prospective Vendors that would perform critical business, operational, risk management or regulatory activities or functions?
- If a Vendor will likely be conducting activities or functions that require registration under FINRA rules, does your firm have a process for determining whether the Vendor's personnel will be appropriately qualified and registered?
- Does your firm evaluate Vendors' controls and due diligence of Vendors' sub-contractors, particularly if the sub-contractor may have access to sensitive firm or customer non-public information or critical firm systems?
- Does your firm include individuals with the requisite expertise and experience in the due diligence process—including with respect to cybersecurity, information technology, risk management, business functions and relevant regulatory obligations—to effectively evaluate potential Vendors? How does your firm handle instances where your firm does not have the expertise or experience in-house?
- Does your firm document its due diligence findings?

- **Conflicts of Interest –** Does your firm put controls in place to mitigate potential conflicts of interest in the Vendor selection process? For example:
  - Does your firm require staff involved in its Vendor selection processes to disclose any personal relationship with the Vendor? If so, what steps does your firm take to assess whether that relationship may influence the choice of Vendor?
  - Does your firm allow staff to receive compensation or gifts from potential or current Vendors, which could influence the decision to select, or maintain a relationship with, a particular Vendor?

- **Cybersecurity**

Does your firm assess the Vendors' ability to protect sensitive firm and customer non-public information and data? Does your firm have access to expertise to conduct that assessment? (See also question, above, regarding SSAE 18 Type II, SOC 2 reports.)

III. Vendor Onboarding

After completing due diligence and selecting a Vendor, firms may wish to consider putting in place a written contract with the Vendor that addresses, among other things, both the firm's and the Vendor's roles with respect to outsourced regulatory obligations.

- **Vendor Contracts**
  - Does your firm document relationships with Vendors in a written contract, and if not, under what circumstances?
  - Do your firm's contracts address, when applicable, Vendors' obligations with respect to such issues as:
    - documentation evidencing responsible parties' and Vendors' compliance with federal and state securities laws and regulations and FINRA rules (*e.g.,* retention period required for preservation of firm records);
    - non-disclosure and confidentiality of information;
    - protection of non-public, confidential and sensitive firm and customer information;
    - ownership and disposition of firm and customer data at the end of the Vendor relationship;
    - notification to your firm of cybersecurity events and the Vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues;
    - Vendor BCP practices and participation in your firm's BCP testing, including frequency and availability of test results;
    - disclosure of relevant pending or ongoing litigation;
    - relationships between Vendors, sub-contractors and other third-parties;
    - firm and regulator access to books and records; and
    - timely notification to your firm of application or system changes that will materially affect your firm.
  - Do your firm's contracts with Vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?

- **Features and Default Settings of Vendor Tools**
  - Does your firm review, and as appropriate adjust, Vendor tool default features and settings, such as to limit use of communication tools to specific firm-approved features (*e.g.,* disabling a chat feature, or reviewing whether the communications are being captured for supervisory review), to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?

IV. Supervision

Member firms have a continuing responsibility to oversee, supervise and monitor the Vendor's performance of the outsourced activity or function. Firms may wish to consider the following potential steps in determining how they fulfill this supervisory obligation:

- Obtaining representations from the Vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;
- Requiring Vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;
- Going onsite to Vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;
- Monitoring and assessing the accuracy and quality of the Vendor's work product;
- Remaining aware of news of Vendor deficiencies and investigating whether they are indicative of a problem with an activity or function the Vendor is performing for your firm;
- Investigating customer complaints that may be indicative of issues with a Vendor and exploring whether there are further-reaching impacts; and
- Training staff to address and escalate red flags at your firm that a Vendor may not be performing an activity or function adequately, such as not receiving confirmation that a Vendor task was completed.

In addition to the above, firms may want to consider asking the following questions, where applicable, with respect to more specific aspects of their supervisory system.

- **Supervisory Control System**
  - Does your firm monitor Vendors (for example, by reviewing SOC 2 reports) and document results of its ongoing supervision, especially for critical business or regulatory activities or functions?
  - Do your firm's WSPs address roles and responsibilities for firm staff who supervise Vendor activities?
  - Does your firm periodically review and update its Vendor management-related WSPs to reflect material changes in the firm's business or business practices?

- **Business Continuity Planning**
  - Does your firm's business continuity planning and testing include Vendors? If so, what are the testing requirements for Vendors and how often are such tests performed? How do these tests inform your firm's overall BCP?
  - Does your firm have contingency plans for interruptions or terminations of Vendor services?
  - If there is a disaster recovery event, has your firm assessed whether the Vendor will have sufficient staff dedicated to your firm?
- **Cybersecurity and Technology Change Controls**
  - **Access Controls**
    - Does your firm know which Vendors have access to: (1) sensitive firm or customer non-public information and (2) critical firm systems?
    - Does your firm implement access controls through the lifecycle of its engagement with Vendors, including developing a "policy of least privilege" to grant Vendors system and data access only when required and revoke it when no longer needed and upon termination?
    - Has your firm considered implementing multi-factor authentication for Vendors and, if warranted, their sub-contractors?
  - **Cybersecurity Events and Data Breaches**
    - Does your firm conduct independent, risk-based reviews to determine if Vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the Vendors' response to such events?
    - If a cybersecurity breach occurred at your firm's Vendor, was your firm notified and, if so, how quickly? Did your firm follow its incident response plan for addressing such breaches?
  - **Technology Change Management**
    - If applicable, how does your firm become aware of, evaluate and, as appropriate, test the impact of changes Vendors make to their applications and systems, especially for critical applications and systems?

FINRA Disciplined Firms for Failure to Supervise Vendors

FINRA disciplined certain firms that violated FINRA Rules 2010 and 3110, among other rules, when they failed to establish and maintain supervisory procedures for their Vendor arrangements reasonably designed to:

- Review, verify or correct vendor-provided expense ratio and historical performance information for numerous investment options in defined contribution plans (*i.e.,* retirement plans), causing firms' customer communications to violate FINRA Rule 2210;
- Oversee, monitor and evaluate changes and upgrades to automated rebalancing and fee allocation functions outsourced to a Vendor for wealth management accounts custodied at the firm, causing errors and imposing additional fees to customer accounts;
- Review, test or verify the accuracy and completeness of data feeds from Vendors that failed to identify the firm's prior role in transactions for issuers covered by firm research reports, resulting in violations of then NASD Rule 2711(h) and 2241(c) when the firm failed to make required disclosures in its equity research reports regarding its status as a manager or a co-manager of a public offering of the issuer's equity securities; and
- Confirm the accuracy and completeness of information provided by Vendors to regulators, including FINRA, both in response to specific requests and as part of regular trade and other reporting obligations, causing inaccurate responses and misreported transactions, order reports, route reports and reportable order events.

Conclusion

As noted throughout this *Notice*, the requirement that a member firm maintain a reasonably designed supervisory system and associated WSPs extends to activities or functions it may outsource to a Vendor. While the manner and frequency by which these activities or functions are overseen is determined by the member firm, and is dependent on a number of factors, the information in this *Notice* is intended to provide firms with ideas and questions they can use to build and evaluate the sufficiency of their Vendor management protocols. Additional helpful resources can be found in the Appendix.

Endnotes

1. *See Regulatory Notice* 20-42 (FINRA Seeks Comment on Lessons from the COVID-19 Pandemic); COVID-19/Coronavirus Topic Page; *Regulatory Notice* 20-16 (FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic); and *Regulatory Notice* 20-08 (Pandemic-Related Business Continuity Planning, Guidance and Relief).

2. *See also* NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance, which clarified that *Notice 05-48* was issued to provide guidance on a member's responsibilities if the member outsources certain activities and was not intended to address the appropriateness of outsourcing a particular activity or whether an activity could be outsourced to a non-broker-dealer third-party service provider.

3. *See Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services).

4. *See Regulatory Notice* 10-19 (FINRA Reminds Firms of Responsibilities When Providing Customers with Consolidated Financial Account Reports).

Appendix – Additional Resources

Regulatory Notices and Guidance

- **Outsourcing and Vendor Management**
  - *Regulatory Notice* 11-14 (FINRA Requests Comment on Proposed New FINRA Rule 3190 to Clarify the Scope of a Firm's Obligations and Supervisory Responsibilities for Functions or Activities Outsourced to a Third-Party Service Provider)
  - *Notice to Members* 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Providers), and NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance
  - *Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services)
- **Cybersecurity**
  - Report on Selected Cybersecurity Practices – 2018
  - Report on Cybersecurity Practices – 2015

FINRA Examination Findings Reports

- 2021 Report on FINRA's Examination and Risk Monitoring Program
- 2019 Report on FINRA Examination Findings and Observations
- 2018 Report on FINRA Examination Findings
- 2017 Report on FINRA Examination Findings

Tools

- Core Cybersecurity Controls for Small Firms
- Small Firm Cybersecurity Checklist
- Outsourcing and Vendor Management section of the Peer-2-Peer Compliance Library
  - Outsourcing Due Diligence Form
  - Sample Vendor On-Site Audit Template
  - Sample Vendor Questionnaire
  - Third Party Matrix
  - Third Party Vendor Contracts Sample Language
  - Vendor Management Considerations
  - Vendor Security Questionnaire

Arnold & Porter

September 13, 2021

Cybersecurity Compliance Is More Than a Policy, Part 1: What Advisers and Brokers Can Do to Ensure Policies Are Followed With Action

Enforcement Edge: Shining Light on Government Enforcement

By Alyssa T. Gerstner, Kathleen Reilly, Jami Vibbert, David F. Freeman, Jr., Ellen Kaye Fleishhacker

On August 30, the US Securities and Exchange Commission (SEC) announced three cybersecurity-related enforcement actions relating to eight different firms. The actions arose from what appear to be routine examinations of registered investment advisers and broker-dealers. This post provides some high-level takeaways for companies to consider in the wake of these actions. Tomorrow, we will dive into the actions and rules violated.

As brief background, the SEC's examination priorities have included a focus on cyber- and information security since at least 2015. As Kristina Littman, chief of the SEC's cyber unit, warned in the press release announcing the actions: "It is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks." Moreover, beyond the SEC, other regulators are focused on companies' cybersecurity policies. For example, FINRA recently published guidance on cloud computing and vendor management, which reminds firms to include vendor management in their "reasonably designed cybersecurity programs and controls consistent with their risk profile, business model, and scale of operations."

In the wake of these recent orders, and the continued focus of regulators in this area, companies would be well-served to review and update their policies and procedures relating to information security, consider whether technology enhancements are required (and swiftly implement them), and ensure that individuals are complying. Additionally, as one of the orders illustrates, companies cannot merely send out form notifications in the event of a cybersecurity breach, as they may prove to be inaccurate especially if they are sent out at different times. Instead, companies should re-evaluate communications each time they are sent in order to make sure that they accurately reflect both the timing of when an issue was identified and the nature of what occurred.

As this area continues to be a focus for all regulators, the costs of compliance can seem daunting. Given this, registered investment advisers and broker-dealers should consider taking the following steps now:

- Confirm that your written cyber- and information security policies are reasonably designed and tailored to the needs and sophistication of your business, and that sufficient and reasonable safeguards are in place with respect to protecting personal information. What is considered sufficient and reasonable in the realm of information security constantly evolves. This may require more frequent policy reviews than those that occur in other areas, especially if you experience any type of cybersecurity attack or breach.
- Confirm that your policies and procedures have been implemented, which will likely require frequent discussion and contact with your Information Technology and Data Security teams.
- Confirm that, in addition to your employees, any independent contractors and individuals located offshore are implementing your policies and procedures.
- Conduct a cybersecurity risk assessment to ensure that you are meeting all of your legal requirements to protect data under the SEC Safeguards Rule and otherwise.
- Implement the findings from the risk assessment! If there is a determination not to implement findings from the risk assessment, document the reasons why not and the alternative measure(s) taken.
- Ensure written policies and procedures are robust and updated and include new findings from the assessment.
- Practice your incident response process. Practice makes perfect, and failing to practice can lead to failure to comply in the moments

when faced with a real crisis (ransomware or otherwise).

Check back tomorrow for an in-depth discussion of the precise rules implicated by these orders. For questions about requirements for cybersecurity incident notices, please see our previous Advisory discussing banking agencies' updated vendor management guidance or contact the authors of this post.

Arnold & Porter

September 14, 2021

Cybersecurity Compliance Is More Than a Policy, Part 2: SEC Cyber Enforcement Actions Remind Advisers and Brokers That Policies Must Be Followed With Action

Enforcement Edge: Shining Light on Government Enforcement

By Alyssa T. Gerstner, Kathleen Reilly, Jami Vibbert, David F. Freeman, Jr., Ellen Kaye Fleishhacker

As we discussed yesterday, this post provides more background about the federal government's recently announced cybersecurity-related enforcement actions, which arise out of what appear to be routine Securities and Exchange Commission (SEC) examinations of registered investment advisers and broker-dealers. As we noted previously, the SEC enforcement actions serve as a reminder that regulators at every level are focused on the measures that companies take to prevent, identify, and address cyber- and information security threats. Additionally, regulators are closely reading the language of any notification sent to impacted individuals for accuracy.

The three orders relate to eight firms: Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, Cetera Investment Advisers LLC (collectively, the Cetera Entities); Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. (collectively, Cambridge); and KMS Financial Services Inc. (KMS). In settling the actions without admitting or denying the findings (except as to jurisdiction and the subject matter of the proceedings), the eight firms collectively paid penalties totaling $750,000.

All of the settled orders assert violations of Rule 30(a) of Regulation S-P, known as the Safeguards Rule, for failing to properly protect customer information. Specifically, the SEC alleges that the firms' failure to adopt and follow adequate written cybersecurity policies and procedures led to email account takeovers, primarily of the cloud-based email accounts of independent contractors, exposing personal information for thousands of customers and clients.

In addition, the order against the Cetera Entities asserted violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 for failing to properly notify clients in connection with a security breach. Although the firms had identified the breach and properly notified most of those impacted, the SEC took issue with the use of a template letter notification for approximately 220 customers whom the firms notified several months later without updating the time when the breach was identified.

Safeguards Rule Violations

The Safeguards Rule requires every broker-dealer and investment advisor registered with the Commission to adopt written policies and procedures that are 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. In each of the orders, the SEC criticized the companies' failures to tailor the security tools or procedures already in place to meet the needs of the businesses.

For example, the Cetera Entities had a written policy requiring multi-factor authentication (MFA) "whenever possible" but, according to the SEC, failed to enforce it. The SEC asserts this enforcement failure resulted in the takeover by unauthorized third parties of over 60 personnel email accounts and the exposure of over 4,388 customers' personal information between 2017 and 2020. Following an initial attack in late 2017, the Cetera Entities had activated MFA for its employees' cloud-based accounts and began a process of activating MFA for contractor representatives' email accounts. According to the SEC, there were still over 1,500 email accounts of contractor representatives and their employees without MFA in December 2018. Nor did the company implement MFA for any offshore contractor email accounts until the end of 2019. The SEC found that these actions were a willful violation of the Safeguards Rule.

The other two orders detailed similar "willful" violations of the Safeguards Rule. Cambridge violated the rule for failing to implement a

policy that mandated MFA for all employees and independent representatives, even though Cambridge's policies appear to have suggested MFA implementation. Specifically, the SEC asserts that Cambridge provided its independent representatives with cybersecurity guidance, including policies and procedures, but each representative was responsible for implementing the guidance. Following several instances of email account takeovers from 2018 to 2021, Cambridge suspended or reset the affected accounts, but did not require any other enhanced security measures and did not enforce the MFA requirement until 2021. Similarly, KMS discovered compromised email accounts in November 2018. While KMS reset the affected emails and enabled MFA, the SEC detailed a Safeguards Rule violation because KMS did not adopt written policies and procedures requiring such security measures until May 2020 and did not implement those changes firmwide until August 2020.

Notice Violation

The SEC also found the Cetera Entities violated Section 206(4) of the Advisers Act and Rule 206(4)-7 by failing to adopt and implement reasonably designed policies and procedures regarding review of communications to advisory clients, which resulted in misleading template language. As noted above, the SEC took issue with notification language that stated identification of the breach(es) occurred two months prior and referred to the breach(es) as "recent." Identification had occurred six months prior, and the date set forth in the notice was not the date of the breach(es), but when the firm completed its review of the compromised accounts. According to the SEC, the customers therefore would not know to look for any potential misuse of personal information beyond the two months indicated, defeating the purpose of the notification.

Cybersecurity continues to be an area of focus for all regulators. These orders serve to remind firms to review and update their policies and procedures relating to information security, consider whether technology enhancements are required (and swiftly implement them), and ensure that individuals are complying. For a discussion of specific steps firms could consider taking to ensure cybersecurity compliance, please refer back to our prior post or contact the authors of this post.

Arnold & Porter

Who We Are

100+ Years of business acumen with a practical, forward-looking, results-driven approach

13 Offices in the US, Europe, and Asia

123 Attorneys ranked in *Chambers USA*, *UK*, *Global, Europe, Latin America*, and *Asia-Pacific*

94 Attorneys who have held senior positions in US and European governments and international organizations

133 Fortune 250 companies have chosen Arnold & Porter as outside counsel

What We Offer

- Nearly 1,000 lawyers with an unyielding commitment to excellence and professionalism
- Exceptional depth of talent across the litigation, regulatory and transactional spectrum
- Leading multidisciplinary practices in the life sciences and financial services industries
- Among the broadest and deepest service offerings in the two key US legal markets of New York and Washington, DC
- Broad reach across geographic, cultural, commercial, and ideological borders
- One of the world's leading pro bono programs, with our attorneys performing more than 121,000 hours of pro bono work in 2020

Principal Areas of Practice

Litigation

- Anti-Corruption
- Antitrust/Competition Litigation
- Appellate & Supreme Court
- Class Actions
- Commercial Litigation
- Consumer Protection and Advertising
- Crisis Management & Strategic Response
- Environmental Enforcement and Toxic Tort Litigation
- False Claims Act Investigations & Defense
- Intellectual Property
- International Arbitration
- Labor & Employment
- Product Liability Litigation
- Securities Enforcement & Litigation
- White Collar Defense & Investigations

Regulatory

- Antitrust/Competition
- Compliance
- Consumer Product Safety
- Corporate Governance
- Energy Regulatory
- Environmental Compliance and Counseling
- Financial Services
- Global Law and Public Policy
- Government Contracts
- International Trade
- Legislative & Public Policy
- Life Sciences & Healthcare Regulatory
- National Security
- Privacy, Cybersecurity and Data Strategy
- Telecommunications, Internet and Media

Transactional

- Antitrust/Competition Merger Review
- Bankruptcy and Restructuring
- Capital Markets Transactions
- Compensation and Benefits
- Emerging Companies & Venture Capital
- Financial Services Transactions
- Investment Management
- Life Sciences Transactions
- Mergers & Acquisitions
- Private Client Services
- Private Equity
- Real Estate
- Sovereign Finance
- Structured Finance & Derivatives
- Syndicated & Leveraged Finance
- Tax
- Tax-Exempt
- Technology Transactions

arnoldporter.com

Recognition

- *The National Law Journal*'s Appellate Hot List (2010, 2013–2019)
- *The American Lawyer*'s "A-List" has recognized the firm 11 times since 2003
- *Chambers USA* 2020 ranked 92 attorneys as "Leading Individuals"
- *Chambers UK* 2021 ranked 14 attorneys as "Leading Individuals"
- *Chambers Global* 2021 ranked 34 attorneys
- *Chambers Latin America* 2021 named the firm a leading law firm
- *Chambers Asia-Pacific* 2021 ranked five attorneys
- *Global Competition Review* ranked the firm on its 2020 "GCR Global Elite" list
- *FORTUNE* Magazine's "100 Best Companies to Work For" (2003–2010, 2013–2016)
- *VAULT* Guide's "Top 100 Law Firms" (2004–2019)
- *Legal 500 US*, *UK*, *Europe*, *Latin America*, and *Asia* ranked 64 practices and recognized 182 attorneys
- *U.S. News Best Law Firms*–45 national rankings and 103 metropolitan rankings in Chicago, Denver, Houston, Los Angeles, New York, San Francisco, San Jose (Silicon Valley), and Washington, DC

Arnold & Porter combines sophisticated litigation and transactional strength with world-class regulatory expertise to resolve clients' complex and demanding matters.

Diversity & Inclusion

- *Mansfield Plus Certification* (2018, 2019 and 2020)
- "Corporate Equality Index" ranking by the Human Rights Campaign (2006, 2008–2021)
- Yale Law Women's "Top 10 Family Friendly Law Firms" (2006–2018) and "Top 10 Female Friendly Firms" (2018)
- Association of Black Women Attorneys (New York) Diversity Award (2019)
- *Working Mother* Magazine, "100 Best Companies for Working Mothers" (1996–1997, 2001–2002, 2004–2021); "Best Law Firms for Women" (2015–2021); "Best Law Firms for Dads" (2020)
- *Chambers Associate*, "Best Law Firms for Diversity" (2018, 2019)
- *National Asian Pacific American Bar Association*, Law Firm Diversity Award (2018)

Pro Bono

- *National Law Journal* Pro Bono Hot List (2018 and 2020)
- *Financial Times* Award for Innovative Lawyers/ Rule of Law & Access to Justice Category (2018 and 2019)
- *The American Lawyer's* 2021 Pro Bono Scorecard ranked the firm #9 in the US and #4 internationally
- Handled numerous death penalty cases, most recently obtaining the release of a client who had been on death row for 17 years for a murder he did not commit
- In the largest pro bono case in our history (more than 150 timekeepers and 31,000 hours), reached a landmark settlement with the Federal Bureau of Prisons requiring appropriate medical treatment for mentally ill prisoners at the famous "Supermax" prison in Colorado
- Obtained a major victory for Planned Parenthood in a case against anti-abortion activists who engaged in a years-long campaign of fraud and deception to "destroy" the organization
- Legal Services of Eastern Missouri Common Good Award (2020)
- Helped secure a groundbreaking victory on behalf of immigration advocacy groups when the Supreme Court ruled that the US could not add a citizenship question to the 2020 census
- Won a high-profile lawsuit in Pennsylvania that struck down the state's congressional districting map as an unconstitutional partisan gerrymander
- Represented dozens of transgender clients on a variety of issues

Arnold & Porter

Privacy, Cybersecurity & Data Strategy

Arnold & Porter's Privacy, Cybersecurity & Data Strategy practice assists businesses in a wide range of industries in the increasingly challenging task of protecting data consistent with applicable law. We provide data protection counsel to technology and business leaders in connection with the development and use of emerging technology platforms; to clients in the financial services and health industries; and to others involved in e-commerce, software development and deployment, telecommunications, government contracting, and a host of other activities.

Cybersecurity: Our attorneys litigate and counsel on a full range of compliance, regulatory and liability issues related to cybersecurity. We represent government contractors in procurement-related cybersecurity matters and advise on strategy and policy matters involving cyber capabilities, defensive and offensive cyber operations, and vulnerability management.

Investigations and Litigation: We represent clients in litigation and investigations involving privacy, cybersecurity, software, internet security, and other specialized information security matters, including representing clients in two litigations brought under the new privacy right of action in the CCPA, defending privacy and data security allegations before the Federal Trade Commission, state attorneys general, the New York Department of Financial Services, and the Department for Health and Human Services Office for Civil Rights.

Compliance and Regulatory: Our attorneys counsel clients on creating and operationalizing data protection programs globally. We look to create flexible and scalable programs that can efficiently change with the ever-increasing data protection regulations, guidance, and rights regimes. Our experience covers a wide span of data protection laws and includes:

- The California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA) and the California Internet of Things (IoT) law,
- The Children's Online Privacy Protection Act (COPPA),
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- The General Data Protection Regulation (GDPR),
- The Chinese Cybersecurity Act,
- State privacy and data security laws, including the Virginia Consumer Data Protection Act, and
- Data protection laws in most other jurisdictions, including Australia, Brazil, Canada, India, Japan, Mexico, Turkey, and South Africa, with the assistance of local counsel where required.

Our lawyers understand risk and advise on ways to manage and reduce privacy perils. We leverage our skills and experience to provide individualized advice that fits the needs of each organization. With our assistance, our clients can partner with their business stakeholders to create global data strategies that move their businesses toward their data goals while reducing the likelihood of regulatory enforcement and litigation.

Due Diligence and Transactions: We advise on structuring and negotiating complex transactions and conducting privacy and data security diligence. Working alongside our clients, we help shape privacy and cybersecurity strategies and objectives for transactions. As appropriate, we assist in executing those strategies, negotiating the transactions, and documenting them. Our work involves assessing the risk of acquisitions, preparing standard policies to prepare for acquisition, and drafting template contracts and provisions, including data protection/processing agreements and business associate agreements.

Legislative Advocacy: Our Privacy, Cybersecurity & Data Strategy team includes members from the firm's Legislative & Public Policy practice group. They team up with their regulatory, transactional and litigation colleagues on advocacy matters where lobbying is only one of multiple avenues for resolving clients' business issues with public policy elements. We ensure that clients are informed and appropriately anticipate and respond to privacy legislation and regulation developments through advocacy and other activities.

Incident Response and Crisis Management: Our Data Breach Rapid Response team can help address security incidents as quickly and efficiently as possible, fortify defenses and minimize short- and long-term losses. We have a full-service team that integrates our privacy, cybersecurity, white collar, healthcare, financial services, corporate, intellectual property, employment, and litigation professionals. Together, we develop appropriately tailored response plans designed to protect incident victims from the very first instance through each stage of crisis management.