Cybersecurity Law Report
An Acuris company

cslawreport.com

February 10, 2021

FINANCIAL SERVICES REGULATION

What the New Information Security Reporting Standards Mean for Financial Institutions

By Jeffrey Naimon, Morari Shah and James Chou, *Buckley LLP*

Regulators recently proposed new rules that would require banking institutions to notify their primary regulators of some computer-security incidents within 36 hours, and service providers to notify regulated entities as soon as possible of any incident affecting its operations for four hours or longer. The FDIC, OCC and Federal Reserve jointly issued their rulemaking in December 2020, just as the massive SolarWinds hacking incident emerged into public view.

Concerns about the SolarWinds breach, election security, and the increasing digitalization of global markets – accelerated by the COVID-19 pandemic – have reinvigorated government efforts to improve the nation's cybersecurity posture. Congress, adopting several key recommendations of the Cyberspace Solarium Commission, included language in the 2021 National Defense Authorization Act that would expand the scope, authority and resources allocated to the recently established Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security, reflecting the priority of many top federal officials advocating for the government and the private sector to have stronger and more resilient defenses against cyber threats.

In this article, we discuss the regulatory environment, including the NYDFS Cybersecurity Regulation and the proposed expansion to GLBA, and detail the new proposed joint rules and their potential implications.

See "How Will the Biden Administration's Approach to Cybersecurity Impact the Private Sector?" (Dec. 20, 2020).

Part of a Trend

Several laws and regulations direct the financial services industry and others to establish broader cybersecurity standards, and more are likely in the pipeline, and the recently proposed rules by the FDIC, OCC and Federal Reserve are part of a trend that conceives of standards that go beyond traditional data breach reporting and concerns about consumer privacy to encompass a range of threats and issues that potentially affect financial institutions' operations and services, such as ransomware, distributed-denial-of-service attacks, insider threats, system bugs and misconfigurations and supply chain risks.

See "Asset Disposal and Vendor Management Lessons From Morgan Stanley's OCC Settlement" (Nov. 18, 2020).

NYDFS Cybersecurity Regulation

The New York Cybersecurity Regulation, issued by the state's Department of Financial Services

in 2017, represented a significant expansion of cybersecurity regulation, requiring supervised entities to report cybersecurity events within 72 hours, including those that "have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity."

New York's regulation identifies reportable events beyond those that compromise confidentiality and security of PII to include any event that affects the confidentiality, integrity, or availability of information systems, commonly known as the "CIA triad." The regulation also requires regulated entities to maintain, as part of its information security program, a variety of information security standards, such as encryption, multifactor authentication, annual testing and incident-response planning, to which such entities must certify annual compliance.

See "The NYDFS' Cybersecurity Regulation's Third-Party Requirement and Beyond" (Mar. 6, 2019).

GLBA Expansion

The FTC proposed in 2019 to expand the Gramm-Leach-Bliley Act's Safeguards rule by covering the entire range of the CIA triad and impose incident-response standards similar to those of New York. In its current form, the proposal does not mandate additional reporting or notification requirements, merely stating that financial institutions and other regulated entities must consider a wider range of security events in its incident-response planning.

However, since the initial rules were proposed, the FTC has conducted a number of information security workshops to further refine and discuss the impacts of the proposed rules, and, if finalized, financial institutions will likely remain obligated to only report data breaches as required under current state and federal laws.

Service Providers Not Spared

CISA and other government agencies continue to rank supply-chain and third-party risk management as critical challenges to managing cybersecurity risks. The SolarWinds incident and data breaches involving major financial institutions represent two emerging facets of supply-chain risk: (1) the automated processes vendors use to protect information systems, such as automatic updates, may be exploited in ways that can cause major disruptions to agencies and businesses; and (2) third-party insiders with intimate knowledge of a company's information system vulnerabilities can use such knowledge to penetrate systems, with little recourse. These concerns, coupled with the banks' increasing reliance on the technology supply chain, have renewed emphasis on effective third-party risk management.

Consequently, the FTC's proposal would extend beyond regulated entities and affect almost every service provider that delivers critical services to and on behalf of a regulated entity. Such services could include critical cloud or backup support, processors that handle payments or other transactions, and telecommunications services critical to operations.

See "Cybersecurity Resolutions for 2021" (Jan. 13, 2021).

The Proposed Joint Rules and Their Implications

The joint proposed rules would require reporting any event that (1) results in actual or potential harm to the confidentiality, integrity,

or availability of an information system or the information that the system processes, stores, or transmits; or (2) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, if such event rises to the level of a "notification incident." The proposal defines a "notification incident" as any event that the regulated entity believes "in good faith" would result in a material disruption, degradation, or impairment of the ability of the entity to carry out banking operations or business lines, or adversely affect U.S. financial stability.

As proposed, the scope of reporting security events is broad, covering a range of cybersecurity events from degradation of services, corruption of data (regardless of whether it is consumer information) and a breach of confidentiality.

Delineating a maximum tolerable downtime threshold is unprecedented, and by establishing a rigid four-hour limit, service providers likely must revise business-continuity plans and assumptions to comply.

See "How Asset Managers and Others Can Mitigate Pandemic-Related Operational Risks and Maintain Business Continuity" (May 6, 2020).

Expanded Incident Response Plans

The proposed 36-hour and service provider reporting rule greatly affects the level and the scope of planning and execution of an entity's incident-response and business-continuity plans. Smaller banking organizations that generally limit incident-response planning to data breaches or other events that affect the security and confidentiality of non-public personal information must now greatly expand their planning to encompass a range of cybersecurity events.

Service providers that maintain business-continuity and disaster-recovery plans that tolerate downtimes longer than four hours may need to reconsider how they plan and respond to any disaster or disruption of services provided to banking organizations. Service provider agreements may need to be revisited to ensure that effective due diligence is being conducted on a service provider's business-continuity and disaster-recovery planning.

The 36-hour reporting window will demand incident-response and business-continuity plans that are robust, executable, detailed and integrated among all the necessary internal and external stakeholders, vendors and support staff. Greater situational awareness and communication will be required between banking organizations and service providers that support incident-response operations, requiring more frequent exercises contemplating a range of cybersecurity events. Banking organizations must have a full understanding and, if at all possible, a documented analysis of the criticality of each service provider in maintaining the banking organization's overall operations and services.

Additional scenarios that banking organizations may need to consider, in addition to traditional responses, include:

- serious insider threat violations, including the exfiltration of sensitive banking information, and sabotage of banking systems;
- large-scale introduction of malware or ransomware that threatens to corrupt consumer information or disrupt services for more than four hours;
- server or application misconfigurations leading to widespread outages or other disruptions to banking services; and

- discovery of shadow IT (unapproved applications or software) utilized across workstations that compromise the security, confidentiality, or integrity of consumer information.

See "Strategies and Tactics for Developing an Effective Tabletop Exercise (Part One of Two)" (Sep. 18, 2019); Part Two (Sep. 25, 2019).

Insider Threat Detection

The other direct implication of the reporting proposal is the renewed focus on the insider threat. It would require reporting of any material event that "constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies," reflecting concerns about employees, contractors and other individuals that abuse or circumvent information systems, or are otherwise negligent in their handling of sensitive information. Traditionally, a large proportion of data breaches are due, in part, to policy violations and a failure to safeguard information. Cybersecurity experts have proposed, in accordance with the National Institutes of Standard and Technology guidance, that banks and other organizations manage this risk through access control, least-privilege principles, training, third-party risk management and data-loss prevention policies.

Banking organizations may now have to report not only data breaches, but also disruptions caused by employees, contractors, or vendors, such as those due to improper software updates, system patching and data loss or corruption due to policy violations — all of which dictate that insider risk management become an important aspect of a bank's overall cybersecurity risk management program.

See "Evolution and Mitigation of Insider Cyber Threats During COVID-19" (Jul. 29, 2020).

Jeffrey P. Naimon is a partner in the Washington, D.C. office of Buckley LLP, with more than 25 years of experience assisting bank and nonbank financial services providers with regulatory, enforcement and transactional matters. He defends financial services companies facing complex examination or enforcement matters before myriad state and federal agencies, as well as assists clients structure, negotiate and operate a variety of partnerships, outsourcing programs and other third-party arrangements.

Moorari K. Shah is a partner in the Los Angeles and San Francisco offices of Buckley LLP. He represents banks, fintechs, mortgage companies, auto lenders and other nonbank institutions in transactional, regulatory compliance and vendor management matters, as well as government enforcement inquiries and investigations before various state and federal agencies.

James C. Chou is an associate in Buckley's Washington, D.C., office. He assists clients in a broad range of transactional and regulatory matters with a focus on cybersecurity and privacy issues, which include security incident management and response. Previously, he was a Defense Analyst and Senior Operations Research Analyst for the U.S. Army.