New York DFS Finalizes Amendments to Cybersecurity Regulations

November 30th, 2023 | Mark D. Metrey and K. Dailey Wilson

On November 1, 2023 the New York Department of Financial Services ("DFS") released amended cybersecurity regulations ("Regulations"). These changes will impose additional controls, demand more frequent risk assessments, and update notification requirements – all in an effort to protect New York consumers and financial services companies.

At a high level, key changes to the Regulations include:

- Enhanced governance requirements, including requiring annual approval of written cybersecurity policies and the development of corresponding procedures and imposing cybersecurity risk management oversight requirements on a covered entity's senior governing body;
- Additional controls to prevent initial unauthorized access to information systems and to prevent or mitigate the spread of an attack, including mandating the use of multifactor authentication ("MFA"), establishing requirements regarding the use of privileged accounts, and imposing specific password standards;
- Requirements for more regular risk and vulnerability assessments and more robust incident response, business continuity, and disaster recovery planning;
- Updated notification requirements for "cybersecurity events," including a new requirement to report ransomware payments; and
- Updated direction for companies to invest in at least annual training and cybersecurity awareness programs that anticipate social engineering attacks and that are otherwise relevant to their business model and personnel.

The Regulations focus on integrating cybersecurity into the decision-making process, risk management, and business planning of regulated entities. Below we delve into four categories of regulatory changes: (1) governance, (2) controls, (3) incident response, and (4) enforcement.

Governance

Enhanced governance standards provide a uniform administration of new policies for covered entities, such as requiring "developed, documented and implemented cybersecurity policies" on an annual basis. Timely reporting and remediation plans are among the new requirements that financial services covered entities must comply with when reporting to their respective boards. In order to certify this compliance, both the covered entity's highest-ranking executive and chief

information security officer ("CISO") must sign off on the reports, which is a change from the previous language which only required sign off from a senior officer. Additionally, if the executive or CISO cannot sign off due to noncompliance, they must provide acknowledgement and identify the section(s) of these Regulations that the covered entity is not in material compliance with, as well as a remediation plan (or confirmation that remediation has taken place or been completed).

Controls

New controls aimed at preventing unauthorized access to information systems include MFA, which is now required "for any individual accessing any information systems of a covered entity." The Regulations effectively prohibit the use of text messaging as an MFA possession factor but allow the CISO to authorize use of similar or more secure controls. DFS says this will "ensure the availability and functionality of the covered entity's information systems" even in the event of a cyberattack. The Regulations also impose limitations on "privileged accounts," limiting the number of privileged accounts and the access functions of such accounts to only those necessary to perform the user's job and limiting the use of privileged accounts to only when performing functions requiring the use of such access. Additional obligations including mandating businesses encrypt all nonpublic information in transit over external networks, report ransomware payments, and invest in annual cybersecurity training and programs.

Incident Response

The Incident Response Plans ("IRPs") must include robust periodic tabletop testing of incident response and business continuity and disaster recovery plans, and nonpublic information to be encrypted in transit. In addition, the Business Interruption and Disaster Recovery ("BCDR") plans must include covered entities to identify all data and information related to their respective operations, as well as plans and procedures for the safeguard and recovery of the same.

Enforcement

Two enforcement provisions were added to define: (1) violations, and (2) mitigating factors. The first provision states that any prohibited act or omission of an obligation is a violation, which includes any form of noncompliance with the Regulations. The other provision lists the 16 mitigating factors that DFS will consider when assessing penalties. The extent to which covered entities operate in good faith, adhere to the Regulations, have any prior violations, and have harmed consumers are some examples of what DFS will consider.

These sweeping changes are not indiscriminate: entities regulated by DFS will be accountable for implementing cybersecurity protections relevant to their business size, nature, and data types. For instance, Class A covered entities, defined as "a covered entity with at least $20,000,000 in gross annual revenue" and "over 2,000 employees," have additional obligations, such as conducting independent audits and monitoring privileged access activity.

Companies operating in New York need to huddle up with their compliance counsel and take a close look at their information security programs, making any changes necessary to comply with the Regulations. Even companies operating outside of New York should take a careful look at the Regulations. Regulatory agencies, including the FTC, often look to the New York Cybersecurity Regulations for guidance regarding standards for effective information security programs and sufficient controls. And remember, these amendments are just the first of many expected updates to New York's cybersecurity strategy.

A copy of the final regulations is available here.