CARTER LEDYARD

our resources

New York DFS Proposes Amendments to its Cybersecurity Regulations; What this Means for Companies and their Boards and Executives

September 22, 2022

The New York State Department of Financial Services (the "DFS") recently announced important proposed amendments ("Proposed Amendments") to its Cybersecurity Regulations, which include annual audits and heightened requirements for certain large entities and specific oversight and management obligations for directors and senior management. While the Proposed Amendments, introduced on July 29, 2022, will still need to go through a formal comment period, Covered Entities and their directors and officers should take notice and evaluate the implications.

The DFS Cybersecurity Regulations, 23 NYCRR 500, the first-of-its-kind state cybersecurity regulations, went into effect in 2017, and require banks, insurance companies, mortgage lenders and brokers, credit reporting agencies and financial institutions and other covered entities ("Covered Entities"), to adopt cybersecurity measures that safeguard information and protect and enhance the security of internal cybersecurity systems.[1]

The Proposed Amendments signify that DFS is serious about addressing the increasingly sophisticated cyber threat landscape and ensuring that companies are stepping up their cybersecurity defenses and threat management.

Heightened Requirements Applicable Only to a New Class of Large Companies

The Proposed Amendments designate a new class of Covered Entities, "Class A" entities, defined as companies with more than 2,000 employees or over $1 billion in gross annual revenue for the prior three fiscal years, including revenue generated by any affiliates. Under the Proposed Amendments, Class A entities will have to comply with certain specific additional requirements, including annual audits of security programs, weekly vulnerability assessments, and implementation of enhanced security measures (such as password controls) for certain privileged accounts. Additional proposed requirements applicable to Class A entities include use of external reports to conduct risk assessments at least once every three years, implementation of an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement (techniques used by cyber threat actors to move through a network in order to search for data and assets that are the ultimate targets of attack campaigns), and implementation of a system that centralizes logging and security event alerting.

The remainder of the Proposed Amendments apply to all Covered Entities, regardless of size.

Governance Requirements for Boards of Directors and Senior Officers

Like the cyber rules proposed by the U.S. Securities and Exchange Commission in March 2022,[2] the Proposed Amendments emphasize the role of the board of directors and senior officers in cybersecurity management and oversight. The Proposed Amendments require the board (or a committee of the board) of Covered Entities to have sufficient expertise and knowledge to exercise effective oversight of cyber risk or be advised by persons with sufficient expertise and knowledge. Further, under the Proposed Amendments, the board must approve all cybersecurity policies at least annually, whereas the current Regulations require approval merely by a senior officer. The executive management

team must develop, implement, and maintain the company's information security program. Once discovered, any material gaps in cybersecurity practices must be documented and timely reported to the board and to senior management.

The Proposed Amendments require an entity's CISO to have adequate independence and authority to ensure cybersecurity risks are appropriately managed. For the CISO's annual report to the board, the Proposed Amendments require the CISO to report on plans to rectify any deficiencies found in a company's cybersecurity program and to address material cybersecurity issues and events. The Proposed Amendments require the annual compliance certification to DFS to be signed by the CISO and CEO, whereas the current Regulations require only the certification by a senior officer. If an entity is not fully compliant, the CISO will need to provide DFS with an acknowledgement, specifying all areas, systems, and processes that require material improvement and the planned remedial efforts.

Risk Assessment, Technology, and Compliance Obligations

Under the Proposed Amendments, all Covered Entities must implement and maintain written policies and procedures designed to ensure complete and accurate asset inventory for all information systems and their components, including hardware, operating systems, applications, infrastructure devices, application programming interfaces, and cloud services. A Covered Entity's cybersecurity policy must be updated at least annually and include procedures addressing end of life management, remote access and vulnerability, and patch management, in addition to all of the requirements of the existing Regulations.

The Proposed Amendments include specific requirements relating to the development of a business continuity and disaster recovery plan in addition to an incident response plan to ensure that businesses can continue to operate in the event of a major disruption, disaster, or emergency. A Covered Entity's business continuity and disaster recovery plan should, at a minimum: (i) identify information essential to the continued operations of the business, (ii) identify the personnel responsible for implementing each aspect of the plan, (iii) include procedures for communicating with essential persons in the event of an emergency or other disruption, (iv) describe procedures for maintenance of back up facilities, systems, and infrastructure, and (v) include procedures for back up of information and identify third parties necessary to continued operations of the business. The Proposed Amendments further require that Covered Entities distribute copies of the plan to employees responsible for implementing the plan and provide training on the employees' roles and responsibilities. All Covered Entities will be required to periodically test their incident response plan, business continuity and disaster recovery plan, and ability to restore systems from backups.

The Proposed Amendments expand the definition of "risk assessment" – which all Covered Entities must conduct – to ensure that it be tailored to the specific circumstances of a Covered Entity, including its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors and their locations and geography and location of a Covered Entity's operations and business relations. DFS has also expanded the scope of the "cybersecurity program" which all Covered Entities must maintain, to include nonpublic information stored on an entity's information systems.

Further, the Amendments require certain physical and technological security measures, such as multi-factor authentication for all remote access to the network, third party applications from which nonpublic information may be accessed, and for certain privileged accounts.

Notifications

The Proposed Amendments will create the following new notification and reporting requirements in connection with cybersecurity incidents:

- Notification to DFS within 72 hours of cybersecurity events involving (i) unauthorized access to certain privileged accounts, or (ii) the deployment of ransomware within a material part of the company's information systems.
- Notification to DFS within 24 hours of making an extortion payment in connection with a cybersecurity incident (such as the payment of ransom to a ransomware attacker).

- Written report within 30 days of any extortion payment, describing why payment was necessary, all due diligence conducted to explore alternatives to payment, and all due diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

These proposed new notifications and reports are intended to increase transparency with respect to cybersecurity incidents, encourage the consideration of alternatives to the payment of ransom, and ensure that sanctions regimes are not violated when ransom payments are made.

Violations and Penalties

The Proposed Amendments clarify that any single act prohibited by the Regulations constitutes a violation, and thus a violation occurs when there has been a failure to secure or prevent unauthorized access to nonpublic information due to noncompliance with any section of the Regulations or a failure to comply with any section of the Regulations for any 24-hour period.

In addition, under the Proposed Amendments, DFS may take several factors into consideration when assessing penalties for violations, such as the following: the extent to which a Covered Entity cooperated with DFS over the course of the investigation; good faith of the Covered Entity; whether the violation was committed unintentionally, recklessly, or intentionally; whether the violation was a result of a failure to remedy previous examination matters requiring attention or due to the failure to adhere to DFS disciplinary letters or instructions; a history of prior violations; whether the violation resulted from an isolated event or repeat, systemic violations; whether the Covered Entity provided false or misleading information to DFS; the extent of harm to consumers; whether required, accurate, and timely disclosures were provided to affected consumers; the gravity of the violations; the number of violations and length of time over which they occurred; the extent to which a senior governing body (such as the board of directors) participated in the violation; any penalty or sanction imposed by another regulatory agency; the financial resources, net worth, and annual business volume of the Covered Entity and its affiliates; and other matters required by justice and the public interest.

Once the Proposed Amendments are adopted, Covered Entities will have 180 days to come into compliance, however some requirements have different compliance timeframes. For example, a Covered Entity will have 30 days to comply with the updated notification requirements, and for certain other requirements (such as implementation of password controls) a Covered Entity will have one year to comply.

Key Takeaways

The Proposed Amendments will significantly expand upon and update the existing Regulations and demonstrate DFS's desire to ensure that all Covered Entities take sufficient steps to address cybersecurity issues and increase preparedness for cybersecurity incidents and attacks. Particularly notable are DFS's heightened standards for disclosure of incidents and the timing of such disclosures; new reporting requirements relating to ransom payments (and the required consideration of alternatives to paying ransoms); DFS's effort to tailor certain requirements only to certain large entities; enhanced testing, training, and risk assessments; and certain technological security requirements. From a governance perspective, the Proposed Amendments will place new burdens on boards of directors and senior management, namely the CISO and CEO.

Covered Entities should become familiar with the Proposed Amendments now, begin to assess their level of compliance, and begin preparing to implement administrative, physical, and technical safeguards to ensure compliance. Covered Entities are encouraged to consult legal counsel to assist in interpreting the Proposed Amendments, evaluating compliance obligations, and advising on measures to ensure compliance.

* * *

[1] For further information about the DFS Regulations, see https://www.clm.com/new-york-states-revised-cybersecurity-legislation-for-financial-institutions-what-you-need-to-know/ and https://www.clm.com/ny-department-of-financial-services-brings-its-first-cybersecurity-regulation-enforcement-action/.

[2] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, SEC, 17 C.F.R. Parts 229, 232, 239, 240, & 249 (Mar. 9, 2022) (available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf).

---

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com