CYBERSECURITY AMENDMENT UPDATE (NOVEMBER 2023)

Written by Mitchell B. Pollack, Attorney at Law, Mitchell Pollack & Associates PLLC

As reported throughout this past year, the New York Department of Financial Services ("DFS") has been working to amend New York's cybersecurity regulations, and on November 1, 2023, the final version of the 23 NYCRR 500 amendment was issued (the "Amendment"). The New York Credit Union Association (the "Association") has been lobbying for the compliance deadlines to be extended, and this request has been acknowledged. The Amendment's new compliance requirements (23 NYCRR 500.22) will take effect in phases and, unless otherwise specified, covered entities now have 180 days from November 1, 2023 to come into compliance (until April 29, 2024). Changes to reporting requirements take effect one month after publication of the amended regulation (or December 1, 2023), and for certain other requirements, the Amendment provides for up to 12 months, 18 months, or two years to come into compliance.

The final version is similar to the June 2023 proposal, but includes some key changes and clarifications to sections that the Association had addressed in its prior DFS comment letters. At the outset, 23 NYCRR 500.1(e) now defines "Covered Entity" as follows:

> Covered entity means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies {*emphasis added*}.

This clarifies that "Covered Entity" includes any institution operating under or required to operate under a license, registration, charter, permit, accreditation or similar authorization under the New York Banking Law, Insurance Law, or Financial Services Law, regardless of whether the Covered Entity is also regulated by other government agencies. In the comment responses recently published, DFS stated that federally regulated institutions "that apply for and are granted a license to perform a service that is regulated by DFS must comply with the regulations that apply to anyone holding such a license, including Part 500." Under N.Y. Banking Law §590(2)(b-1), an exempt Mortgage Loan Servicer must notify DFS that it will act as a servicer and since the notification is not an authorization from DFS, an exempt Mortgage Loan Servicer is not a Covered Entity under §500.1(e). If an exempt Mortgage Loan Servicer also holds a license, registration, or received approval under the provisions of Part 418.2(e), however, it will be considered a Covered Entity and must comply with the Cybersecurity Regulations. This appears to be confirmation that the Amendment would not apply to federal credit unions unless they have applied for a separate New York State license which subjects them to DFS oversight or oversight by another NY State agency. However, due to rising cybersecurity risks, DFS is strongly encouraging all financial institutions, including those exempt Mortgage Loan Servicers that are not Covered Entities, to adopt cybersecurity protections consistent with those required by Part 500.

The limited exception in 23 NYCRR 500.11(c) which stated that "[a]n agent, employee, representative or designee of a covered entity who is itself a covered entity need not develop its own third party information security policy pursuant to this section if the agent, employee,

representative or designee follows the policy of the covered entity that is required to comply with this Part" was removed, but only because it was basically duplicative of §500.19(b). 23 NYCRR 19(b) states that: "[a]n employee, agent, wholly owned subsidiary, representative or designee of a covered entity, who is itself a covered entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, wholly owned subsidiary, representative or designee is covered by the cybersecurity program of the covered entity."

Section 500.2(a) was amended to clarify that Covered Entities shall maintain cybersecurity programs designed to protect their information systems and the nonpublic information stored on those systems. Section 500.2(d) was re-lettered to (e) and clarifies that Covered Entities adopting cybersecurity programs of their affiliates must provide the Superintendent, upon request, all documentation related to those programs.

Section 500.14 labeled "Training and Monitoring," requires each Covered Entity to implement "risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content" and to provide regular cybersecurity awareness training, which includes social engineering, for all personnel, at least annually. The policies must monitor the activity of authorized users and detect unauthorized access or use of Nonpublic Information. It also added a subdivision 500.14(b) which only applies to Class A Companies.

Cyberattacks are on the rise, and the Amendments require the financial services industry to institute stronger policies and controls to secure sensitive data. DFS will host a series of webinars to provide an overview of the amended cybersecurity regulations. Registration details for these training events and compliance timeline are available on the DFS website.

For full details surrounding the updated cybersecurity regulation, please visit the Cybersecurity Resource Center.