NEW YORK creditunion ASSOCIATION

strength in members.

August 18, 2022

Via electronic mail: Joanne.Berman@dfs.ny.gov

Ms. Joanne S. Berman
Counsel to the Cybersecurity Division
NYS Department of Financial Services
One State Street
New York, NY 10004

Re: Request for Comment Draft Amendment to 23 NYCRR 500 - Cybersecurity Requirements For Financial Services Companies

Dear Ms. Berman,

On behalf of the New York Credit Union Association, which has represented both state and federal credit unions for more than one-hundred years, I would like to take this opportunity to comment on the Department's proposed amendments to 23 NYCRR 500. The Department's cybersecurity regulations are among the most important compliance obligations imposed on state-chartered credit unions as well as Credit Union Service Organizations (CUSOs) licensed by New York State. While the Association recognizes the need to update this framework to address emergent issues such as ransomware, we believe that subtle changes to these amendments would allow impacted institutions to better balance compliance with the costs associated with these changes.

§ 500.1(j) Amendments to Penetration Testing Definition

The Association is supportive of this change because the new definition better reflects what penetration testing actually is. Our support, however, is based on the assumption that institutions performing penetration testing in compliance with the existing definition will continue to be in compliance if they use the same methodology.

§ 500.2 Risk Assessment

The proposed regulations expand the definition of a Risk Assessment to include, for example, *the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties,*

service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations. Risk assessments incorporate threat and vulnerability analyses, and consider mitigations provided by security controls planned or in place. While many of the elements to be included in the expanded definition are sensible and appropriate, the regulations should be made as easy and understandable as possible for institutions of widely divergent sizes and skill sets to comply with. Therefore, to avoid any confusion about what constitutes compliance with § 500.2, the finalized regulations should include or be coupled with a Risk Assessment Template that can be used by institutions. This approach will help credit unions and all other institutions appropriately organize and assess the strengths and weaknesses of their cybersecurity protocols. In short, a detailed checklist would be an appropriate tool for both institutions and examiners.

§ 500.4 Amendments to Authority and Independence of Chief Information Security Officer (CISO)

This amendment is highly problematic. While the Association certainly agrees that a "*… CISO must have adequate independence and authority to ensure cybersecurity risks are appropriately managed*", reasonable individuals can and will disagree about how to accomplish these goals. Financial institutions must have the flexibility to comply with this and all other priorities in a way that best reflects the unique needs of their respective institutions. In contrast, this language is so precatory that examiners will be able to substitute their judgement for that of a board without having to point to any specific shortcomings in an institution's organizational chart or budget priorities. The lack of objective criteria is all the more troubling since a putative violation of this provision could lead to large fines. In order to ensure there is an appropriate balance between a board's good-faith exercise of its discretion and the legitimate safety and soundness priorities of DFS, this language should be amended to read as follows:

> *In order to ensure that a CISO has adequate resources and independence, they must directly report to the board and senior management as reflected in the organization's organizational chart.*

§ 500.11 Removal of: [(c) Limited exception. An 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.]

The removed language minimizes the administrative burden that would otherwise be imposed on both financial institutions and DFS by providing a mechanism for individual employees, such as mortgage loan originators, to be exempted from these regulations. With removal of this language, this proposal would mandate that every individual employed by a covered entity create a cyber security plan. This clearly is not DFS's intent, and this drafting oversight should be remedied before the regulation takes effect.

§ 500.14(b)(1) et seq. Definition of "lateral movement"

Given the ubiquity of cyber-attacks, even the most vigilant institutions should assume that their systems may be penetrated. Anecdotally, it is common for hackers to spend weeks or even months within an IT system before executing an actual attack. Class A institutions are required to take steps to not only detect cyber breaches but also to minimize the ease with which successful hackers can move within a system. Therefore, while the Department understandably wants larger institutions to address these circumstances, its existing language should better clarify and define Department expectations.

For example, given the importance of restricting a hacker's "lateral movement," the regulations should include a definition of "lateral movement" to make sure that IT teams are put on notice with regard to this important cybersecurity concept.

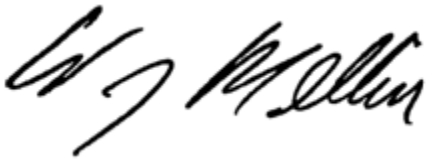
§ 500.22 Compliance deadlines should be extended

The vast majority of these changes will become effective six months after they are finalized. Six months is too short a time to properly comply with these procedures. Impacted institutions will have to analyze and update existing policies and procedures and in some instances create entirely new ones. Vendors will have to be notified and in some cases, contracts will need to be amended. Staff will have to be appropriately trained and boards of directors will have to approve of these changes. Under these circumstances, a one-year compliance timeline would be more appropriate, especially since there are serious reputational and legal risks associated with non-compliance. By mandating compliance within six months, the Department is underestimating the impact of complying with these changes. It will present a significant burden to impacted organizations since there are certain items that could take time to address and pose the need for credit unions to potentially obtain services or additional systems to aid in management. It will impact budgets, staff time, and potentially mean that other strategic projects will have to be delayed. This could also delay projects that are already in process and planned before this proposal was made.

Conclusion

Credit unions share DFS's commitment to ensuring that consumer information is appropriately protected. Furthermore, as the risk environment evolves, so too should regulations designed to combat cyber intrusions. The changes outlined by the Association would enable the Department to achieve all its core goals in proposing these amendments while doing so in a way which helps smaller to mid-size institutions comply with these regulations in a cost-effective manner.

Sincerely,



William J. Mellin
President/CEO

WM:HM/cw