November 14, 2016

Maria T. Vullo, Esq.
New York State Department of Financial Services
One State Street
New York, NY 10004

Dear Superintendent Vullo:

On behalf of the New York Credit Union Association ("NYCUA") and the Credit Union National Association ("CUNA"), we are writing this joint letter to comment on New York's proposed regulation mandating that banks and credit unions, insurance companies and financial service providers establish cybersecurity programs to protect nonpublic electronic information.

We are jointly offering our comments because the requirements ultimately mandated by New York will lead to confusion and conflicting cybersecurity requirements for financial services companies. The Department of Financial Services ("DFS") needs to consider the national impact of cybersecurity regulations issued by only one state when robust national standards exist that could be adopted by the DFS. Credit unions and other financial institutions are already subject to many similar requirements and would welcome all industries having to provide cybersecurity protections.

Unfortunately, New York's proposal is seriously flawed. Most importantly, it is too prescriptive. It fails to give covered state chartered institutions the flexibility they need to satisfy the proposed requirements by demonstrating comparable measures they have already taken to satisfy cybersecurity requirements. It would implement a one-size-fits-all approach to cybersecurity that does not clearly allow credit unions to develop and implement cybersecurity policies, devise plans, and allocate resources in a way that reflects their unique cybersecurity profile, and fails to appropriately delineate those institutions that would be subject to its mandates. Ultimately, it makes little sense for a $19 million asset credit union with six employees—the median size of New York credit unions—to be subject to the same baseline requirements as the world's largest financial institutions; but that is exactly what New York State proposes.

Existing Cybersecurity Standards are Robust. The financial industry is already subject to extensive cybersecurity regulations and requirements. Presently, the Consumer Financial Protection Bureau ("CFPB"), Securities and Exchange Commission ("SEC"), Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve System ("Fed"), Federal Trade Commission ("FTC"), National Credit Union Administration ("NCUA"), and the Office of the Comptroller of the Currency ("OCC"), provide cybersecurity regulations, requirements and guidance to the financial services industry. These comprehensive requirements govern all areas of cybersecurity protection, including board engagement, staffing and management, written information security plans, cybersecurity training, technical controls, disposal of sensitive information, and numerous other aspects of cybersecurity.

Credit Unions Already Have Rigorous Cybersecurity Regulations with Which to Comply

Proposed 500.01(e) defines an Information System as *"*a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." Section 500.01(d) defines a Cybersecurity Event as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."

Over the last 15 years, credit unions have been subject to numerous cybersecurity mandates designed to protect member information by identifying and deterring cyber-crime. NCUA has joined with other financial regulators in issuing guidance stressing the need for monitoring information security and changing protocols to address evolving threats. For example, as far back as August 8, 2001, the FFIEC issued guidance on Authentication in an Electronic Banking Environment. The guidance stressed "an enterprise-wide approach to identification," which included a risk assessment and Information Security Framework. It stressed that, "[b]ecause the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and service providers should periodically review authentication technology and ensure appropriate changes are [made]."

As cyber threats have evolved, the obligations of credit unions to protect data have become more sophisticated. The 2001 FFIEC guidance was followed by an updated guidance mandating that, "[w]here risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties."

Most recently, credit unions have been strongly encouraged to integrate the FFIEC's cybersecurity assessment tool into their compliance framework. This tool provides a framework for institutions to both assess the vulnerability of their institution to cyber-attacks and ensure that appropriate steps are taken to militate against such risks.

There are also numerous federal statutory requirements. Sections 15 USCA 66801 and 6805(b), of the Gramm–Leach–Bliley Act ("GLBA") have been responsible for having a program that identifies, prevents and mitigates identity theft (12 CFR 717 App. J). This program must be overseen by each credit union's board of directors. Compliance with this plan includes monitoring developments that pose a threat to the integrity of account information by electronic means. Like New York's program, board members must oversee the program's development, credit unions must periodically test information security, and ensure adequate staff training. Oversight of third party providers and disaster preparedness plans providing for the swift recovery of electronically stored information is also required.

Finally, even without statutory and regulatory mandates, both credit unions and banks face the prospect of costly civil litigation if they fail to adhere to "commercially reasonable" electronic fund transfers under NY UCC Article 4A (Regatos v. N. Fork Bank, 257 F. Supp. 2d 632, 646 (S.D.N.Y. 2003)).

In addition to these legal mandates, many credit unions that offer credit and debit cards comply with PCI requirements developed by the major credit card issuers as a compliance baseline. Among the core elements of PCI is the encryption of electronic data.

The Final Regulation Should Enable Institutions to Show They Already Comply with Comparable Federal Requirements

The purpose of this regulation is to mandate adequate, not duplicative, cybersecurity requirements. Nevertheless, despite the fact that credit unions already invest time, money, and manpower to detect and deter cyber threats, the regulation, as drafted, does not explicitly allow institutions to satisfy its mandates by demonstrating how existing programs and protocols satisfy the requirements. This is particularly troubling because boards of directors will be required to certify that their credit unions are in compliance with New York's regulation.

While there are many similarities between New York's proposal and existing federal requirements, perhaps the most important distinction is that federal regulations permit institutions to base their information security plans on the size and sophistication of their operations. New York's proposal provides no such flexibility.

This is unfortunate, particularly for smaller institutions. Requirements such as quarterly risk assessments and periodic penetration tests may be entirely appropriate for a credit union that relies heavily on technology, but make little sense for a credit union that provides limited online banking and is struggling to grow. (Section 500.09 requires institutions to perform annual risk assessments but does not allow the institution to choose the requirements with which it must comply.) The final regulation should adopt the approach of federal regulators in 12 CFR 748 and include language specifying that a Covered Entity must:

> Design its cybersecurity program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of its activities. Each covered entity must consider whether the following securities measures are appropriate for it to adopt . . . .

Section by Section Concerns

The mandated staffing requirements would allow examiners to intrude into decisions that are within the exclusive authority of credit unions. Each credit union would be required to employ a dedicated Chief Information Security Officer; provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and require all personnel to attend regular cybersecurity awareness training sessions. The costs associated with these staffing mandates should not be underestimated. They will result in rebalancing work hours so that employees can receive training while branches are open and may very well involve paid trainers. Furthermore, while it is increasingly common for many larger institutions to have individuals who are responsible for information security, many smaller institutions do not have individuals solely dedicated to this responsibility, nor could they afford to. Chief Information Security Officers do not come cheaply. The authority to use third party vendors only partially addresses these concerns. Institutions will now have to absorb an additional cost and will still have to make sure that there is someone on staff knowledgeable enough about cybersecurity to monitor the vendor's activity.

The existing exemption in 500.18 is too small and too limited. The NCUA defines a small credit union as one with less than $100 million in assets. Credit unions below this threshold are exempt from certain regulatory requirements. In contrast, covered entities are only exempt from this regulation if they service 1,000 or fewer customers, generate less than $5 million in revenue, and have less than $10 million in assets. The exemption threshold should be raised to $100 million. Institutions of this size have more staff and resources and also tend to be more heavily invested in technology. In contrast, some smaller institutions are struggling to afford even a single compliance officer and, to the extent they

are considering investing in technology, may simply forgo doing so if they must also comply with this regulation.

We suggest that the DFS adopt a risk-based approach as used in federal rules and regulations. The Interagency Guideline issued by FDIC, Fed, NCUA, and OCC pursuant to the GLBA require firms to (1) identify "reasonably foreseeable internal and external threats"; (2) "[a]ssess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information"; and (3) assess the "sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks." Firms are required to develop a "comprehensive information security program" to address such identified risks "that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities."[i] Technical controls and other security measures must be implemented to "control identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities."

Flexible requirements based on an assessment of the level of risk would make compliance with requirements easier for smaller institutions because it would allow them to allocate the proper resources to match risks. Many small institutions do not offer a full slate of banking services and products and thus have vastly reduced risk profiles, which should be contemplated by these requirements. The final regulation should permit firms to target resources and controls based on their size and complexity, the level of risk, and the sensitivity of the information.

The final regulation should clarify the scope of the State's jurisdiction. As currently drafted, this regulation applies to any individual, partnership, corporation, association or other entity 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 (501.019(c), (h)). This definition is so broad that it will include institutions over which the state has no oversight authority. For instance, even though mortgage originators employed by federally-chartered credit unions are not subject to state registration requirements, they are subject to certain state servicing requirements. Does it follow that the employees of a federally chartered institution are subject to this regulation? To prevent this and similar examples of jurisdictional confusion, the definition of covered entity should be amended as follows (*changes in italics*).

> 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 who is e*ither Incorporated, Chartered, or licensed to operate pursuant to New York State Law.*

This definition ensures that the state can oversee the activities of institutions such as credit union CUSOs and bank affiliates incorporated in New York State while ensuring that federal institutions would not have to be concerned about the compliance implications of requesting a certificate from, or registering with the State, for whatever reason.

Proposed section 500.11 addresses third party information security policies. NCUA has emphasized vendor due diligence for more than a decade. Based on this experience, the final provision has to be clarified to reflect operational realities. While many credit unions negotiate contract changes with vendors, given their relative lack of size and market share, many third party vendors are unwilling to make the changes requested of them. The final rule should not include specific provisions that must be in vendor contracts. Simply put, if credit unions have to insist on specific vendor requirements that go beyond operational concerns before signing contracts, many would be unable to secure needed vendor services. Ultimately, the state is in a better position to mandate that vendors provide products that are free of viruses, trap doors, time bombs, and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information.

The Final Regulation Should Clarify the Definition of Nonpublic Information. NYCUA and CUNA recognize the importance of ensuring that nonpublic information is as secure as possible and commend the Department's efforts to protect the personal information of consumers from cyber threats. However, NYCUA and CUNA submit that the definition of nonpublic information can be improved by narrowing it and including only nonpublic personal information rather than business-related information.

The proposed regulations include an extraordinarily expansive definition of "nonpublic information." Proposed 23 NYCRR § 500.01(g). Among the numerous issues that arise with such a broad definition is the fundamental problem of not being able to readily identify what information might be considered nonpublic. For example, under the proposed regulations, nonpublic information includes "[a]ny business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity." Proposed 23 NYCRR § 500.01(g)(1). This definition is too broad to be interpreted with any degree of confidence and too subjective to be applied uniformly across the vast landscape of financial institutions within its purview.

In addition, the proposed definition of nonpublic information includes business-related information, specific to the Covered Entity in addition to personal consumer information. The Gramm-Leach-Bliley Act more narrowly defines a specific subset of nonpublic information, *i.e.*, nonpublic personal information.

> (4) The term "nonpublic personal information" means personally identifiable financial information—
> (i) provided by a consumer to a financial institution;
> (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
> (iii) otherwise obtained by the financial institution.
> (B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.
>
> 15 U.S.C. § 6809(4) (2016).

NYCUA and CUNA respectfully request that the Department consider similarly narrowing the scope of the definition in the final regulation to include only nonpublic personal information rather than business-related information. After all, the primary concern here is the protection of personal data. Financial institutions should be left to determine how best to protect their own information. The current proposed definition is too prescriptive and is overly burdensome, particularly to smaller credit unions.

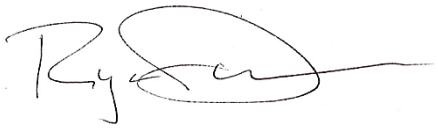
Finally, section 500.17 requires **covered entities to provide the Superintendent notice** of any cyber-security event that has "a reasonable likelihood of materially affecting the operation of the Covered Entity or that affects Nonpublic Information." While notification to the superintendent is appropriate in concept, this provision is entirely too broad. Since a cybersecurity event includes any act or attempt to gain unauthorized access to an entity's data, even relatively small institutions would have to provide the DFS cybersecurity notification on a daily basis and sometimes multiple times within a day. In order to make this useful, the final regulation must be narrowed so that all institutions have at least some guidance as to when to notify the DFS.

Conclusion

NYCUA and CUNA respectfully urge the Department to consider the foregoing comments and implement the recommended changes in the final regulations. As described in detail above, not only are existing cybersecurity standards quite robust, credit unions are currently also subject to rigorous cybersecurity regulations. Application of the regulations as proposed would be entirely inappropriate and counterproductive to DFS' objective of enhancing the safety and soundness of the state's financial institutions.

Sincerely,

William J. Mellin, President/CEO
New York Credit Union Association



Ryan Donovan, Chief Advocacy Officer
Credit Union National Association

[i] Interagency Guidelines, 12 C.F.R. pt. 364, App. B, at II.A; *see also* SEC, Regulation SCI, 17 C.F.R. § 242.1001(b)(1); Red Flags Rule, 7 C.F.R. § 162.30(d)(1) (CFTC), 12 C.F.R. § 717.90(d)(1) (NCUA); 16 C.F.R. § 681.1(d)(1) (FTC); 12 C.F.R. § 571.90(d)(1) (FDIC); 12 C.F.R. § 222.90(d)(1) (FRB); 12 C.F.R. § 41.90(d)(1) (OCC).