November 14, 2016

Cassandra Lentchner
Deputy Superintendent for Compliance
New York State Department of Financial Services
One State Street
New York, NY 10004-1311

Re: New York Department of Financial Services Proposed Regulation: "Cybersecurity Requirements for Financial Services Companies [23NYCRR Part 500 (Financial Services Laws)]

Dear Ms. Lentchner:

On behalf of the Independent Bankers Association of New York State (IBANYS) and the Independent Community Bankers of America (ICBA),[1] we are pleased to submit our collective comments in response to the proposed "Cybersecurity Requirements for Financial Services Companies" [23 NYCRR Part 500 (Financial Services Laws)].[2] Community banks, including their boards', management and employees in New York State recognize and take seriously their responsibility to protect customer data and personal information. Beyond existing regulatory and

[1] The Independent Community Bankers of America®, the nation's voice for nearly 6,000 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education and high-quality products and services. With 51,000 locations nationwide, community banks employ 700,000 Americans, hold $3.9 trillion in assets, $3.1 trillion in deposits, and $2.6 trillion in loans to consumers, small business, and the agricultural community. For more information, visit ICBA's website at www.icba.org.

[2] New York Department of Financial Services (NYDFS); Proposed "Cybersecurity Requirements for Financial Services Companies". Published 28 September 2016. [23 NYCRR Part 500 (Financial Services Law)]. http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf. Hereinafter referred to as "proposed regulation".

statutory requirements directed at data breaches, the community bank business model is based on customer trust and service. A failure to safeguard data resulting in a breach would have a significant negative impact on a community bank. Compromised customers of such institutions have multiple choices for their business in the financial marketplace. Beyond any legal or regulatory requirements, cybersecurity is a business imperative for community banks in the digital marketplace.

Cybersecurity risks are constantly evolving. Community banks are cognizant of these risks and are investing in security controls to protect data and critical systems. In addition, public-private partnerships and organizations that support the financial sector are working diligently and collaboratively to mitigate some of these risks through enhanced information sharing. Some of these public-private partnerships include the Financial Services Sector Coordinating Council (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC), the Financial Services-Information Sharing and Analysis Center (FS-ISAC) and Federal and state governments are valuable in gathering the intelligence necessary to collectively mitigate against threats and defend customer information. The State of New York is a member of the Multi-State ISAC (MS-ISAC) of which the FS-ISAC is a partner. The MS-ISAC is also a member of the National Council of ISACs of which FS-ISAC is also connected. The New York Department of Financial Services is a member of the FS-ISAC, as is the New Jersey Cybersecurity and Communication Integration Cell (NJCCIC). These partnerships strengthen the overall sector resilience against cyber threats.

A Profile of Community Banks in New York State

Community banks are just that – community institutions designed to meet the needs of consumers and businesses in their communities. Relationship banking, personal attention and a high degree of trust are hallmarks of community banks in New York State and nationally. While more than half of the banks in the state are community banks below $1 billion in asset size, most of these are even smaller, with assets below $300 million. These smaller community banks average 37 employees, with half having less than 35 employees. This is sharply contrasted with much larger institutions who employ, on average, 5,888 employees, with half having less than 1,169 employees. The chart below illustrates the profile of community banks in New York:

NY Bank Stats	Less than $300M	$300M-$1B	$1B-$10B	$10B or More
Number of institutions	55	45	43	12
Number State Chartered	25	29	24	7
Average employees	37	109	404	5,888
Median employees	35	100	358	1,169
Average Total Revenue 2015 - $M	$6.5	$22.4	$125.2	$1,530.6
Median Total Revenue 2015 - $M	$6.4	$22.0	$99.6	$1,227.2
Average Deposit Account Customers	6,531	21,786	103,459	1,011,847
Median Deposit Account Customers	4,800	18,308	53,441	914,782

All New York Chartered Community Bank are Impacted by the Proposed Regulation

The proposed regulation, at Section 500.18, allows for an exemption of certain financial companies. To meet the exemption, three elements must be met in their entirety:

1) The entity must have fewer than 1,000 customers in each of the last three calendar years, and
2) Less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and
3) Less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates...[3]

[3] See Ibid, Section 500.18(a). Page 10.

Meeting these three conditions would exempt a "Covered Entity," defined as "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"[4] from only nine of the proposed regulation's provisions. Based on the profile presented above and the definition of "Covered Entity," it is clear that all New York state chartered community banks will be impacted by this proposed regulation.

We strongly disagree with the "one size fits all" approach this proposed regulation adopts. In the Department's "Report on Cyber Security in the Banking Sector" from May 2014, the report, in its conclusion states:

> …although the issue of limited resources will continue to plague small institutions in particular, the amount of money spent on a cyber program is by no means the best reflection of its strength. Costly software that is rarely updated, deployed in an ineffective manner, or fails to take into account social engineering does little to contribute to an institution's cyber program. Much more relevant is an institution's ability to identify its top cyber risks and design a program around those risks. **The Department recognizes that cyber security does not have a "one-size fits all" solution and that a successful cyber program will be based on an institution's size, its business model, and sensitivity of data collected…**[5]

Indeed, limited resources are a concern for community banks around the country and in New York State. The survey and the proposed regulation, however, do not reflect that community banks, governed by boards of directors, set their risk parameters and determine how best to

[4] See Ibid, Section 500.01(c). Page 2.
[5] New York State Department of Financial Services. "Report on Cyber Security in the Banking Sector." May 2014. http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf . Emphasis added.

allocate resources to combat cyber threats, in accordance with their risk assessment. We agree with the Department, in their written survey analysis, that one size does not fit all. However, there is not a meaningful differentiation between megabanks and community banks in this proposed regulation.

Risk mitigation for community banks include framework and control adoption, selection of qualified vendors, penetration tests, audits, information sharing and personnel decisions, including the employment of shared information security personnel, among other measures as DFS examiners are aware through their current examinations. The proposal, however, applies a de facto uniform and unequal application of risk mitigation tactics some of which when, in practice, may go beyond the risk profile of the institution.

The Regulation Does Not Match the Risk

The proposed regulation, does not correlate to existing Federal efforts. This creates a significant regulatory mandate and burden on community banks and does not correspond to an institution's risk profile.

Framework Harmonization

Cybersecurity is a national issue and should be coordinated with both state and federal regulators. This proposed regulation exceeds the current approach taken by the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve Board (FRB) to cybersecurity. The Federal Financial Institution Examination Council recently released its voluntary Cybersecurity Assessment Tool (FFIEC CAT). It is important to note that the FFIEC CAT is a voluntary tool that institutions may use. The FFIEC reinforced the voluntary nature of the CAT in their recently released "Frequently Asked

Questions,"[6] which correctly recognized that oftentimes it is not just one tool, framework or assessment a bank employs to guide their compensating controls but it is a variety of controls that match the risk of the institution, to wit: … [u]se of the Assessment by institutions is voluntary to identify inherent risk and cybersecurity preparedness. Institution management may choose to use the Assessment, or another framework, or another risk assessment process to identify inherent risk and cybersecurity preparedness".[7] Even with its voluntary nature, community banks have voluntarily adopted this tool to help them assess their current risk and cybersecurity preparedness because of its relative ease of use and ability for information security personnel to discuss cybersecurity with their boards of directors.

DFS should allow community banks to adopt a reasonable risk assessment tool that would be used by DFS in the conduct of their examination for compliance to the cybersecurity regulations.

Without a risk-based approach, the proposed regulation is overly broad without appropriate distinction between systemically important banks and New York State community banks. A flexible approach allows community banks to tailor their cybersecurity programs to their size and complexity. The proposed regulation, in contrast, contains specific personnel, assessment and technical requirements regardless of the size and complexity of the institution.

Matching the Burden with the Risk Profile

While the work of the Department is appreciated, as mentioned, Federal regulators have been aggressively pursuing cybersecurity preparedness through regulation, guidance, proposed rules, voluntary cybersecurity assessments and support for public-private partnerships. The goal

[6] Federal Financial Institutions Examinations Council. "FFIEC Cybersecurity Assessment Tool Frequently Asked Questions" 17 October 2016. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT%20FAQs.pdf
[7] Ibid. Page 1.

of improved cybersecurity would be better served by DFS working in conjunction with the Federal entities and the multiple public-private partnerships.

Without coordination with Federal regulatory agencies, this places community banks in the difficult situation of being examined based on different requirements. It also forces banks to consider the efficacy of their state charter if the regulatory burden is significantly greater at the state level than the federal level. This is particularly true if there are blanket regulatory requirements which are not tied to the banks' risk profile, complexity, scope, business model, data sensitivity and size. To be clear on this point, community banks would consider leaving the state charter not for fear of not meeting the regulatory requirements of the proposed regulation, but rather because of the disproportionate burden it places on community banks to comply. This includes the reporting requirements and costly mandates that must take place at regular intervals regardless of size, complexity, scope, business model, data sensitivity or risk of the institution.

It is clear that both federal and state bank regulators are examining the most effective approach to ensure that appropriate cybersecurity measures are implemented by banks. This mutual goal should not be lost in the rush to regulation. A measured and coordinated approach with commonality would provide a more effective regulatory platform for this important issue.

Notification Requirements

The proposed regulation, at Section 500.17, requires "[e]ach Covered Entity to notify the superintendent of any Cybersecurity Event that has a reasonable likelihood to materially affect the normal operation of the Covered Entity or that affect Nonpublic Information".[8] While we do not disagree with the notion of reporting significant, successful cyber events to the state regulator, as is currently the requirement of institutions examined in accordance with a federal

[8] New York Department of Financial Services (NYDFS); Proposed "Cybersecurity Requirements for Financial Services Companies". Published 28 September 2016. [23 NYCRR Part 500 (Financial Services Law)]. 16.

charter,[9] we oppose this broad approach of reporting "any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information".[10] This section alone will add a substantial burden and will be difficult to overcome at a small institution.

Notification Timeline

In addition to our general concerns with the proposed reporting requirement, the time by which an institution must report to the Superintendent is challenging. Section 500.17 mandates that a bank must notify the superintendent within 72 hours after identifying any material risk of imminent harm. A cybersecurity event is defined in Section 500.01(d) as an attempt, whether successful or not, to gain access. This time frame negatively impacts the bank and DFS personnel without a corresponding benefit. We recommend that the time frame be lengthened and the classification of reportable information be narrowed to cover only significant and/or systemic events on which DFS must take action.

Certification Requirements

Section 500.17 also requires that the bank's board chair submit to the Superintendent annually a certification that the bank is in full compliance with the proposed regulation. The

[9] The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Incident Response Guidance) outline the steps a financial institution should take when unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer occurs. The components, according to the Guidance include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused;
- Prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention;
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence; and
- Notification to customers when warranted.

[10] Ibid. Section 500.17(a)(2).

chair of the bank is not nor should not be in a position to sign a statement guaranteeing full compliance. It is the chair and board's obligation to ensure that a cybersecurity policy is in place and management is implementing the same. It should not, however, fall to the chair or the board to audit all the activities of management or third party contractors to ensure that they are in compliance with every aspect of this regulation, particularly since the currently drafted regulation is very broad and subject to various interpretations. This certification exposes the certifying party to potential personal liability if the bank is found to be noncompliant and overreaches from a corporate governance and practical perspective. There is no defensible rationale which supports this punitive approach. No evidence exists that community banks have intentionally or otherwise neglected to deal with cybersecurity issues. To date no community bank in New York State has been subject to a security breach.

Chief Information Security Officer and Personnel

Section 500.04 requires a bank to designate a "qualified individual," which is undefined, to serve as chief security information officer (CISO). In community banks, personnel often hold multiple positions such as compliance officer, risk management officer, etc. New York Community banks would likely be required to add a person with the title required by the regulation, which would mandate an executive designation for such person. Adding such a position would add substantial costs to small banks. Although the proposed rule recognizes a third party service provider as a possible alternative to a CISO, such an option would also be an increased financial cost to the bank as well as expanded liability for the provider.

In addition to a designated CISO, Section 500.10 requires the bank to employ sufficient personnel to manage cybersecurity risks and to provide such personnel with regular training. This provision appears to contradict the possibility of delegating CISO duties to a third party

service provider. It also provides DFS with broad authority to mandate that banks add cybersecurity employees. Such a provision is not commensurate with a bank's risk profile but leaves unfettered authority with DFS to mandate an undefined level of employment, which is an overreach of authority. The bank needs to be responsible for their personnel.

To underscore our concerns with Section 500.10, according to the 2015 (ISC)[2] "Global Information Security Workforce Study,"[11] the projected shortfall in cybersecurity professionals is expected to be 621,000 people worldwide in 2016 (271,000 people for the Americas); 901,000 people worldwide in 2017 (389,000 people for the Americas); 1,172,000 people worldwide in 2018 (516,000 people for the Americas); and 1,536,000 people worldwide in 2019 (649,000 people for the Americas). As the demand for cybersecurity professionals increases not only locally but globally, community banks will be forced to compete with megabanks with unlimited resources, as well as with other industries, offering excessive salaries and benefits. This puts community banks at a disadvantage that could be negatively assessed by the Department.

In addition, the DFS proposal does not recognize that community banks may participate in shared resource arrangements to achieve compliance and economies of scale. In September 2016, the Conference of State Bank Supervisors released a white paper entitled "Shared Resource Arrangements: An Alternative to Consolidation" (CSBS Paper or "paper").[12] The paper states a well-known fact – that "[c]ommunity banks face particular regulatory and operational cost challenges compered to their competitors…[they] often compete with large banks who benefit from economies of scale and nonbank financial institutions that are not subject to the

[11] Frost & Sullivan. 16 April 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

[12] Conference of State Bank Supervisors. "Shared Resource Arrangements: An Alternative to Consolidation". September 2016. https://www.csbs.org/news/presentations/annualreports/Documents/Shared%20Resource%20Arrangements%20Whitepaper%20FINAL.pdf

same degree of regulatory requirements."[13] The paper underscores a recent Congressional Research Service report that specialized expertise such as information systems may be more costly for smaller firms than their larger counterparts. For community banks, especially smaller community banks including state chartered community banks in New York, shared arrangements help provide the specialized expertise, reduce costs and increase efficiencies. The paper highlights the potential benefit of shared arrangements in information security areas for community banks.[14] The CSBS paper further explains the operational and business risk of shared arrangements along with possible mitigation techniques including existing Federal regulatory guidance.[15]

Multi-Factor Authentication, Encryption and Testing

There are a number of requirements including multi-factor authentication,[16] encryption of non-public information in transit and at rest,[17] penetration testing annually,[18] vulnerability assessments quarterly[19] and maintaining audit trail systems[20] which are required without regard to the risk profile of the banks. Penetration testing and vulnerability assessments are used by community banks; based, however, on the bank's judgment that such procedures are commensurate with their risk exposure. It is critical that there is a reasonable correlation between the regulation and the risk profile of a bank and the cybersecurity regulatory requirements. Regulatory mandates beyond the risk profile of an institution exposes that institution to unnecessary, and oftentimes, costly, testing without any apparent benefit to the institution or

[13] Ibid. Page 4.
[14] Id., Pages 6-7.
[15] Ibid, Pages 9-10.
[16] Proposed Regulation. Section 500.12
[17] Ibid. Section 500.15 and 500.11.
[18] Id., Section 500.05(a)(1).
[19] Section 500.05(a)(2).
[20] Section 500.06.

customers of that institution. Requirements such as these, including the application of encryption requirements to non-public information would represent a significant cost factor for community banks.

Non-Public Information

Section 500.01(g) defines the term non-public information. The definition in Section 500.01(g) is too broad and provides a significant expansion from General Business Law 899-aa, which regulates data breaches and defines private information in the nature of personal information relating to Social Security Number, driver's license number or account information. The proposed regulation's broad definition does not distinguish personal information based on the nature and sensitivity of the information making its scope extremely broad.

Third Parties

Section 500.11 provides that banks are required to include in the contracts of third party service providers the right to perform audits and a representation and warranty that their product is free of mechanisms which would impair the security of the bank's systems or new public information. This provision disproportionately impacts community banks more than their megabank counterparts as community banks use third parties to a larger degree than megabanks. As a result, community banks would be required to do more audits and simply do not have the resources to conduct such audits on all additional third parties. Conducting these audits would be costly and more than likely, most community banks would hire a third party to perform these audits.

Community banks do not enjoy the same market share to leverage third party contract negotiations in their favor as larger banks do so it is therefore doubtful that third party providers would agree to the representations and warranties proposed in the regulation. If a third party does agree, it may come with a significant cost.

IBANYS and ICBA encourages DFS to consider certification of critical cybersecurity vendors rather than relying on the community banks to police third party service providers. This would accomplish the presumed goal of this regulation - to ensure that the safety of customer data is well-protected from cybersecurity threats. Certification by DFS will provide an assurance to the bank that the third party is qualified to provide services required by the regulation. Simply stated, DFS should undertake the certification of third party vendors directly rather than placing the burden of policing and examining these vendors on the bank.

Reporting Requirements as Regulatory Burden and Not Information Sharing

Every sector of American business faces countless cyberattack attempts every day. Reporting potential attacks would result in a flood of reports to the Department by financial services companies across the state that contain detailed and critical information. The Department should inform industry stakeholders what will be done with this information including whether it will remain confidential, how the information will be sorted, and how the information will be used during bank examinations. Also, it is critical to understanding the purpose of gathering this information and whether it will be used for the purposes of sharing information to fend off existing, future and/or potential cyber-attacks.

If the Department plans to use the reports for the purposes of information sharing, it is important to know how the information is collected, analyzed, anonymized and distributed to the financial services companies under the Superintendent's purview. A much broader infrastructure already exists for just this purpose through the FS-ISAC and other public-private partnerships and we strongly recommend that the Department utilize the existing information sharing channels already in place.

The Department may justify requiring this information to be reported to the Superintendent based on the findings of the Department's 2014 Survey[21] which claimed "less than 25% of small institutions" reported membership in an ISAC. As stated earlier in this letter, the findings from the survey, which "helped to inform the rulemaking process,"[22] is dated information. This is particularly true when reviewing the number of community institutions utilizing information sharing services, such as those offered through the FS-ISAC. While the Survey indicates a low adoption rate amongst community institutions, the fact is information-sharing has drastically increased since the Department's survey. While the FS-ISAC does not have membership numbers specific to New York State, cumulatively they have 7,000 members with over 3,500 of those as members of the Community Institution Council (CIC), which is a designated community within the FS-ISAC for community institutions. The CIC has seen an increase of 642% since 2013. We respectfully suggest that the data used to substantiate the proposed regulation may no longer be an accurate reflection of the institutions participating in information sharing within New York State and recommend the Department conduct a more recent survey before issuing a final rule.

In addition to the public-private partnerships, the United States Congress passed, and the President signed, the "Cybersecurity Information Sharing Act of 2015 ("CISA")."[23] This law permits voluntary, reciprocal sharing of cyber threat indicators and defensive measures by non-federal entities with the Federal government. Guidance was issued jointly by the Department of Homeland Security and Department of Justice on June 15, 2016 ("Guidance").[24] For existing FS-

[21] http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf. Page 2.
[22] New York Department of Financial Services. Press Release. 13 September 2016. "Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions." http://www.dfs.ny.gov/about/press/pr1609131.htm
[23] U.S. Congress. Public Law 114-113, "Consolidated Appropriates Act, 2016" Division N, Title I. https://www.congress.gov/bill/114th-congress/house-bill/2029/text.
[24] Department of Homeland Security and Department of Justice. "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015." 15 June 2015. https://www.us-cert.gov/sites/default/files/ais_files/Non-

ISAC users, including community banks that already share information through the FS-ISAC, the Act provides clarity of the legal protections provided to institutions that voluntarily share cyber threat indicators and defensive measures. For institutions that do not use the FS-ISAC for these purposes, this Act permits community banks the ability to share cyber threat indicators and defensive measures through a variety of new voluntary methods: through the DHS's Automated Indicator Sharing (AIS) initiative,[25] a web form on a DHS National Cybersecurity and Communications Integration Center (NCCIC) website, or through email. Sharing information through these avenues, including via FS-ISAC, provides community banks certain legal protections, provided that the shared information meets the criteria as set forth in the Guidance and does not include personal information.[26] As a result of this, the information reporting requirement in the proposed regulation is redundant and unnecessary.

The financial services sector is often recognized as the most advanced sector in terms of cybersecurity preparedness. This is, in large part, due to the sector's recognition of the great importance of the data held by its participants. To protect that data, institutions of all sizes share information with each other to enable consistent information sharing across the entire banking sector. It also assists institutions of all sizes, including community banks, in detecting and mitigating a broad range of cyber threats which are ever-evolving and quickly changing. Put concisely, information sharing, when done with the intent of truly sharing information and not for simply reporting requirements, leads to a more resilient banking sector.

The Department should encourage information sharing through the existing channels rather than mandating excessive reporting requirements.

Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf. See also: https://www.us-cert.gov/ais. Referred to hereinafter as "Guidance."

[25] DHS AIS uses a "technical specification for the format and exchange of cyber threat indicators and defensive measures using the Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)". See page 13 of "Guidance".

[26] FS-ISAC operating rules dictate that an institution must remove personal information from threat information before sharing that information with FS-ISAC.

Enforcement Authority

Section 500.19 of the proposed rule provides the Superintendent with broad enforcement authority under any applicable laws including the enforcement authority under both the Banking Laws and Financial Services Law. This approach permits the Superintendent to fashion a penalty without specific notice of such penalty for a violation of a specific requirement to the offender prior to the offense. The Financial Services Law in Article Four, provides significant penalties for fraud and misrepresentation in addition to a general penalty authority provided to the Superintendent pursuant to Banking Law, Section 44 under this regulation. There should be express penalties attached to violations of the regulations not an open ended list of penalties that are available without limitation or relationship to the offense. This approach permits the Superintendent to fashion a penalty without any specific notice of the penalty for a violation of a specific requirement to the offender prior to the offense.

The regulatory focus in New York should be on assisting banks in identifying their appropriate risk profile and providing assistance to ensure that banks have appropriate tools to mitigate cybersecurity threats, which corresponds to their risk profiles.

Education

Education is a critical part of an effective cybersecurity regulatory regime, not only for the regulated banks but also for the Department of Financial Service examiners. Regulators examining financial institutions in cyber security measures, including DFS personnel tasked with examining New York banks for this issue, would need significant training to effectively discharge the oversight required on this regulation, if finalized as proposed. This regulation

should not simply require that a box be checked. Rather it should be predicated on a continuing conversation between the regulator and the bank to achieve an appropriate level of cybersecurity. Implementation of such sweeping regulations should be dependent on DFS staff being prepared with adequate training to ensure balanced enforcement.

Conclusion

To achieve the best result for the public and the regulated community, we are requesting that the Department does not issue a final rule, but rather issue a revised proposal incorporating our comments, and requesting additional comments from the industry. This will enable community banks, the financial services industry, third party vendors and federal regulators to work collaboratively to issue balanced regulations that effectively attack and mitigate current and potential cyber threats.

IBANYS and ICBA respectfully request that this proposed regulation be held in abeyance pending resolution of the following:

- Collaboration with Federal regulatory bodies, including the FFIEC to achieve a consensus for addressing cybersecurity issues. The end goal should be to ensure that no significant regulatory divide exists between state and federally chartered banks, which would encourage charter flipping; and

- Permitting community banks to adopt a reasonable risk assessment tool which would achieve an appropriate level of cybersecurity preparedness and would be used by DFS in the conduct of any examination for cybersecurity compliance. This would allow recognition of different

risk profiles of small community banks and those of large systemically important banks by not subjecting them all to the same requirements; and

- Consideration of certification of third party cybersecurity vendors by DFS; and
- Providing additional time for DFS to prepare and educate its personnel on cybersecurity issues so that there is an effective workforce to assist and regulate the banks in meeting their regulatory obligations; and
- Reconsidering the requirement that the chair of the board of directors would be required to provide a blanket compliance statement; and
- Eliminating the purpose of mandatory information reporting and clarifying the types of incidents to be reported to the Superintendent; and
- Extending the time period by which a bank must report an incident; and
- Including the utilization of shared resources by community banks as a means to obtain economies of scale.

Community banks are unique financial institutions in New York State. Small in size, they strive to serve their communities and are trusted statewide. However, as the regulatory burden increases, so too, does the cost of compliance. Community banks are not asking to be exempted from regulations where it is appropriate; however, regulations should be based on the size of the institution and the operative business model. The continued viability of the community bank model is dependent both on regulatory recognition of a targeted approach based on risk profiles and a consistent approach by the state and federal regulators.

Your consideration of our collective comments is greatly appreciated. If you have any questions, please don't hesitate to contact the undersigned.

Respectfully submitted,

/s/ William Y. Crowell III

William Y. Crowell III
Of Counsel, Cozen O'Connor

Jeremy J. Dalpiaz
Assistant Vice President, Cyber Security and Data Security Policy
Independent Community Bankers of America