New York State Department of Financial Services Proposes New Cybersecurity Regulations

October 13, 2016

In September 2016, the New York State Department of Financial Services (the "**NYDFS**") proposed new **cybersecurity regulations** (the "**Proposed Rules**") for banks, insurance companies and other financial institutions regulated by the NYDFS ("**Covered Entities**").[1] The Proposed Rules reflect an ongoing interest in cybersecurity by the NYDFS and other regulators as a result of recent high-profile cyberattacks on banks and other institutions, such as the **attack on the Bangladesh Central Bank** earlier this year.[3] The NYDFS's interest in this area has been especially pronounced given New York's importance to the financial markets and was evidenced by the fact that the Proposed Rules were announced by New York Governor Andrew Cuomo.

The Proposed Rules would require each Covered Entity to establish and maintain a cybersecurity program[4] with the following specific elements, among others:[5]

- a written cybersecurity policy;
- a chief information security officer ("**CISO**");
- annual penetration tests and quarterly vulnerability assessments;
- a written incident response plan;

Covered Entities include the following types of entities, among others, chartered or licensed by the NYDFS.

- Insured depository institutions;
- Branches, agencies or offices of a non-U.S. bank;
- Trust companies;
- Credit unions;
- Check cashers;
- Money transmitters;
- Institutions with BitLicenses;[2] and
- Mortgage brokers.

Institutions that would not be Covered Entities include, for example:

- National banks or banks chartered in other states, including their New York branches;
- Federal credit unions;
- Broker-dealers;
- OCC-chartered branches or agencies of non-U.S. banks; and
- An affiliate of a Covered Entity that is not itself a Covered Entity.

---

[1] Covered Entities that have less than $10 million in year-end total assets and that meet certain other conditions are exempt from many, but not all, of the requirements under the Proposed Rules.

[2] *See* Davis Polk Visual Memorandum, New York's Final "BitLicense" Rule (June 5, 2015), available **here**.

[3] The Federal Deposit Insurance Corporation ("**FDIC**") may also be considering proposing cybersecurity regulations. *See* FDIC Board Meeting Agenda for October 19, 2016, available **here**. Regulatory concern over cybersecurity is apparent not only in the United States, but also internationally. Finance ministers and central bank governors of the G-7, including the U.S. Department of the Treasury and the Board of Governors of the Federal Reserve System, published on October 11, 2016 a list of eight Fundamental Elements of Cybersecurity for the Financial Sector ("**G-7 Fundamental Elements**"), available **here**. In June 2016, the Committee on Payments and Market Infrastructures ("**CPMI**") and the Board of the International Organization of Securities Commissions, two international standard-setting bodies, released guidance on cyber resilience for financial market infrastructures, available **here**. The press release for this guidance noted that it was the first internationally agreed guidance on cybersecurity for the financial industry. In addition, in September 2016, the CPMI announced that it established a task force to review the security of wholesale payments that involve banks, financial market infrastructures and other financial institutions. *See* Press Release, CPMI, Central Banks are Reviewing Wholesale Payments Security (Sept. 16, 2016), available **here**.

[4] The cybersecurity program must be designed to (i) identify cybersecurity risks, (ii) protect the Covered Entity's information systems using defensive infrastructure and the implementation of policies and procedures, (iii) detect cybersecurity events, (iv) respond to detected cybersecurity events, (v) recover from cybersecurity events, and (vi) fulfill all regulatory reporting obligations.

[5] *See* Davis Polk's recent podcast series on cybersecurity risks that should be considered by boards, **Before the Board: Cybersecurity Risks and Responses – Part 1** and **Part 2** (August 8 and September 23, 2016), and a CLE presentation on **the Role of Lawyers Before, During and After a Cyber Event** (Nov. 5, 2015).

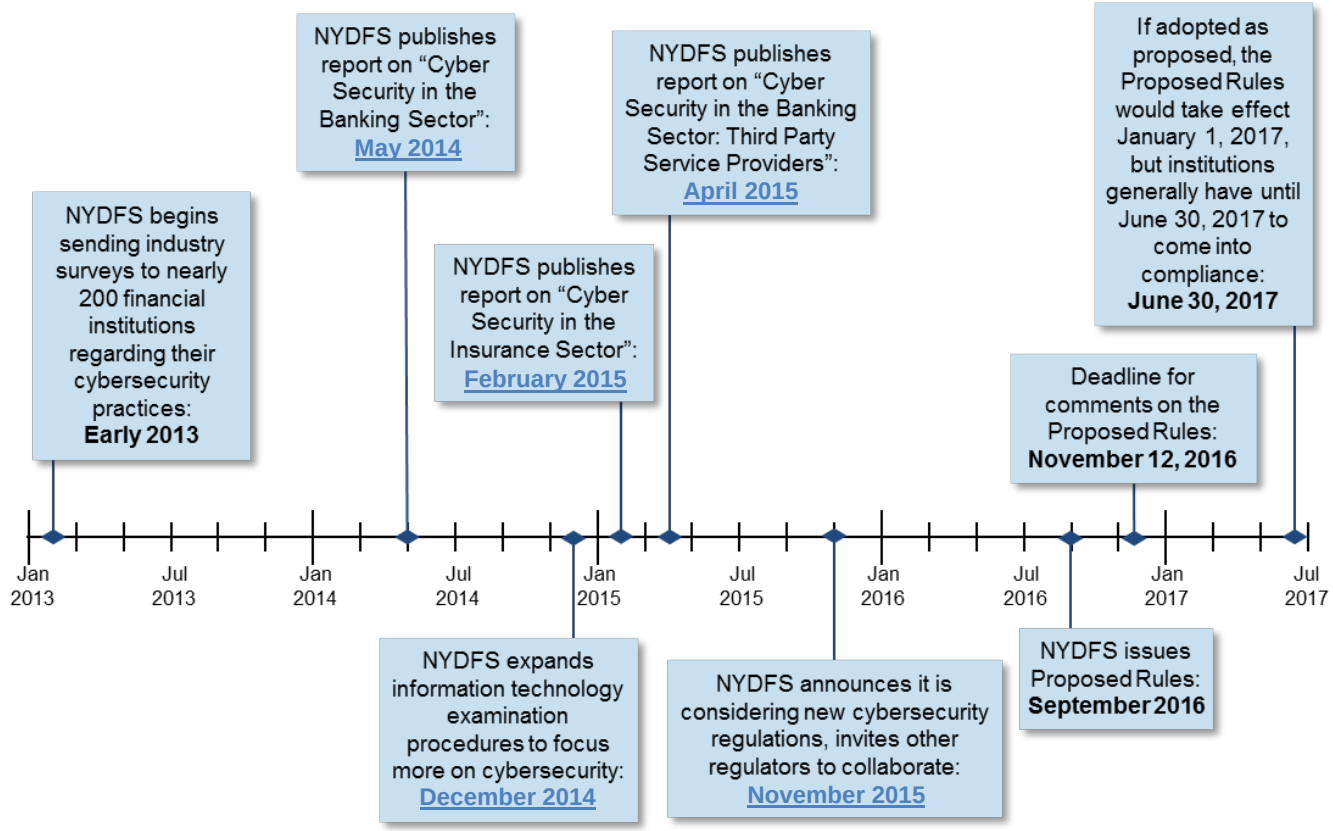
- encryption of nonpublic information in transit and at rest;
- notifications to the NYDFS within 72 hours of certain cybersecurity events; and
- annual certifications of compliance signed by the board of directors or a senior officer.

In some respects, and as discussed further below, the Proposed Rules would go beyond existing federal-level cybersecurity requirements. For example, the Proposed Rules would require each Covered Entity to encrypt all Nonpublic Information (which is broadly defined), rather than allowing the entity to determine what data to encrypt based on a risk assessment, as is currently required. In addition, the Proposed Rules would require each Covered Entity to notify the NYDFS of certain cybersecurity events within 72 hours, which is a shorter timeframe than is required under existing state and federal data breach notification rules. The Proposed Rules would also impose entirely new requirements. For example, on an annual basis, the board of directors or a senior officer of each Covered Entity would be required to certify to the NYDFS that the Covered Entity is in compliance with the Proposed Rules. This annual certification requirement potentially imposes personal liability for boards of directors or senior officers signing such certification.

"Nonpublic Information" would generally include information that is not publicly available and that is (1) business related information of the Covered Entity that, if disclosed, accessed or used on an unauthorized basis, would cause a material adverse impact; (2) information that a Covered Entity obtains about an individual in connection with providing a financial product or service to that individual; (3) health-related information about any individual; (4) information that could be used to distinguish or trace an individual's identity.

The timeline below illustrates the actions taken by the NYDFS with respect to cybersecurity over the last several years, including the publication of the Proposed Rules, and notes when comments are due and when the Proposed Rules are expected to become effective.

Timeline of Actions Taken by the NYDFS on Cybersecurity



Comparison to Existing Rules and Guidance

Although the press release announcing the Proposed Rules declared that it is a "first-in-the-nation cybersecurity regulation," financial institutions operating in New York are already subject to various existing cybersecurity rules and guidance. For example, banks must comply with federal Interagency Guidelines Establishing Information Security Standards on safeguarding the confidentiality and security of customer information (the "**Security Guidelines**"), which were issued pursuant to the Gramm-Leach-Bliley Act of 1999.[6] These institutions must also take into account the Federal Financial Institutions Examination Council's ("**FFIEC**") Information Security Booklet ("**FFIEC Guidance**"),[7] which was updated in September 2016. Covered Entities that are affiliated with public companies may also need to consider applicable requirements of the Securities and Exchange Commission, among other federal requirements.[8] In addition to federal requirements, New York and most other states also maintain data breach laws that require notifications to relevant regulators (e.g., the state attorney general), as well as to customers and third parties whose data has been compromised.[9] Financial institutions have also voluntarily strengthened cybersecurity protections as a result of business and reputational concerns.[10]

The Proposed Rules are largely consistent with the existing federal cybersecurity rules and guidance and existing cybersecurity practice. For example, pursuant to the FFIEC Guidance and the Security Guidelines, firms are already expected to conduct risk assessments, designate an information security officer and establish a written cybersecurity policy. However, the Proposed Rules go beyond existing requirements in various ways; for example:

- ***Encryption of Nonpublic Information.*** Covered Entities would be required to encrypt all Nonpublic Information (as defined in the sidebar), whether in transit or at rest.[11] The FFIEC Guidance, on the other hand, notes that decisions regarding what data to encrypt and whether to encrypt it at rest or in transit should be based on the risk of disclosure and the costs of encryption. In addition, the broad definition of Nonpublic Information under the Proposed Rules could require encryption of various internal documents and emails that Covered Entities may not already

> The Proposed Rules do not define information "at rest" or "in transit." Information at rest generally refers to data that is held on a single system – on its hard drive or in memory – and is not in motion. Information in transit refers to information when it is being transferred from one system to another, for example through the internet.

[6] *See* 12 CFR 30, appendix B (OCC); 12 CFR 208, appendix D-2 and 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA).

[7] The FFIEC is composed of the principals of the following: the Board of Governors of the Federal Reserve System ("**FRB**"), the FDIC, the National Credit Union Administration ("**NCUA**"), the Office of the Comptroller of the Currency ("**OCC**"), the State Liaison Committee ("**SLC**"), and the Consumer Financial Protection Bureau ("**CFPB**"). Although the FFIEC Guidance is not a formal regulation, it is used by bank examiners in assessing the level of security risks to a financial institution's information systems and, as such, sets forth regulatory expectations with respect to financial institutions' cybersecurity programs.

[8] Many Covered Entities will be subsidiaries of public companies that must comply with the Securities and Exchange Commission's expectations regarding cybersecurity programs and reactions to cybersecurity events, such as the expectation that public companies will publicly disclose material cybersecurity breaches. *See* SEC, CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 13, 2011), available here (noting that a significant cyber event triggers the materiality reporting requirements).

[9] *See*, *e.g.*, N.Y. Gen. Bus. Law. § 899-aa.

[10] In the introduction to the Proposed Rules, the NYDFS itself recognized that firms have proactively increased their cybersecurity programs with great success. Many institutions have adopted the Framework for Improving Critical Infrastructure Cybersecurity, a voluntary cybersecurity framework published in February 2014 by the National Institute of Standards and Technology ("**NIST**") pursuant to an executive order from President Obama. The SEC has suggested that it regards the NIST standard as a baseline for regulated companies, as noted here. Institutions will also likely review and consider incorporating into their cybersecurity approaches the October 2016 G-7 Fundamental Elements.

[11] In addition to developing their own encryption processes, Covered Entities would be required to establish preferred provisions to be included in contracts with third-party service providers addressing the use of encryption to protect Nonpublic Information.

be encrypting. Perhaps recognizing that it may be difficult for Covered Entities to encrypt all Nonpublic Information, the NYDFS adopted a transition period for this requirement. Specifically, to the extent that the required encryption is infeasible, Covered Entities would be able to use appropriate alternative compensating controls approved by the Covered Entity's CISO until January 2018, with respect to information in transit, and January 2021, with respect to information at rest.

- ***Notifications to the NYDFS Superintendent.*** Each Covered Entity would be responsible for notifying the NYDFS Superintendent within 72 hours of becoming aware of a cybersecurity event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects its Nonpublic Information or if it identifies any material risk of imminent harm relating to its cybersecurity program. The Proposed Rules clarify that such a cybersecurity event would include any cybersecurity event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information. These triggers for notification are much broader than is currently the case under the FFIEC Guidance, the Security Guidelines and state data breach notification laws.[12] In addition, the 72-hour timeframe is shorter than under existing federal and state requirements,[13] but is consistent with certain European regulations.[14] This amount of time may be insufficient to allow a Covered Entity to determine whether Nonpublic Information was accessed and could trigger burdensome reporting obligations where it later turns out there was no material risk to the Covered Entity's operations or Nonpublic Information. The fact that the 72-hour timeframe is shorter than under other state and federal requirements will help ensure that the NYDFS is the first regulator that begins to investigate a cybersecurity event, and may reflect the NYDFS's attempt to become a primary regulator in this area.
- ***Annual Certification of Compliance.*** On an annual basis, the board of directors or a senior officer of a Covered Entity would be required to certify to the NYDFS that, to the best of the board's or senior officer's knowledge, the Covered Entity is in compliance with the Proposed Rules.[15] This certification of compliance could potentially subject the directors or officers signing such certification to personal liability under New York laws prohibiting false statements to the NYDFS.[16]
- ***Enforcement.*** Because the FFIEC Guidance is a set of expectations for examiners and not a formal regulation, an examiner could issue a supervisory notice requiring an institution failing to comply with

---

[12] Forty-seven states plus the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted cybersecurity breach notification laws, collectively referred to as "state data breach notification laws." State data breach notification obligations are typically triggered by the discovery of a breach or the reasonable belief that a breach has occurred. Furthermore, the information covered under state data breach notification laws is generally limited to particular types of data (for example, a person's social security number, driver's license number, state identification card number, passport number, or taxpayer identification number), which is narrower than the definition of Nonpublic Information under the Proposed Rules.

[13] Although the timing requirements under certain state data breach notification laws are non-specific (for example, notice must be provided in the "most expeditious time possible" or "without unreasonable delay"), several states clarify that notice must be provided no later than 10, 30, 45 or 90 days following the trigger, with 30 or 45 days being the most common.

The 72-hour timeframe under the Proposed Rules is consistent with the Department of Defense ("**DOD**") requirement that its contractors report cyber incidents implicating non-classified DOD information or other non-classified information related to the contract within 72 hours of discovering the incident. *See* 32 CFR 236.4. However, given the heightened sensitivity of data breaches relating to DOD data (even when non-classified), the 72-hour timeframe for notification of breaches relating to any Nonpublic Information under the Proposed Rules is particularly striking.

[14] *See*, e.g., the European Union's General Data Protection Regulation.

[15] If the Proposed Rules are adopted as proposed, the first certification would be due by January 15, 2018. In addition, each Covered Entity would be required to maintain for examination by the NYDFS all records, schedules and data supporting this certification for a period of five years.

[16] *See*, *e.g.*, New York Banking Law § 672.

the FFIEC Guidance to remediate such failure (*e.g.*, via an MRA or MRIA) but a regulator could not immediately bring an enforcement action. By contrast, the Proposed Rules would be directly enforceable by the NYDFS leading to public orders and/or fines (the Security Guidelines are also enforceable by the relevant federal agencies).

- ***Minimum Timeframes.*** The Proposed Rules would establish minimum timeframes for various processes, such as penetration testing (annually), vulnerability assessments (quarterly) and risk assessments (annually). By contrast, the FFIEC Guidance generally permits institutions to establish the frequencies for these processes based on the specific risks faced by the institution.

The following table compares the Proposed Rules with the Security Guidelines and the FFIEC Guidance at a high level.

Requirement	Required by New York Proposed Rules	Required by Federal Security Guidelines / FFIEC Guidance
Risk Identification		
Penetration testing	Yes, at least annually	Yes, at a frequency based on risk assessment process
Vulnerability assessments	Yes, at least quarterly	Yes, at a frequency based on risk assessment process
Risk assessments	Yes, at least annually	Yes (frequency not specified)
Governance		
Appointment of an information security officer	Yes (may be satisfied by third-party, subject to conditions)	Yes
Written cybersecurity policy	Yes, which must be reviewed by the board of directors or equivalent governing body[17] and approved by a senior officer at least annually	Yes, which must be reviewed and approved by the board of directors at least annually
Reporting status of cybersecurity program to the board of directors	Yes, at least bi-annually[18]	Yes, at least annually
Training for bank personnel	Yes	Yes
Risk Mitigation		
Limit access to information systems based on job responsibility	Yes	Yes
Security control requirements for internally and externally developed applications	Yes	Yes

[17] If no such board of directors or equivalent governing body exists, the cybersecurity policy must be reviewed and approved by a senior officer.

[18] If no such board of directors or equivalent governing body exists, the report must be presented to a senior officer responsible for the Covered Entity's cybersecurity program. This report must be provided to the NYDFS Superintendent upon request.

Requirement	Required by New York Proposed Rules	Required by Federal Security Guidelines / FFIEC Guidance
Controls relating to third-party service providers, including due diligence and minimum cybersecurity practices	Yes	Yes
Mandatory multi-factor authentication for individuals accessing (i) internal systems from an external network or (ii) database servers that allow access to nonpublic information	Yes	Not explicitly, although robust authentication methods generally required
Procedures requiring destruction of nonpublic information no longer necessary	Yes	Not explicitly, although procedures governing disposal of information required
Encryption of nonpublic information	Yes, in all cases (e.g., transit and at rest), subject to phase-in schedule	Yes, based on risk of disclosure and costs of encryption
Responding to Cybersecurity Events		
Incident response plan	Yes	Yes
Reporting to Regulators		
Notice to regulator upon cybersecurity event	Yes, notice to NYDFS superintendent within 72 hours of cybersecurity event	Yes, notice to primary federal regulator required as soon as possible after becoming aware of unauthorized access to sensitive customer information[19]
Annual certification of compliance by board of directors or senior officer	Yes	Not explicitly

[19] Notifications may also be required pursuant the federal regulators' suspicious activity report regulations. *See* 12 CFR 21.11 (national banks, federal branches and agencies); 12 CFR 163.180 (federal savings associations); 12 CFR 208.62 (state member banks); 12 CFR 211.5(k) (edge and agreement corporations); 12 CFR 211.24(f) (uninsured state branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (state non-member banks); and 12 CFR 390.355 (state savings associations). In addition, as referenced above, notification may also be required under state data breach notification laws.

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

John L. Douglas	**202 962 7126**	**john.douglas@davispolk.com**
Avi Gesser	**212 450 4181**	**avi.gesser@davispolk.com**
Reuben Grinberg	**212 450 4967**	**reuben.grinberg@davispolk.com**
Joseph Kniaz	**202 962 7036**	**joseph.kniaz@davispolk.com**
Jon Leibowitz	**202 962 7050**	**jon.leibowitz@davispolk.com**
Neil H. MacBride	**202 962 7030**	**neil.macbride@davispolk.com**
Gabriel D. Rosenberg	**212 450 4537**	**gabriel.rosenberg@davispolk.com**
Mark Sater	**212 450 3142**	**mark.sater@davispolk.com**
Margaret E. Tahyar	**212 450 4379**	**margaret.tahyar@davispolk.com**