September 15, 2016
Special Edition

Skadden

Privacy & Cybersecurity Update

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

Four Times Square
New York, NY 10036
212.735.3000

New York State Proposes Cybersecurity Regulation for Financial Institutions

New York state has proposed a new regulation — to go into effect January 1, 2017 — that would require banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services (DFS) to establish and maintain a cybersecurity program. The proposal is the result, in part, of a DFS survey of approximately 200 regulated banking institutions and insurance companies regarding the industry's efforts to prevent cyberattacks.

If enacted, this would be the first statewide regulation mandating that financial institutions create such a program. As explained in the introductory section to the proposal, the regulation would set forth fairly general minimum standards. The rationale was to not be "overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances." Although many institutions will find that elements of the proposed regulation are similar to those found in existing regulatory and technical guidance, they have not previously been required as a matter of law. While the related press release and preamble suggest that the rule is flexible and can accommodate an individual institution's situation and technical developments, it also makes clear that the rule is enforceable under the DFS' authority. In addition, how the application of these requirements interacts with the expectations of other regulators with overlapping jurisdiction, and how those requirements are implemented by institutions that operate across multiple states or countries, will have to be examined by each such institution.

The proposed regulation is now subject to a 45-day notice and public comment period before its final issuance. We summarize below the key requirements of the proposed regulation.[1] Entities subject to the new regulation, if it goes into effect, would have 180 days to comply after the effective date.

Who Would Be Covered?

The proposed regulation covers any individual or entity operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under

[1] A copy of the proposed regulation can be found here.

Privacy & Cybersecurity Update: New York State Proposes Cybersecurity Regulation for Financial Institutions

New York state banking, insurance or financial services laws (a Covered Entity), with an exception for small entities.[2]

Nonpublic Information

As discussed below, much of the proposed regulation focuses on systems that include nonpublic information. This is defined as any information that (1) if disclosed or tampered with could cause a material adverse impact to the Covered Entity's business, operations or security, (2) an individual provides to a Covered Entity in connection with obtaining a financial product or service, results from a transaction with the individual, or a Covered Entity otherwise obtains about the individual in connection with providing a financial product or service to that individual, (3) is about an individual's health and is received from a health care provider or individual or from the payment of health care costs, and (4) can be used to distinguish or trace an individual's identity.

The second definition — information relating to the provision of financial products or services —generally tracks how personal information is defined under the Gramm-Leach-Bliley Act and should not be controversial. The third definition, relating to insurance information, is loosely based on the definition provided in the Health Insurance Portability and Accountability Act, but given that the proposed regulation covers a wide swath of businesses that are not engaged in the health care industry, it would require entities to consider how they store and handle employee health information that they might receive.

The final category of what is considered nonpublic information is perhaps the most interesting, since it creates an unusually broad definition of what constitutes personal information. Specifically, it includes not only traditional categories of personal information but also "any information that can be used to distinguish or trace an individual's identity" and "any information that is linked or linkable to an individual, including but not limited to medical, educational, financial, occupational or employment information, information about an individual used for marketing purposes or any password or other authentication factor." This picks up on a new trend to classify information as personal information if it can simply be used as a building block toward identifying an individual. Although publicly available information is carved out of the definition, the Covered Entities will need to carefully consider whether any type of information they have about individuals is nonpublic information. We suspect there will be considerable public comment on these definitions.

[2] Entities with (1) fewer than 1,000 customers in each of the last three calendar years, (2) less than $5 million in gross annual revenue in each of the last three fiscal years, and (3) less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles and including assets of all affiliates, are exempt from certain requirements.

Key Requirements

- Create a **cybersecurity program** designed to ensure the integrity of the Covered Entity's systems that includes the following components:
  - a risk assessment component that identifies the nonpublic information stored on the Covered Entity's systems, its level of sensitivity and how it can be accessed. In this respect, we note that the proposed regulation is similar to the National Institute of Standards and Technology's Cybersecurity Framework, which begins with risk assessment.
  - uses defensive infrastructure and implements policies and procedures to protect information systems and nonpublic information from cyberattacks;
  - detects, responds to and recovers from cyberattacks to mitigate their impact; and
  - complies with regulatory reporting requirements.
- Create a written **cybersecurity policy** document that is approved by a senior officer and reviewed at least annually by the Covered Entity's board of directors or equivalent governing body. The policy addresses, among other matters:
  - information security (which includes physical security and environmental controls as well as systems and network monitoring)
  - business continuity/disaster recovery;
  - data governance and classification;
  - access controls and identity management;
  - systems and application development and quality assurance;
  - customer data privacy;
  - vendor management; and
  - incident response.
- Appoint a **chief information security officer (CISO)** to oversee the cybersecurity program and policy. Interestingly, the CISO can be a third-party provider as long as the Covered Entity remains responsible for the program and policy; designates a senior representative to oversee the CISO; and ensures the third-party provider itself complies with the proposed regulation.
  - The CISO must develop a biannual cybersecurity report for the board (or equivalent governing body), or, where no governing body exists, to a senior officer. The report must be made available to the DFS superintendent upon request. In general, the report must summarize the state of the program and policy, any cyberattacks, new risks and steps to address any inadequacies.

- Conduct **penetration testing** and a **vulnerability assessment** at least once a year. This is one of the few specific requirements in the proposed regulation (along with the multifactor authentication requirements discussed below) and reflects the widespread acceptance of the importance of such regular testing and assessment.
- Implement and maintain an **audit trail** system that, among other specified items, can track and log access and allow data to be reconstructed in the event of an attack. The audit documents must be preserved for at least six years.
- Limit access to systems to only those who require such access.
- Secure **development practices for in-house developed applications and procedures** for assessing and testing the security of externally developed applications (reviewed annually by the CISO).
- Create an **annual, written risk assessment**.
- **Employ cybersecurity personnel** sufficient to manage the Covered Entity's cybersecurity risks and perform the core cybersecurity functions. We believe this is among the more ambiguous requirements of the proposed regulation, since it will be unclear to most Covered Entities how large a staff satisfies this requirement. These individuals must be regularly trained and, adding to the uncertainty of the requirement, must keep abreast of "changing threats and countermeasures." A third party can be retained to fill this staffing role.
- Implement **written vendor policies** for any vendor that can access the Covered Entity's information systems. This includes risk assessment and due diligence of the Covered Entity as well as minimum cybersecurity standards they must meet. These third parties must be reassessed on at least an annual basis.
  - The vendor policies should include preferred contract provisions to include vendor contracts that might include those relating to multifactor authentication (where applicable); use of encryption to protect nonpublic information in transit and at rest; prompt notice in the event of a cyberattack; identity protection services for customers materially impacted by an attack that results from the third party's negligence or willful misconduct; reps and warranties that the third party's products and services are free from viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's information systems or nonpublic information; and an audit right. We expect that this requirement will provide Covered Entities with considerable leverage when negotiating with vendors on these points.
- Require **multifactor authentication** for any individual accessing the Covered Entity's internal systems or data from an external network and require **risk-based authentication** in order to access web applications that capture, display or interface with nonpublic information. Risk-based authentication are systems that detects anomalies or changes in an individual's normal use patterns and requires additional verification, such as through the use of challenge questions.
- Limit **data retention** by destroying nonpublic information when it is no longer required, except where such information is otherwise required to be retained by law or regulation.
- **Monitor usage** to detect unauthorized access, use or tampering of nonpublic information.
- Provide **cybersecurity awareness training**.
- **Encrypt** all nonpublic information held or transmitted by the Covered Entity both in transit and at rest. The CISO also can approve secure methods aside from encryption in the short term, but Covered Entities must comply with encryption in transit within one year and encryption at rest within five years. The longer period for adopting encryption for data at rest reflects the reality that most Covered Entities likely do not implement such encryption today and would need to devote time and resources to comply.
- **Create a cyberattack incident response plan.** The plan must include, among other matters, the internal processes for responding to an attack, clearly defined decision-making authority, external and internal communications and information sharing, documentation and reporting, and evaluation of the event.
- Provide **notice to the DFS superintendent** of a cybersecurity event. While many Covered Entities likely already take many or all of the other steps required by the proposed regulation, this would be a new reporting requirement. Covered Entities would be required to:
  - notify the superintendent of any event affecting nonpublic information, where notice was provided to any other government body or self-regulatory agency or that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity. Notification must occur as promptly as possible but **no later than 72 hours** after the Covered Entity becomes aware of the event; and
  - provide an annual certification by January 15 (using a form provided by DFS) that the Covered Entity complied with this requirement. (The documents and records supporting the certification must be kept for five years) This annual report must document any remediation efforts that are underway. Assuming the proposed regulation goes into effect on January 1, 2017, the first annual report would not be required until January 2018. As is the case with the DFS anti-money laundering rule, we expect that many Covered Entities will focus on this requirement, especially given that the DFS has made explicit its authority to enforce the rule.

Privacy & Cybersecurity Update: New York State Proposes Cybersecurity Regulation for Financial Institutions

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Joseph L. Barloon
Partner / Washington, D.C.
202.371.7322
joseph.barloon@skadden.com

Jamie L. Boucher
Partner / Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

James R. Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian D. Christiansen
Partner / Washington, D.C.
202.371.7852
brian.christiansen@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Richard J. Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy S. Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Anand S. Raman
Partner / Washington, D.C.
202.371.7019
anand.raman@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

William J. Sweet, Jr.
Partner / Washington, D.C.
202.371.7030
william.sweet@skadden.com

Helena J. Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com