SPECIAL ALERT: REVISED NYDFS CYBERSECURITY RULE

On December 28, 2016, the New York Department of Financial Services (DFS) issued a revised version (Revised Proposed Rule) of its cybersecurity rule for financial institutions issued on September 13, 2016 (Proposed Rule). The revision came after DFS received more than 150 comments in response to the Proposed Rule, as well as a hearing before New York State lawmakers. The Revised Proposed Rule retains the spirit of the original Proposed Rule, but offers covered entities somewhat more flexibility in implementing the requirements.

Background

The Proposed Rule marked the next step in a period of increased focus on cybersecurity by the agency. Between May 2014 and April 2015, DFS issued three reports relating to cybersecurity in the financial and insurance industries. In November 2015, DFS issued a letter to federal financial services regulatory agencies, which alerted the federal regulators to DFS's proposed regulatory framework and invited comment from the regulators.

In the September release, DFS explained that the Proposed Rule is a response to the "ever-growing threat posed to information and financial systems by nation-states, terrorist organizations, and independent criminal actors." As originally written, the Proposed Rule covered financial institutions operating under a charter or license issued by DFS, and set cybersecurity program, policy, training, and reporting requirements that are more stringent than the current federal requirements. The Proposed Rule gave a January 1, 2017 effective date, with a 180-day transitional period. Taking into consideration these concerns, on December 19, 2016, the New York State Assembly's Standing Committee on Banks held a public hearing regarding cybersecurity and the Proposed Rule. Among the chief concerns expressed at the hearing and in the comment letters was the cost of compliance, especially for smaller banks, and that the Proposed Rule's "one-size-fits-all" requirements do not consider the varying operational structures, business models, and risk profiles of financial institutions. There was also concern that the Proposed Rule was too different from the current federal requirements.

Financial institutions also took issue with certain specific requirements of the Proposed Rule, including:

- Incident reporting requirements, which instruct covered entities to report a cybersecurity event to DFS within 72 hours—regardless of whether or not the attempt was successful.
- Very broad third party oversight requirements that are more stringent than federal requirements under the GLBA Safeguards Rule.
- A broad scope of coverage, particularly because of the defined term "Nonpublic Information," which includes not only personally identifiable information, but also certain proprietary business information.
- A mandate that covered financial institutions must have a Chief Information Security Officer.
- Stringent audit trail requirements, including that audit trail materials must be maintained for at least six years.

- Requirements that Nonpublic Information must be encrypted both in transit and at rest.

Revised Proposed Rule

Two days after the hearing, DFS announced that it would revise and reissue the Proposed Rule. On December 28, 2016, DFS released the Revised Proposed Rule. In general, the Revised Proposed Rule provides (1) longer timeframes for compliance with its requirements, (2) more flexibility for compliance with certain requirements and acknowledgement that some requirements may not be applicable to all financial institutions, and (3) clarifications to certain key definitions.

More specifically, the Revised Proposed Rule has been revised as follows:

- The definition of "Nonpublic Information" has been narrowed to cover a smaller pool of information, though certain proprietary business information is still included.
- Although a Covered Entity must designate a qualified individual to oversee the Cybersecurity Program and Policy, the person no longer must have the title of Chief Information Security Officer.
- Monitoring and testing performed to assess the effectiveness of a Cybersecurity Program must include "continuous monitoring or periodic penetration testing and vulnerability assessments, and shall be done periodically."
- The required record retention for audit trails has been reduced from six years to five years.
- Requirements on employee access to Nonpublic Information have been relaxed.
- The frequency of mandated risk assessments of Third Party Service Providers is now based on risks presented.
- Although data nonretention requirements remain in the Revised Rule, the situations in which data may be retained have been broadened.
- While requirements for encryption of Nonpublic Information have been retained in the Revised Rule, the requirements have been clarified and a provision for compensating controls where encryption at rest is infeasible has been added.
- The Incident Response Plan need only address Cybersecurity Events materially affecting the Covered Entity's Information Systems.
- The circumstances under which Cybersecurity Events must be reported to DFS have been narrowed. Cybersecurity Events that require reporting are those that (1) are required to be provided to any government body, self-regulatory agency, or supervisory body; and (2) have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.
- Disclosure of information by the Covered Entity is subject to exemptions pursuant to the Banking Law, Insurance Law, Financial Services Law, Public Officers Law, or any other applicable state or federal law.
- The effective date has been moved back two months to March 1, 2017.

- The transitional periods have been extended. For sections 500.04(b) (Chief Information Security Officer reports to the Covered Entity's board), 500.05 (penetration testing and vulnerability assessments), 500.09 (risk assessments), 500.12 (multi-factor authentication), and 500.14(a)(2) (cybersecurity awareness training), Covered Entities have a one-year transitional period. For sections 500.06 (audit trail), 500.08 (application security), 500.13 (data retention limits), 500.14 (a)(1) (user monitoring) and 500.15 (encryption), Covered Entities will have an eighteen-month transitional period. Finally, for section 500.11 (Third Party Service Provider oversight), Covered Entities will have a two-year transitional period.

The Revised Proposed Rule will be subject to another 30-day comment period, which commenced on December 28, 2016.

Notwithstanding the revisions, the Revised Proposed Rule is still fundamentally different from the federal regulatory approach. For many financial institutions, compliance with the Revised Proposed Rule will require significant effort and expense.

We will continue to monitor the DFS rulemaking process. If you have questions about the Revised Rule or other cybersecurity issues, visit our Privacy, Cyber Risk & Data Security practice for more information, or contact a BuckleySandler attorney with whom you have worked in the past.