CLIFFORD
CHANCE

Client briefing March 2017

NY DFS Cybersecurity Rules Take Effect

On March 1, 2017, the new requirements on Cybersecurity from the New York Department of Financial Services ("**DFS**") take effect (the "**Cybersecurity Rules**"). The Cybersecurity Rules are an unprecedented action by a state government agency and contain strict requirements for DFS-licensed entities ("**Covered Entities**") to establish enhanced cybersecurity programs, adopt written cybersecurity policies and procedures, and report cyber-events to DFS.

In contrast to the Federal banking agencies' advanced notice of proposed rulemaking on enhanced cyber security standards (briefing available here), the Cybersecurity Rules focus on creating a comprehensive cybersecurity program with strict reporting requirements. The two regulatory approaches remain widely different.

As discussed in our client alerter regarding DFS's original proposed rule, the proposed rule indicated DFS' aggressive approach to cyber security regulation. Although the form and scheme of the original proposal is largely intact in the Cybersecurity Rules, there are a number of key differences, including:

- Clarification on the Cybersecurity Program and Policy requirements (integrating the Risk Assessment in Covered Entities' approaches);
- New timelines and timing requirements;
- Loosening and clarification of various other requirements; and
- Exemptions for certain Covered Entities.

Key Requirements under the Cybersecurity Rules

Cybersecurity Program and Policies

The Cybersecurity Rule requires Covered Entities to adopt a Cybersecurity program and policies or procedures, which are based on the Covered Entities risk assessment. The risk assessment must be carried out in accordance with written policies and procedures, which must include (i) criteria for evaluation and categorization of threats, (ii) criteria for assessment of confidentiality, integrity security and availability of the Covered Entity's Information Systems and Nonpublic Information, and (iii) requirements describing risk mitigation or acceptance.

Based on the risk assessment, the Cybersecurity Rules require each Covered Entity to establish a cybersecurity program designed to ensure the confidentiality, integrity, and availability of the Covered Entity's information systems. The program must be designed to identify cyber risks, implement policies and procedures, detect and respond to cybersecurity events, recover from cybersecurity events and restore normal operations, and comply with all regulatory reporting obligations, among other requirements.

The policies and procedures must also be based on the risk assessment and may address (to the extent relevant), several enumerated areas including information security, access controls, network security, and customer data privacy. The

cybersecurity policy must be approved by the Covered Entity's board of directors or equivalent governing body, or by a Senior Officer of the Covered Entity.

Chief Information Security Officer and Cybersecurity Personnel

Each Covered Entity must designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("**CISO**"). The CISO is responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. The CISO would have to also develop a written report assessing the Covered Entity's cybersecurity program and identifying any cybersecurity risks, to be presented at least annually to the Covered Entity's board of directors and/or Senior Officer.

Penetration Testing and Vulnerability Assessments

Under the Cybersecurity Rules, the cybersecurity program for each Covered Entity must provide for monitoring and testing developed as a result of the Covered Entity's risk assessment.

Audit Trail

Based on its risk assessment, Covered Entities must maintain systems that (i) are designed to reconstruct material financial transactions, and (ii) include audit trails designed to detect and respond to a Cybersecurity Event that have a reasonable likelihood of materially harming any material part of the normal operation of the Covered Entity. Covered Entities must maintain audit records for at least five years.

Cybersecurity Training

All personnel within each Covered Entity would be required to attend regular cybersecurity awareness training sessions. The training sessions must be updated to reflect risks identified by the Covered Entity in its annual risk assessment.

Multi-Factor Authentication

Any individual accessing the Covered Entity's internal systems from an external network of non-public information must pass a "Multi-Factor Authentication" system, unless the CISO has approved the use of at least equivalent access controls. A Multi-Factor Authentication system requires that access to sensitive systems and information is granted through verification of at least two of the following three factors: Knowledge factors (e.g. password); Possession factors (e.g. token or text message on a mobile phone); or Inherence factors (e.g. fingerprint or other biometric characteristic).

Third Party Service Provider Security Policy

The Cybersecurity Rules require Covered Entities to implement written policies and procedures designed to ensure security of information systems and nonpublic information that are accessible to, or held by, Third Party Service Providers. The policies and procedures should be based on the Covered Entity's risk assessment and may include the identification and risk assessment of third parties with access to the Covered Entity's information systems or non-public information, minimum cybersecurity practices required to be met by such third parties, and due diligence and annual assessment practices used to evaluate the third parties' cybersecurity practices.

Reporting Requirements

If a Covered Entity identifies any cybersecurity events presenting material risk of imminent harm relating to its cybersecurity program, the Covered Entity must notify the DFS Superintendent of Financial Services within 72 hours and include such items in its annual report. Such cybersecurity events include that (i) impacting the Covered Entities of which notice is required to be

provided to any government body, self-regulatory agency or any other supervisory body, or (ii) have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

Certification Requirement

Finally, and most importantly, each Covered Entity would have to submit to the Superintendent an annual Certification by February 15 of each year, certifying that the Covered Entity is in compliance with the requirements set forth in the Cybersecurity Regulations. Each Covered Entity also would have to maintain for at least five years all records, schedules, and data supporting the Certification (including documentation of the identification and remedial efforts regarding any cybersecurity events), to be made available for DFS examination upon request. To the extent a Covered Entity identifies areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and remedial efforts underway.

Timelines

The timeline for transition under the Cybersecurity Regulation is as follows:

- **180 Days (August 28, 2017):**
  - Covered Entities must be in compliance, with the below exceptions.
- **11.5 Months (February 15, 2018)**:
  - Covered Entities begin annual submission of Certificate of Compliance to the DFS superintendent.
- **12 Months (March 1, 2018):**
  - CISO reports (500.04(b));
  - Penetration testing and vulnerability assessments (500.05);
  - Risk Assessments (500.09);
  - Multi-factor authentication (500.12); and
  - Cybersecurity awareness training (500.14(a)(2)).
- **18 Months (September 1, 2018):**
  - Audit trail (500.06);
  - Application security (500.08);
  - Data retention limits (500.13);
  - User monitoring (500.14(a)(1)); and
  - Encryption (500.15).
- **24 Months (March 1, 2019):**
  - Third Party Service Provider oversight (500.11).

Conclusion

The Cybersecurity Rules establish strict minimum standards that each Covered Entity must meet to address cybersecurity risks. The conformance period is fairly short, and DFS regulated institutions should promptly take steps to ensure that they are able to meet the requirements by reviewing their existing cybersecurity policies and procedures. This is particularly important in light of the certification requirement embedded in the Rules and DFS's generally aggressive enforcement stance.

Authors

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon
@cliffordchance.com

Daniel Silver
Partner
T: +1 212 878 4919
E: daniel.silver
@cliffordchance.com

Philip Angeloff
Counsel
T: +1 202 912 5111
E: philip.angeloff
@cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

www.cliffordchance.com