New York Department of Financial Services Proposes Cybersecurity Regulations

On September 13, 2016, the New York Department of Financial Services ("**DFS**") proposed new and unprecedented regulations establishing minimum cybersecurity regulatory requirements (the "**Proposed Regulations**"). The Proposed Regulations demonstrate that cybersecurity continues to be a top priority for the DFS and signal that the DFS intends to vigorously enforce compliance with minimum cybersecurity standards. The Proposed Regulations would require each entity licensed by the DFS ("**Covered Entity**") to establish an enhanced cybersecurity program, adopt written cybersecurity policies, and file an annual certification of compliance ("**Certification**") to be provided by the board of directors or Senior Officers of each Covered Entity. The required Certification leaves little doubt that the new regulations will soon be an examination and enforcement priority for the DFS.

The Proposed Regulations are subject to a 45-day notice and public comment period before final issuance. If adopted, the Proposed Regulations would be effective on January 1, 2017, with a 180-day transitional period during which Covered Entities would be required to conform to the new regulatory requirements. The first Certification would be due in January 2018.

The DFS's cybersecurity focus is not new. In a letter issued in December 2014 to all DFS-licensed banking institutions the DFS announced that it would conduct targeted cybersecurity examinations and outlined a new cybersecurity examination process. Also, the Proposed Regulations were previewed in a letter sent in November 2015 by the DFS to a number of federal financial services regulatory agencies. In that letter the DFS stated that the DFS considers cyber security to be among the most critical issues facing the financial world today, and that there is a demonstrated need for robust regulatory action in the cyber security space. The DFS letter also stated that the DFS believes that it would be beneficial to coordinate its efforts with relevant state and federal agencies to develop

a comprehensive cyber security framework that addresses the most critical issues, but apparently has determined that it should take unilateral regulatory action.

The federal banking regulators have issued general guidance and basic requirements regarding information technology examination procedures and risk assessments. Among other initiatives, the Federal Financial Institutions Examination Council (FFIEC) has developed a "Cybersecurity Assessment Tool," the output of which can assist a financial institution's senior management and board of directors in assessing the institution's cybersecurity risk and preparedness. The FFIEC also maintains a webpage dedicated to Cybersecurity Awareness that contains a compilation of cybersecurity guidance provided by the federal banking regulators. No regulations have yet been issued by the federal financial services regulatory agencies, however, incorporating minimum cybersecurity requirements.

The Proposed Regulations apply broadly to any entity operating under, or required to operate under, a DFS license, charter, or similar authorization. Importantly, under the Proposed Regulations, a foreign bank licensed by the DFS to operate a banking office in New York would itself be a Covered Entity (i.e., the Proposed Regulations appear to apply not just to the New York offices of DFS-licensed foreign banks but to the foreign banks themselves). Additionally, law firms and other third-party service providers working with any Covered Entity would also be subject to certain authentication and audit requirements.

Key Requirements Under the Proposed Regulations:

Cybersecurity Program

The Proposed Regulations 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.

Cybersecurity Policies and Procedures

As part of its cybersecurity program, each Covered Entity would be required to adopt written cybersecurity policies and procedures. The policies must address, "at a minimum," several enumerated areas including information security, access controls, network security, and customer data privacy. The cybersecurity policy must be reviewed by the Covered Entity's board of directors or equivalent governing body, and approved by a Senior Officer of the Covered Entity. Such review and approval must occur at least once a year, or more frequently to address any applicable cybersecurity risks.

Chief Information Security Officer and Cybersecurity Personnel

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

directors and/or Senior Officer. The CISO must be supported by sufficient cybersecurity personnel, who will manage cybersecurity risks and perform any core cybersecurity functions identified in the Covered Entity's cybersecurity program.

Penetration Testing and Vulnerability Assessments

Under the Proposed Regulations, the cybersecurity program for each Covered Entity must provide for annual penetration testing of its information systems, i.e., a simulated cyber attack that aims to breach the Covered Entity's information security, exploit critical systems, and gain access to sensitive data. The program must also provide for quarterly vulnerability assessments, by which the Covered Entity performs an in-depth evaluation of its information security posture to identify and quantify security vulnerabilities.

Audit Trail

Any activity related to the Covered Entity's information security systems would have to be traced and documented through an audit trail system. The audit trail system must, at a minimum, ensure that the Covered Entity is able to log access and alterations made to any critical systems or the audit trail, protect the integrity of hardware or any data collected as part of the audit trail, and maintain audit records for at least six years.

Monitoring and Risk Assessment

Non-public information must be protected from unauthorized access, use, or tampering through regular monitoring. Additionally, an annual risk assessment must be carried out in accordance with written policies and procedures and documented in writing. The relevant policies and procedures must include, at a minimum, criteria for the evaluation and categorization of risks, criteria for the assessment of the Covered Entity's information systems, and requirements for documentation on how identified risks will be mitigated based on the risk assessment.

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 of non-public information must pass a "Multi-Factor Authentication" system. 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 Information Security Policy

Cybersecurity policies and procedures must include provisions designed to ensure the security of information systems that accessible to, or held by, third parties or vendors doing business with the Covered Entity. Such third parties and vendors include law firms and other service providers, who often have access to a financial institution's information technology systems. The relevant policies and procedures must address, at a minimum, 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. The policies and procedures must also provide for establishing preferred provisions to be included in contracts with third party service providers, including the use of Multi-Factor Authentication to limit access, the use of encryption to protect non-public information, notice requirements for any cybersecurity events, representations and warranties from the third party providing that its services or products is free from cybersecurity risks, and the right of the Covered Entity to perform cybersecurity audits as it deems necessary.

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, but are not limited to, any event involving the actual or potential unauthorized tampering with, access to, or use of the Covered Entity's information system or non-public information.

Certification Requirement

Finally, and most importantly, each Covered Entity would have to submit to the Superintendent an annual Certification by January 15 of each year, certifying that the Covered Entity is in compliance with the requirements set forth in the Proposed 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.

Conclusion

The Proposed Regulations establish strict minimum standards that each Covered Entity must meet to address cybersecurity risks. Even though the Proposed Regulations have yet to be finalized, the proposed 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 Proposed Regulations and DFS's generally aggressive enforcement stance. Further, vendors and third-party service providers should also be prepared to comply with third party information security policies that the Covered Entities would be obligated to adopt under the Proposed Regulations.

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