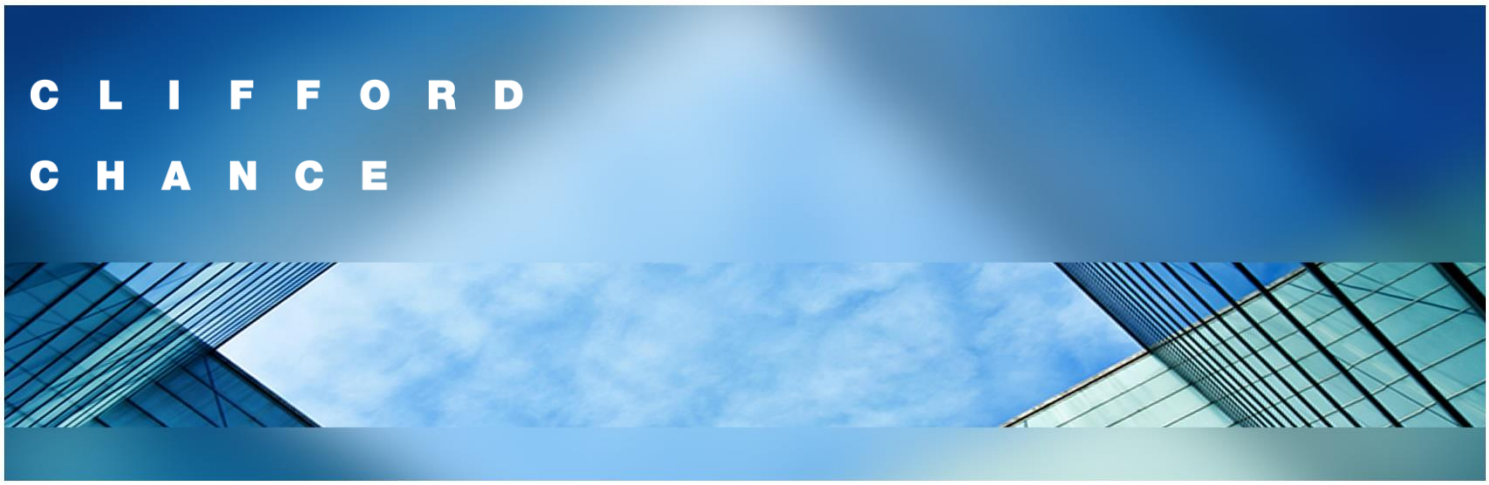

FIRST CERTIFICATIONS UNDER NY DFS CYBERSECURITY RULES DUE FEBRUARY 15, 2018

On February 15, 2018, banks, insurance companies, and other financial services providers covered by the new Cybersecurity Rules issued last year by the New York Department of Financial Services ("DFS") will be required to submit to DFS a certification that they are in compliance with the regulation – or at least with those parts of the regulation that are in effect. The Certification of Compliance, in the format laid out in Appendix A to the Cybersecurity Rules, 23 NYCRR Part 500, requires either the Board of Directors or a Senior Officer of a covered entity, as defined in the Rules, to certify that they have "reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary," and that "[t]o the best of [their] knowledge," the covered entity's Cybersecurity Program complies with the Cybersecurity Rules.

Notably, while covered entities must have a Cybersecurity Program and Policy in place, must have hired a Chief Information Security Officer (or "CISO"), must have an incident response plan, and must provide notices of "Cybersecurity Events" to the Superintendent, other requirements of the Cybersecurity Rules – such as the penetration testing or continuous monitoring requirement, the risk assessment requirement, and the multi-factor authentication requirement – are not in effect until March 1, 2018, and are therefore technically not included in the certification requirement. Nevertheless, covered entities would be well advised to comply with these requirements, as the effective date is right around the corner and DFS has also announced that it will be incorporating cybersecurity in all of its examinations of financial services companies.

KEY REQUIREMENTS UNDER THE CYBERSECURITY RULES THAT ARE NOW IN EFFECT

As we have previously summarized, 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.

Key requirements under the Rules that are now in effect, and that must be considered in the Certification of Compliance filed on February 15, include:

Cybersecurity Program and Policies

The Cybersecurity Rule requires Covered Entities to adopt a Cybersecurity Program and policies or procedures. The Cybersecurity Program must be designed to ensure the confidentiality, integrity, and availability of the Covered Entity's information systems, and must also 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 Cybersecurity Policy should address (to the extent relevant), several enumerated areas including information security, access controls, network security, and customer data privacy. The 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.

Both the Cybersecurity Program and the Cybersecurity Policy are to be based on a Risk Assessment, but the Risk Assessment requirement of the Cybersecurity Rules – described further below – is not actually in effect until March 1, 2018. Accordingly, DFS anticipates that an entity's cybersecurity program and policy will likely need to be updated once the Risk Assessment is completed. (See FAQ #19)

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 will also have to 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, but this requirement is not in effect until March 1, 2018.)

Access Privileges

Each Covered Entity must limit user access privileges to its Information Systems that provide access to Nonpublic Information.

Incident Response Plan

Each Covered Entity must establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event, including the internal process for responding to such an incident, the goals of the response

plan, definition of roles and responsibilities of those who carry out the plan, external and internal communications and information sharing, identification of remediation efforts, and documentation and reporting regarding any Cybersecurity Event.

Reporting Requirements

If a Covered Entity identifies any Cybersecurity Event 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 those (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) having a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

OTHER SIGNIFICANT REQUIREMENTS THAT GO INTO EFFECT IN THE NEXT SIX MONTHS

Under the timeline established under the Cybersecurity Rules, which provide for certain transitional periods, other provisions are scheduled to go into effect March 1, 2018, and still others on September 1, 2018, and will therefore be covered by the compliance certifications to be filed next year and by any examinations conducted by DFS after the relevant effective date. These requirements include:

Penetration Testing and Vulnerability Assessments (effective March 1, 2018)

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.

Risk Assessment (effective March 1, 2018)

Each Covered Entity is required to conduct a periodic Risk Assessment of its Information Systems, sufficient to inform the design of the Entity's cybersecurity program. 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. The Risk Assessment must be updated as necessary to address changes in the Information Systems, and must be carried out in accordance with written policies and procedures and be documented. The Risk Assessment in turn informs the design of the entity's cybersecurity program and the provisions of the entity's cybersecurity policy. DFS accordingly anticipates, as noted above, that an entity's cybersecurity program and policy may need to be updated once a Risk Assessment is completed. (See FAQ #19)

Multi-Factor Authentication (effective March 1, 2018)

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).

Audit Trail (effective September 1, 2018)

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 (effective September 1, 2018)

All personnel within each Covered Entity will 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.

Encryption of Nonpublic Information (effective September 1, 2018)

By September 1, 2018, Covered Entities are required to encrypt Nonpublic Information, both in transit over external networks and at rest, unless the entity determines that encryption is not feasible and the entity puts compensating controls in place that meet the approval of the entity's CISO.

CONCLUSION

Even though a number of key provisions in the Cybersecurity Rules – including penetration testing and monitoring, risk assessment, multi-factor authentication, audit trails, training and monitoring, and encryption – are not currently in effect and are therefore not covered, as a technical matter, by the first Certification of Compliance due on February 15, 2018, banks, insurers and other covered financial services providers should promptly take steps to ensure that they are able to meet these requirements by reviewing their existing cybersecurity policies and procedures. This is particularly important because DFS has announced that it will be testing compliance with the Cybersecurity Rules as part of its examination process. Indeed, DFS will want to make sure that entities are in compliance with its first-in-the-nation rules.

In addition, each Covered Entity must 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. Finally, while the Rules contemplate that a Covered Entity may identify areas, systems or processes that require material improvement, updating or redesign, in which case the Covered Entity must document the identification and remedial efforts underway and make such documentation available for inspection by the Superintendent, DFS has made clear that it expects full compliance with its Cybersecurity Rules. (FAQ #21)

CLIFFORD
CHANCE

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

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

Alice Kane
Counsel

T +1 212 878 8110
E alice.kane
@cliffordchance.com