REPRINT

CD corporate disputes

NEW CYBER SECURITY REGULATIONS PROMULGATED BY NEW YORK'S DEPARTMENT OF FINANCIAL SERVICES

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JAN-MAR 2017 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

PERSPECTIVES

NEW CYBER SECURITY REGULATIONS PROMULGATED BY NEW YORK'S DEPARTMENT OF FINANCIAL SERVICES

BY **BARRY R TEMKIN / ROBERT USINGER**
> MOUND COTTON WOLLAN & GREENGRASS LLP / ONEBEACON INSURANCE GROUP

Effective 1 January 2017, the New York State Department of Financial Services (DFS) is expected to implement new cyber security requirements which require regulated financial companies doing business in New York to adopt comprehensive written programmes and procedures to prevent data breaches and other cyber security events. The new cyber security regulations affect any licensed entity doing business under the New York Banking Law, Insurance Law, or Financial Service Law, including insurance carriers, banks, insurance agents, consumer lenders, mortgage brokers and other entities under DFS jurisdiction. This regulation may signal a potential wave of cyber security requirements imposed by financial industry regulators. Since most financial firms do business in New York, the implications of the DFS cyber security regulations can be expected to be broad-reaching.

And while Massachusetts has recently enacted a law requiring all businesses to encrypt confidential personal information stored on portable devices or transmitted electronically where technically feasible, New York's regulations are directed specifically toward the financial services industry.

Under the new cyber security regulations, each financial services company operating in New York "shall establish and maintain a cybersecurity program to ensure the confidentiality, integrity and availability of the covered entity's information systems". The DFS regulations further require each cyber security programme to identify internal and external cyber risks, develop and implement defensive infrastructure to protect the company's information system, detect cyber security events and fulfil regulatory reporting obligations.

The DFS issued the proposed rules on 28 September 2016 for a 45-day public comment period, which ended on 14 November 2016. The final rules are expected to be issued before the end of 2016 with an effective date of 1 January 2017. The proposed effective date of 1 January 2017 is subject to a 180 day grace period. Covered entities are required to prepare and submit a certificate of compliance to the DFS, starting 15 January 2018.

The new rules apply to "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law." A

limited exception to the regulations is carved out for otherwise covered entities with fewer than 1000 customers, fewer than $5m in gross annual revenue and less than $10m in year-end total assets.

The proposed regulations require each covered company to establish a comprehensive written cyber security policy addressing 14 specific areas, including information security, data governance and classification, a business continuity and disaster recovery plan, systems operations and availability concerns, network security, customer data privacy, risk assessment and related topics. The written cyber security policy should also contain a proposed plan of response to a potential data breach or other cyber event, which must be reviewed and approved by the board of directors and chief executive on an annual basis.

Each covered entity is required to designate a chief information security officer (CISO) to implement the firm's cyber security programme and to report, on a biannual basis, to the board of directors or CEO regarding major issues affecting the company's cyber security programme. The CISO's biannual report should identify cyber risks, evaluate the effectiveness of the company's cyber security programme and propose to remediate any inadequacies. In addition, the regulations require penetration testing on an annual basis and the maintenance of an audit trail sufficient to identify persons who accessed the entity's information systems. The audit trail records must be maintained for at least six years.

The regulations require the covered entity certify its compliance in an annual report, certified by the chair of its board or a comparable senior manager. In addition, a covered entity must promptly notify DFS of a cyber event "that has a reasonable likelihood of materially affecting the normal operation of the covered entity or that affects non-public information".

"Financial services companies doing business with vendors such as law firms will be required to affirm that these vendors maintain minimum cyber security practices, including encryption of electronic data."

Of particular note for law firms representing financial service companies, Section 500.11 of the DFS regulations requires each covered entity to implement written policies and procedures designed to ensure the security of information systems and non-public information "that are accessible to or held by third parties doing business with the covered entities". These policies must identify

third parties with access to sensitive data, and require minimum cyber security practices to be maintained by them. According to Section 500.11, each covered entity shall implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by, third parties doing business with the covered entity. Such policies and procedures shall address, at a minimum, the following areas: (i) the identification and risk assessment of third parties with access to such information systems or such non-public information; (ii) minimum cyber security practices required to be met by such third parties in order for them to do business with the covered entity; (iii) due diligence processes used to evaluate the adequacy of cyber security practices of such third parties; and (iv) periodic assessment, at least annually, of such third parties and the continued adequacy of their cyber security practices.

Financial services companies doing business with vendors such as law firms will be required to affirm that these vendors maintain minimum cyber security practices, including encryption of electronic data.

Encryption is a key part of the new regulations, which require each covered entity to "encrypt all non-public information held or transmitted by the covered entity both in transit and at rest". Non-public information which cannot be feasibly encrypted must be secured with alternative controls. The DFS regulations require encryption of non-public information, which includes personal identifying information (PII), competitively sensitive information and any information that would be considered non-public under the Gramm-Leach Bliley Act of 1999. In addition, the regulated entity must prepare a written incident response plan designed to respond, to and recover from, a potential data breach. The encryption requirement is delayed until "one year from the effective date of the regulation."

The new regulations will also require multi-factor authentication for privileged access to database servers of covered entities or for individuals accessing systems from an external network. Such authentication would entail the use of two of the three following sensors: (i) knowledge factor, such as a password; (ii) possession factor, such as a token or text message on a mobile phone; or (iii) inherent factor, such as a biometric characteristic like a fingerprint. Thus, regulated financial entities now need more than just a password to access sensitive computer data.

The new regulations also propose "limitations on data retention", mandating the destruction of non-public information that is no longer necessary. This requirement could place these regulations, and the covered entities that follow them, in potential conflict with a body of case law about electronically-stored information, spoliation and maintenance of electronically stored data, as required by financial industry regulations and court rules. The regulations

also provide a carve-out for information required to be maintained by law or regulation.

Conclusion

Lawyers who represent covered entities regulated by DFS should advise their clients regarding compliance with the new DFS cyber security regulations. In addition, law firms transmitting data to and from financial service companies in New York would be well-advised to ensure that their own information systems are adequately encrypted in order to facilitate their clients' compliance with the new regulations.

Financial industry regulators, such as the US Securities and Exchange Commission and Financial Industry Regulatory Authority, have reported investigations and audits of firms for cyber security deficiencies. Given New York's prominence as an international financial centre, it is likely that the new DFS regulations will accelerate the trend toward further regulation of cyber security by government agencies and self-regulatory organisations. CD

Barry R. Temkin
Partner
Mound Cotton Wollan & Greengrass LLP
T: +1 (212) 804 4221
E: btemkin@moundcotton.com

Robert J. Usinger
Assistant Vice President of Financial Institutions Claims
OneBeacon Insurance Group
T: +1 (212) 440 6580
E: rusinger@onebeacon.com