**Edward J. McAndrew** Partner
mcandrewe@ballardspahr.com

**Marjorie J. Peerce** Partner
peercem@ballardspahr.com

**Kevin D. Leitão** Of Counsel
leitaok@ballardspahr.com

**Kim Phan** Of Counsel
phank@ballardspahr.com

Ballard Spahr LLP, Philadelphia and Washington DC

# New York regulators drive cyber security accountability for the financial sector

Edward J. McAndrew, Marjorie J. Peerce, Kevin D. Leitão and Kim Phan of Ballard Spahr LLP, discuss the proposed cyber security regulations issued by the New York State Department of Financial Services ('DFS'), the background to the proposed regulations and the obligations that would be imposed on financial institutions relating to the establishment and maintenance of cyber security programmes.

The DFS issued proposed regulations in September 2016 that would require many covered financial institutions to establish and maintain cyber security programmes that meet specific minimum standards[1]. These proposed regulations would apply to all financial institutions supervised by the DFS ('Covered FIs') and would be applied by Covered FIs contractually to their third party service providers and business partners. Given the range of affected companies, there is a realistic possibility that any final regulations promulgated by the DFS could become the *de facto* standard for cyber security programmes and their governance when engaging in financial activities in the US. Other individual states may also choose to adopt similar regulations.

These proposed regulations are generally consistent with current regulatory guidance and best practices but may be a game-changer in cyber security regulation because they set forth prescriptive requirements. Current data security regimes in the US, examination guidance, and regulatory expectations are generally principle-based, rather than prescriptive. Many financial institutions rely on the Federal Financial Institutions Examination Council ('FFIEC') principle-based guidance from their information security booklets[2]. In a similar vein, Federal Trade Commission ('FTC') enforcement actions have focused on 'reasonableness,' while articulating a series of principles and related standards[3].

Perhaps the most important, and somewhat daunting, provision is the requirement that each Covered FI's board of directors or a senior officer annually prepare and submit to the DFS a 'Certification of Compliance.' To understand the context and substance of the proposed regulations and the certification requirement, it is helpful to summarise the DFS's analysis and outreach in the three years leading up to publication of the proposed regulations.

In May 2014, the DFS issued a 'Report on Cyber Security in the Banking Sector,' using the underlying data as part of an expansion and revision of its IT examination procedures[4]. The DFS issued a similar report in February 2015 on insurance companies that included health, property and casualty, and life insurers[5]. In April 2015, the DFS released an update to its 2014 report, focusing on a survey of 40 banks on their management of third party vendors. This report concluded that 'banking organizations appear to be working to address the cyber security risks posed by third-party service providers, although progress varies depending on the size and type of institution[6].' While this research was underway, DFS Superintendent Benjamin Lawsky articulated the agency's goals in a 25 February 2015 speech. He outlined the need for state financial services regulators to be more proactive and lamented the limitations of using enforcement actions to promote sound risk management. The Superintendent went on to announce that the DFS intended to play a catalytic role as to: Wall Street accountability; preventing money laundering; and strengthening cyber security in the financial sector.

## Proposed cyber security regulations

Some of the major requirements of the proposed regulations include:

- Establishing a cyber security programme designed to ensure the confidentiality, integrity, and availability of information systems;
- Adopting a written cyber security policy, reviewed by the organisation's board of directors and approved by a senior management officer;
- Designating a qualified individual to serve as the company's Chief Information Security Officer ('CISO'), who will be responsible for overseeing and implementing the company's cyber security programme and enforcing its cyber security policy;
- Maintaining policies and procedures related to managing third party

continued

relationships, including conducting appropriate due diligence prior to entering into any such relationship and appropriately monitoring for and assessing the adequacy of cyber security measures by those third parties;
- Creating a written incident response plan designed to promptly respond to and recover from any broadly defined 'Cybersecurity Event[7];' and
- Notifying the DFS Superintendent within 72 hours of any 'Cybersecurity Event that has a reasonable likelihood of affecting the normal operation' of the company, that affects non-public information, or involves the 'actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.'

The proposed regulations also set forth more granular security measures as 'minimum standards,' such as: annual penetration testing and risk assessments; logging and audit trail systems capable of 'complete and accurate reconstruction' of transactions and accounting relating to cyber security events; multifactor authentication for remote or privileged access to internal systems or database servers; data destruction standards; and encryption of all non-public information at rest and in transit.

Cyber security programme governance requirements include at least biannual reports by the CISO to the Covered FI's board of directors about the cyber security programme.

*Scope - Extended to third parties*
All financial institutions supervised by the DFS are subject to these requirements, including banks, state-licensed lenders, mortgage industry companies, insurance companies, and money services businesses[8].

The impact will be even greater because Section 500.11 of the proposed regulation requires Covered FIs to implement programmes 'designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by' third parties. The requirements include identification and risk assessment of third parties; minimum cyber security practices; due diligence processes used to evaluate the adequacy of their cyber security practices; and periodic assessment of third parties and the continued adequacy of their cyber security practices. Covered FIs also must develop 'preferred provisions' to be included in contracts with third parties, where applicable. These provisions should address multifactor authentication; encryption to protect data in transit and at rest; prompt notification of a cyber security event; certain representations and warranties; and the right to conduct audits.

*Notification - Expedited disclosure of 'cyber security events'*
Covered FIs will be required to notify the Superintendent of a broad range of actual or attempted cyber security incidents within 72 hours of initial discovery - including any event that involves 'Nonpublic Information.' Third parties must 'promptly' notify Covered FIs of such incidents. This leaves little time for companies to investigate and contain an incident before initial disclosure to the Superintendent. The proposal highlights the critical need for advance incident response planning, while portending that the DFS will likely become actively engaged in the investigation of significant cyber incidents as soon as it becomes aware of them.

*Certification - A brave new world*
The proposed regulations also include a dramatic innovation - a requirement that each Covered FI submit annually to the DFS Superintendent a 'certification of compliance' with the regulations. The potential impact of this certification on the individuals who provide it should not be underestimated. In the Superintendent's February 2015 speech, the discussion on 'Wall Street accountability' focused on the need to hold individuals at companies responsible for corporate wrongdoing, "even if there are certain circumstances where the misconduct does not rise to the level of criminal fraud [...]." While that discussion was focused on wrongdoing in the recent financial crisis, it is clear that the DFS is looking to hold individuals at companies accountable for key compliance requirements.

**Final thoughts**
**The proposed regulations are tentatively scheduled to go into effect on 1 January 2017, with a transition period of 180 days for Covered FIs to achieve compliance with any new requirements.**

**The proposed regulations will impose significant new and ongoing obligations on a wide range of organisations beyond those directly regulated by the DFS. Preparation and continual cyber security diligence will be the keys to maintaining compliance and best positioning an organisation to respond to inevitable cyber security incidents.**