

THE REVIEW OF  
**SECURITIES & COMMODITIES  
REGULATION**

AN ANALYSIS OF CURRENT LAWS AND REGULATIONS  
AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 50 No. 13 July 19, 2017

## THE NEW YORK STATE DFS CYBERSECURITY REGULATION: PREPARING FOR COMPLIANCE

*Compliance with a significant portion of the New York State DFS cybersecurity regulation is required by August 28 of this year. The authors discuss the background and coverage of the regulation. They then address key provisions of the six basic functions and 14 topics of the required cybersecurity program. They note that the chairperson of the board of directors (or a senior officer) must certify annually to DFS that the program complies with the DFS rule.*

Jeffrey P. Taft, Lawrence R. Hamilton, Stephen Lilley, and Matthew Bisanz \*

Financial services companies, like businesses across the U.S. economy, have invested heavily in the development and implementation of risk-based cybersecurity practices. In doing so, financial services companies have assessed and responded to the specific threats facing their enterprises, and the particular systems they operate and data they hold. Substantial collaboration between the public and private sectors has supported this risk-based approach. In particular, the NIST Cybersecurity Framework reflects the joint efforts of

public and private stakeholders to develop and implement risk-based security practices.<sup>1</sup>

One basic assumption behind this approach has been that there is no one-size-fits-all cybersecurity standard for American businesses. In a similar vein, key stakeholders in the private and public sectors have warned against the issuance of static, prescriptive regulations, which would mistakenly turn cybersecurity into a compliance exercise driven by static checklists

---

<sup>1</sup> NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (Feb. 12, 2014).

---

\* JEFFREY P. TAFT is a partner in the Financial Services Regulatory & Enforcement practice in Mayer Brown LLP's Washington D.C. office. LAWRENCE R. HAMILTON is a partner in the firm's insurance practice at its Chicago office. STEPHEN LILLEY is a litigation partner in the firm's Washington D.C. office. MATTHEW BISANZ is an associate in the Financial Services Regulatory & Enforcement practice in Mayer Brown LLP's Washington D.C. office. Each is a member of the firm's Cybersecurity and Data Privacy practice. Their e-mail addresses are [jtaft@mayerbrown.com](mailto:jtaft@mayerbrown.com), [lhilton@mayerbrown.com](mailto:lhilton@mayerbrown.com), [slilley@mayerbrown.com](mailto:slilley@mayerbrown.com), and [mbisanz@mayerbrown.com](mailto:mbisanz@mayerbrown.com).