New York's DFS Narrows Proposed Cybersecurity Regulations

Jan 20, 2017

Categories:

Blockchain and Digital Assets
Blogs
Publications

Authors:

Courtney Rogers Perrin

On September 13, 2016, the New York State Department of Financial Services ("NYDFS") issued proposed cybersecurity regulations ("Original Proposed Regulations") that would impose new, stringent cybersecurity requirements on banks, money transmitters, insurance companies, and other financial service providers regulated by the NYDFS (collectively, "Regulated Institutions").

During the 45-day notice and public comment period, NYDFS received over 150 comments from Regulated Institutions, trade associations, individuals and third party service providers, including cybersecurity service providers. On December 28, 2016, the NYDFS published revised proposed regulations ("Revised Proposed Regulations") to address the comments received. Below is a table summarizing the most salient changes to the Original Proposed Regulations. Please note that the information in the table is not a comprehensive summary of the proposed regulations.

Requirement	Original Proposed Regulation	Revised Proposed Regulation
Chief Information Security Officer ("CISO")	Appointment of an exclusive CISO with only information security duties; bi-annual written reports to the Regulated Institution's governing body	Appointment of a non-exclusive CISO who may perform other functions; annual written reports to the Regulated Institution's governing body
Risk Assessments	Annual	Periodic

Data Retention and Destruction	Destroy nonpublic information no longer necessary to provide products and services	May maintain nonpublic information if necessary for business operations or other legitimate purposes
Penetration Testing and Vulnerability Assessments	Annual penetration testing and quarterly vulnerability assessments	Continuous monitoring or periodic penetration testing and vulnerability assessments; absent effective continuous monitoring, the Regulated Institution must conduct annual penetration and bi-annual vulnerability assessments
Access Privileges	Limited to individuals who require access to perform their responsibilities	Limited to individuals based on the Regulated Institution's risk assessment
Multifactor Authentication	Multifactor authentication and risk-based authentication for specified circumstances	Regulated Institutions select appropriate controls, which may include multifactor or risk-based authentication, based on its risk assessment

Encryption	Compensating controls for a limited transition period: one year for encryption of data in transit and five years for encryption of data at rest	Compensating controls may be used indefinitely for nonpublic information in transit and at rest, as approved by the CISO who annually reviews feasibility and effectiveness
Audit Trail	Maintenance of audit trail systems based on prescriptive requirements; maintain records for six years	Maintenance of audit trail systems based on the Regulated Institution's risk assessment; maintain records for five years
Third-Party Service Providers	Required to include security language in contracts	Security guidelines to be provided to third-party service providers
Nonpublic Information	Broad definition	More limited definition
Notice to NYDFS of Cybersecurity Events	If risk of materially affecting the Regulated Institution's operations or nonpublic information	If risk of material harm to the Regulated Institution's normal operations
Use of Affiliates to Help Comply with Requirements	Not permitted; only third party service providers permitted	Permitted

Confidentiality Regarding Exemptions from Disclosure	None	Information provided by a Regulated Institution is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law, or any other applicable state or federal law

	Transitional Period	180 days from the effective date to comply with regulations	Adds three exceptions: By March 1, 2018: • CISO reporting • Periodic risk assessments • Annual penetration testing and bi-annual authentication • Regular cybersecurity training By September 1, 2018: • Maintain audit trail systems • Encrypt nonpublic information • Implement written procedures • Secure disposal of nonpublic information • Controls to monitor authorized users By March 1, 2019: • Implement written policies and procedures relating to third party

Effective Date	January 1, 2017	March 1, 2017

New Exemptions

The NYDFS added several new exemptions in the Revised Proposed Regulations. Any Regulated Institution claiming an exemption must file a notice of exemption with the NYDFS. A Regulated Institution may be excluded from certain provisions, including appointing a CISO, penetration testing, application development, multifactor authentication, encryption and incident response plan obligations if it has (a) fewer than 10 employees or independent contractors; (b) less than $5 million in gross annual revenue in each of the past three fiscal years; or (c) less than $10 million in its and its affiliates' GAAP year-end total assets. Additionally, if a Regulated Institution is an employee, agent, representative, or designee of another Regulated Institution, no program is required. Finally, a Regulated Institution that does not directly or indirectly maintain information systems or possess nonpublic information is exempt from most requirements of the Revised Proposed Regulations, except for requirements relating to risk assessments, implementation of written third party service provider policies, disposal of nonpublic information and notice to the NYDFS.

The NYDFS will finalize the Revised Proposed Regulations following a second notice and public comment period. Comments on the Revised Proposed Regulations are due January 27, 2017. We encourage Regulated Institutions to check whether their cybersecurity policies, procedures and programs comply with the Revised Proposed Regulations' requirements.

For questions about the regulations or for assistance in ensuring compliance by March 1, 2017, contact Michael Nitardy, or any other member of Frost Brown Todd's Privacy & Data Security Team.

FBT Gibbons