LOEB & LOEB LLP

Privacy

NOVEMBER 2016

Proposed NY Cybersecurity Regulations to Impose Rigorous Requirements on Financial Services Companies

by Ieuan Jolly, Partner

The New York State Department of Financial Services recently announced proposed cybersecurity requirements that would apply to financial services companies, insurance companies and banks. Aimed at protecting customer information and the information technology systems of DFS-regulated entities from cyberattacks, the proposed regulations would require covered financial services companies to assess their specific risk profiles and design cybersecurity programs that address their risks in a "robust fashion." While the DFS claims that its proposed rules are not "overly prescriptive" so that cybersecurity programs can match the relevant risks and keep pace with technological advances, the regulations contain numerous mandatory requirements that will likely increase operational and compliance costs for companies governed by them.

Under the regulations, companies must identify internal and external cyber risks by identifying the nonpublic information they collect and store, the sensitivity of that nonpublic information, and how and by whom the information may be accessed. The regulations broadly define nonpublic information to include any information an individual provides in connection with the seeking or obtaining of any financial product or service – a definition that captures far more data than what New York's existing data protection law defines as "personal information." The definition incorporates the federal Gramm-Leach-Bliley Act definition of customer information, bringing under the regulations information that a consumer provides to a financial institution or insurance company to obtain a product or service, information resulting from the transaction and any information that the company obtains about the consumer in connection with providing the product or service.

Regulated entities must implement and maintain a comprehensive written cybersecurity policy that addresses a number of different areas, including system and information security, customer data privacy, and vendor and third-party service provider management. The policy must be reviewed by the board of directors and approved by a senior officer. Companies must designate a chief information security officer responsible for implementing and overseeing the cybersecurity program (this requirement may be met using a third-party service provider instead of an employee of the company). The CISO must develop and issue a biannual report assessing the effectiveness of the cybersecurity

program for their boards and the DFS. The regulations also require that the boards of these companies perform annual risk assessments.

The cybersecurity program must also include annual penetration testing and quarterly vulnerability assessments; audit trail systems; limitations on access privileges; multifactor authentication and encryption of nonpublic information "at rest," not just while in transit; and timely destruction of information. It must also provide for personnel training and monitoring of authorized users and limited information access. Companies must put in place qualified personnel to manage the cybersecurity risks and core cybersecurity functions, and they must provide regular cybersecurity updates and training sessions. (Companies may also use a third-party service provider to meet these requirements.)

The regulations require that senior managers of regulated entities must also certify annually to the DFS superintendent that the entity is in compliance with the regulations. Companies must maintain for five years the records supporting certification and make them available for examination by the DFS.

Companies must also establish a data breach incidence response plan that addresses responding to and recovering from a cybersecurity breach. In the event of a breach or attempted breach involving nonpublic information, companies must notify the DFS superintendent within 72 hours. The company must also notify the superintendent within 72 hours of any "material risk of imminent harm" a company identifies relating to the cybersecurity program and must include these material risks in its annual certification report.

Given New York's importance in the financial services industry, the effects of the proposed requirements likely will be felt across the country – and other regulators may follow New York's example. The proposed rules are now subject to a 45-day notice and public comment period, which ends on Nov. 12, 2016. The rules are set to take effect on Jan. 1, 2017, and covered companies would have only 180 days to put in place the required programs. In light of this extremely short time frame, financial services companies must be prepared to reassess their cybersecurity risks, policies and procedures; enhance their cybersecurity programs; and document their compliance efforts.

For more information on this development or assistance complying with these regulations, please contact Ieuan Jolly at ijolly@loeb.com or 212.407.4810.

Advanced Media and Technology Practice

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ELIZABETH J. ALLEN	EALLEN@LOEB.COM	312.464.3102
AMIR AZARAN	AAZARAN@LOEB.COM	312.464.3330
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MEG CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
CARNELL L. CHERRY	CCHERRY@LOEB.COM	202.618.5029
ALESON CLARKE	ACLARKE@LOEB.COM	310.282.2240
PAULA K. COLBATH	PCOLBATH@LOEB.COM	212.407.4905
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
TATYANA V. GILLES	TGILLES@LOEB.COM	312.464.3125
MARK GOLDBERG	MGOLDBERG@LOEB.COM	212.407.4925
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
SUSAN E. ISRAEL	SISRAEL@LOEB.COM	212.407.4177
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
BENJAMIN B. KABAK	BKABAK@LOEB.COM	212.407.4174
CAROL M. KAPLAN	CKAPLAN@LOEB.COM	212.407.4142
ALISON M. KELLY	AMKELLY@LOEB.COM	212.407.4194
ELIZABETH H. KIM	EKIM@LOEB.COM	212.407.4928
MICHELLE LA MAR	MLAMAR@LOEB.COM	310.282.2133
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
SCOTT S. LIEBMAN	SLIEBMAN@LOEB.COM	212.407.4838
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ELISABETH O'NEILL	LONEILL@LOEB.COM	312.464.3149
SUE K. PAIK	SPAIK@LOEB.COM	312.464.3119
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
MEREDITH SILLER	MSILLER@LOEB.COM	310.282.2294
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
JOHN T. UM	JUM@LOEB.COM	310.282.2397
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960