The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION MARCH 2018

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 135 **NUMBER 3** **March 2018**

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:
Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call
Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISBN: 978-0-7698-8020-4 (eBook)
ISSN: 0005-5506 (Print)
ISSN: 2381-3512 (Online)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Sheshunoff is a registered trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2018 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt® Publication

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS
James F. Bauerle
Keevican Weiss Bauerle & Hirsch LLC

Barkley Clark
Partner, Stinson Leonard Street LLP

John F. Dolan
Professor of Law, Wayne State Univ. Law School

Satish M. Kini
Partner, Debevoise & Plimpton LLP

Douglas Landy
Partner, Milbank, Tweed, Hadley & McCloy LLP

Paul L. Lee
Of Counsel, Debevoise & Plimpton LLP

Givonna St. Clair Long
Partner, Kelley Drye & Warren LLP

Stephen J. Newman
Partner, Stroock & Stroock & Lavan LLP

David Richardson
Partner, Dorsey & Whitney

Stephen T. Schreiner
Partner, Goodwin Procter LLP

Elizabeth C. Yen
Partner, Hudson Cook, LLP

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2018 Reed Elsevier Properties SA., used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form— by microfilm, xerography, or otherwise— or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer. Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258 (phone). Material for publication is welcomed— articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

Developing Cybersecurity Requirements in Banking (and Other Financial Services)

Theodore P. Augustinos*

This article provides a description of some of the critical provisions of the New York Department of Financial Services' Cybersecurity Requirements for Financial Services Companies and the National Association of Insurance Commissioners' Model law, and the differences and nuances between them.

The financial services industry has been dealing with requirements for cybersecurity since 1999, but 2017 brought new, significant, and proliferating obligations. The bar for the whole industry was clearly raised by the unilateral action of the New York Department of Financial Services ("DFS"), which adopted a new regulation, Cybersecurity Requirements for Financial Services Companies ("DFS Regulation").[1]

The DFS Regulation imposes significant new responsibilities on DFS licensees (which includes banks, insurers and producers, mortgage lenders and brokers, and others) over a transition period ending in 2019.

THE NAIC MODEL

Taking up the mantle, the National Association of Insurance Commissioners ("NAIC"), which had been working on a model information security law for two years, essentially scrapped its prior drafts and, in October 2017, adopted much of the terminology and concepts of the DFS Regulation to promulgate a model law that would not create substantial inconsistencies with the DFS.[2]

In fact, a drafter's note to the NAIC Model specifies that compliance with the DFS Regulation would be deemed compliance with the NAIC Model.[3] There are, however, important differences and distinctions between the two regimes, and it is certainly possible that states will adopt the NAIC Model with their own revisions that could create additional inconsistencies, which would complicate compliance, and drive up the cost.

---

* Theodore P. Augustinos is a partner at Locke Lord LLP advising clients in various industries on privacy and data protection, cybersecurity compliance and incident preparedness, and breach response. He may be reached at ted.augustinos@lockelord.com.

1 23 NYCRR 500, effective March 1, 2017.

2 NAIC Model Law 668.

3 NAIC Model Law 668, § 2.

The NAIC Model, if and as adopted into law by the various states, would apply to licensees of state insurance regulators.[4] The DFS Regulation applies to all DFS licensees (as well as those required to obtain DFS permits, registrations, and other authorizations), including licensees in the insurance, banking and other financial services industries, but does not include securities firms, which are not, in New York, licensed by the DFS.[5]

It is interesting to note that the Colorado Division of Securities and the Vermont Securities Division have adopted regulations, similar in many respects to New York's, but specific to the securities industry.[6]

Between the NAIC Model and other state initiatives, the technical cybersecurity requirements for the financial services industry may certainly be expected to proliferate. Even for financial services participants outside the insurance industry, and for those in jurisdictions that may not take immediate action to adopt the NAIC Model, a review of the new duties would be well-advised, as the themes, if not the actual technical requirements, should be addressed in any serious cybersecurity program.

CRITICAL PROVISIONS OF THE DFS REGULATION AND THE NAIC MODEL

The following is a description of some of the critical provisions of the DFS Regulation and the NAIC Model, and the differences and nuances between them.

Information Security Program

Both the DFS Regulation and the NAIC Model require the adoption of an Information Security Program (called a Cybersecurity Program in the DFS Regulation) to govern the protection of data and systems.[7]

One of the important developments of the DFS Regulation and the NAIC Model is the recognition that cybersecurity must go further than protection of information, and must protect information and operating systems.[8]

Both the NAIC Model and the DFS Regulation contemplate that the program should take into account the size and sophistication of the licensee,

---

[4] NAIC Model Law 668, § 3I.

[5] 23 NYCRR 500.01(c).

[6] 3 CCR 704-1, § 51-4.8, 4.14(1A); V.S.R. § 8-4.

[7] 23 NYCRR 500.02; NAIC Model Law 668, § 4.

[8] 23 NYCRR 500.1(e) & (g); NAIC Model Law 668, § 3H & K.

and the nature of its risks, although the NAIC Model is more explicit on this point.[9]

Risk Assessment

Under both regimes, the Information Security Program itself, and the other, related policies and procedures, are to be based on a risk assessment.

The DFS Regulation is far more specific on the technical requirements for a risk assessment, including that it must be conducted in accordance with written policies and procedures.[10]

Qualified and Trained Personnel

As cybersecurity cannot be addressed with exclusively technical solutions, and as human error plays so prominently as a cause of compromises, both the DFS Regulation and the NAIC Model impose responsibilities related to personnel.[11]

The DFS obligations concerning personnel are far more exacting and onerous, but both require the designation of a specific person to be responsible for cybersecurity, and the implementation of awareness training for all personnel.

Access Control

A key element of any cybersecurity program, controlling access to information systems, is a specific requirement of both the DFS Regulation and the NAIC Model.[12]

Encryption

While the NAIC specifically requires encryption only of certain data transmitted over a public network, and stored on laptops and other mobile devices, the DFS Regulation also requires encryption of data at rest (e.g., on desktops and servers, or in storage), with some flexibility for compensating controls where encryption is not feasible.[13]

Notification of Certain Cybersecurity Events

Consistent with the new European regime under the General Data Protection Regulation, both the DFS Regulation and the NAIC Model require

---

[9] *See* NAIC Model Law 668, § 4(A).

[10] 23 NYCRR 500.09; NAIC Model Law 668, § 4C.

[11] 23 NYCRR 500.04, 500.10, 500.14(b); NAIC Model Law 688, § 4C(1), (4)(a), D(5).

[12] 23 NYCRR 500.07; NAIC Model Law 668, § 4D(2)(a).

[13] 23 NYCRR 500.15; NAIC Model Law 668, § 4D(2)(d).

notification to the regulator of certain compromises of data and systems within 72 hours.[14]

Both also leave the obligation to notify affected individuals and other parties to the general breach notification statutes, except that the NAIC Model also requires 72 hour notice by reinsurers to ceding insurers.[15]

Annual Certification of Compliance

Under both the DFS Regulation and the NAIC Model, annual certificates of compliance must be filed with the regulator.[16]

It is important to note, however, that the certification requirement of the NAIC Model applies only to insurance companies, and not to other licensees such as producers and others.[17]

Exemptions

Both the DFS Regulation and the NAIC Model contain exemptions for certain risk retention groups and others, but the DFS Regulation contains several additional, important exemptions.

For example, while the NAIC Model would exempt licensees with fewer than 10 employees, the small business exemption of the DFS Regulation also contains an asset and revenue threshold below which a business is exempt.[18] This could reflect the fact that the NAIC Model has expressly provided that its obligations are to be based on the size and sophistication of the licensee; the DFS Regulation has less built-in flexibility.

It is important to note that the DFS exemptions for certain covered entities are only partial, and still require compliance with significant elements of the DFS Regulation.[19]

Significantly, several NAIC Model exemptions are self-executing, while several of the exemptions under the DFS Regulation require the filing of a notification of exemption.[20]

FORECAST

As indicated by the new DFS Regulation, the NAIC Model, and the new cybersecurity regulations in Colorado and Vermont, the banking industry can

---

[14] 23 NYCRR 500.17(a); NAIC Model Law 668, § 6A, B.

[15] NAIC Model Law 668, § 6E.

[16] 23 NYCRR 500.17(b); NAIC Model Law 668, § 4I.

[17] NAIC Model Law 668, § 4I.

[18] 23 NYCRR 500.19(a); NAIC Model Law 668, § 9A.

[19] 23 NYCRR 500.19(a), (c), (d).

[20] 23 NYCRR 500.19(e).

expect increased regulatory focus on cybersecurity. This increased focus will likely take the form of additional and more specific requirements for the protection of the financial services industry's data and systems. In the United States, state regulators are expected to continue to drive most of the expected developments.