AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2017
VOL. 3 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 2 | February/March 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
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) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... 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 ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [297] (LexisNexis A.S. Pratt)

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. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2017 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

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

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

Emilio W. Cividanes
Partner, Venable LLP

Richard Cohen
Special Counsel, Kelley Drye & Warren LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Aaron P. Simpson
Partner, Hunton & Williams LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2017 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 Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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 *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

New Rules of the Cyber Road: Federal Banking Regulators' Proposed Cybersecurity Regulations

By Christopher C. Burris, Nicholas A. Oldham, Kyle Sheahen, and Joseph L. Zales*

This article focuses on proposed cybersecurity standards in an advance notice of proposed rulemaking jointly issued by key federal banking regulators: the Office of the Comptroller of the Currency, the Federal Reserve, and the Federal Deposit Insurance Corporation.

Continuing the trend of recent years, cybersecurity has remained at the top of the regulatory agenda for several federal and state agencies.[1] For financial institutions, keeping track of the dizzying array of proposed regulations is a challenge. This

* Christopher C. Burris (cburris@kslaw.com) is a partner in the White Collar Defense & Government Investigations Practice Group at King & Spalding LLP. Nicholas A. Oldham (noldham@kslaw.com) is a partner at the firm, assisting clients with cybersecurity and risk management, data privacy, incident response, internal and government investigations, and litigation. Kyle Sheahen (ksheahen@kslaw.com) and Joseph L. Zales (jzales@kslaw.com) (pending admission to the New York Bar) are associates in the firm's White Collar Defense & Government Investigations Practice Group.

[1] On October 20, 2016, the U.S. Department of the Treasury and the U.S. Department of Homeland Security co-hosted a meeting with financial regulators and financial services executives to discuss cybersecurity. *See* Readout from a Treasury Spokesperson of the Administration's Meeting with Financial Regulators and CEOs on Cybersecurity in the Financial Services Sector (Oct. 20, 2016).

On September 13, 2016, the New York Department of Financial Services ("DFS") issued Proposed Cybersecurity Requirements for Financial Services Companies. Entities covered by the law would include those currently licensed or registered under New York's banking, insurance, or financial services laws. As currently proposed, the requirements would mandate the establishment of a cybersecurity program, the adoption of a cybersecurity policy, the designation of a chief information security officer, penetration tests and vulnerability assessments, the implementation of audit trails, the establishment of access privileges, the creation of policies and procedures ensuring security of third-party service providers, and the encryption of all nonpublic information. While much of the DFS proposal is already standard practice at major financial institutions with sophisticated information technology departments, certain aspects appeared problematic, as either unduly onerous, overly prescriptive, or too broad in scope. The comment period closed November 12, 2016 and the requirements are scheduled to take effect January 1, 2017. *See* 23 NYCRR 500.

On September 8, 2016, the Commodity Futures Trading Commission ("CFTC') issued final rules on cybersecurity system safeguards. The CFTC's final rules, which apply to derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories, require five different types of cybersecurity testing: (1) vulnerability testing; (2) penetration testing; (3) controls testing; (4) security incident response testing; and, (5) enterprise technology risk assessments. The final rules will be published in the Federal Register. *See* Fact Sheet – Final Rules on System Safeguards Testing Requirements (September 8, 2016).

article focuses on proposed cybersecurity standards in an advance notice of proposed rulemaking jointly issued by key federal banking regulators: the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve, and the Federal Deposit Insurance Corporation ("FDIC").

The advance notice of proposed rulemaking was a formal invitation to participate in shaping any proposed cybersecurity standards and started the notice-and-comment process in motion. Per the rulemaking procedures, these agencies sought public comment on their initial proposal. The comment period closed on January 17, 2017.

THE OCC, FEDERAL RESERVE, AND THE FDIC

On October 19, 2016, the OCC, Federal Reserve, and the FDIC issued a joint advance notice of proposed rulemaking on enhanced cyber risk management standards.[2] At this early stage, the agencies sought assistance from the private sector in the form of comments on all aspects of their proposal. Relying on those comments, the agencies will then develop a more detailed proposal and conduct a subsequent notice-and-comment period. Therefore, entities who may not have previously commented but who might be subject to or impacted by any final standards will have an additional opportunity to shape the standards.

As currently drafted, entities subject to the potential standards would include depository institutions and depository institution holding companies with consolidated assets of $50 billion or more, the U.S. operations of foreign banking organizations with U.S. assets of $50 billion or more, as well as financial market infrastructures and nonbank

---

On August 29, 2016, the Federal Trade Commission ("FTC") announced it would seek public comment on its Standards for Safeguarding Customer Information ("Safeguards Rule"). The Rule, promulgated in 2003 pursuant to the Graham-Leach-Bliley Act ("GLBA"), applies to all financial institutions under the FTC's jurisdiction. As it stands, the Rule requires financial institutions to maintain a comprehensive information security program, particularly designed for protecting customer information. Such a program consists of the safeguards—technological, administrative, or physical—the financial institution employs in regards to the handling of customer information. In its current form, the Rule is not overly prescriptive, but rather requires just that the safeguards be "reasonably designed to achieve the [Rule's] objectives." The FTC sought comments on a number of general and specific issues under the Rule. As certain federal agencies are required by the GLBA to have their own standards for the safeguarding of customer information by financial institutions, any amendments made by the FTC to its Safeguards Rule—such as an increase in specificity or prescription—could very well trigger identical amendments across the board. The comment period closed November 21, 2016. *See* 81 Fed. Reg. 61632, 61633 (Sept. 7, 2016); 16 C.F.R. § 314.3.

[2] OCC: 12 CFR Part 30, Docket ID OCC-2016-0016, RIN 1557-AE06; Federal Reserve: 12 CFR Chapter II, Docket No. R-1550, RIN 7100-AE 61; FDIC: 12 CFR Part 364, RIN 3064-AE45.

financial companies supervised by the Federal Reserve.[3] As the agencies are concerned that cyber risks in one division of an entity could have a detrimental effect on other divisions, the proposed standards would apply to these covered entities on an enterprise-wide basis across all subsidiaries and affiliates. Notably, the agencies are also considering whether to apply the standards to third-party vendors servicing those institutions.

The proposed regulations are designed to increase the operational resilience of large financial institutions and reduce the impact a cyber-attack on one institution would have on the financial industry as a whole. To that end, the proposed standards address five categories:

1) cyber risk governance;
2) cyber risk management;
3) internal dependency management;
4) external dependency management; and
5) incident response, cyber resilience, and situational awareness.

In the category of *cyber risk governance*, the agencies are considering requiring covered entities to develop a written, board-approved, enterprise-wide cyber risk management strategy, complete with policies and reporting structures. As an entity's board of directors would be charged with overseeing and holding senior management accountable for cyber risk governance, board members may be required to have cybersecurity expertise or at least access to such expertise. In the second category of standards, the agencies are considering tasking three independent functions (*i.e.*, business units, independent risk management, and audit) with responsibility for *cyber risk management*. As an initial line of defense, business units would be required to assess cyber risks associated with their activities on a daily basis. An independent risk management function would then be required to identify cyber risks on an enterprise-wide basis and develop action plans to mitigate those risks. Finally, the audit function would be required to evaluate the appropriateness and effectiveness of the entity's overall risk management as part of its larger audit of the entity.

Categories three and four of the enhanced standards pertain to *internal* and *external dependency management*. Internal dependencies are the "business assets . . . upon which such entity depends to deliver services, as well as the information flows and interconnections among those assets." External dependencies are the "relationships with outside vendors, suppliers, customers, utilities . . . and other external organizations

[3] Generally, the standards would apply to large institutions (those with total consolidated assets of $50 billion or more) subject to the agencies' jurisdiction. *See* 12 U.S.C. §§ 321, 1818, 1831p-1 (Federal Reserve); 12 U.S.C. §§ 1, 93a, 161, 481, 1463, 1464, 1818, 1831p-1, 3901, 3909 (OCC); 12 U.S.C. §§ 1818, 1819, 1831p-1 (FDIC). Financial market infrastructures are multilateral systems among participating financial institutions used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions, and are supervised by the Federal Reserve pursuant to Dodd-Frank.

and service providers that the covered entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties." In both of these areas, the agencies are considering requiring covered entities to identify and rank all such dependencies and their associated cyber risks so as to prioritize their mitigation.

The final category of standards, *incident response, cyber resilience, and situational awareness*, addresses how a covered entity plans for and responds to a cyber-attack. The agencies are considering standards in this area that would require covered entities to execute plans allowing them to "anticipate, withstand, contain, and rapidly recover from a disruption caused by a significant cyber event." Indeed, as proposed, the standards require entities to be capable of operating critical functions both during and in the aftermath of cyber-attacks.

The agencies have stressed that these new standards would complement the existing regulatory framework.[4] Moreover, those financial institutions with "sector-critical systems"—systems whose failure would affect the entire financial industry—would be subject to an additional layer of more stringent standards, such as the requirement that these entities be able to fully recover from a cyber-attack in just two hours.

The federal regulators sought comment on all aspects of the proposed standards, including what form the final promulgation should take (*e.g.*, formal regulation or mere guidance), the scope of its application, the costs and benefits of the various proposed standards, possible methods for quantifying cyber risk, and defining what should constitute a sector-critical system.

In all, the regulators sought comment on 39 discrete questions. There are several particularly concerning issues with the standards as proposed, which affected entities should consider addressing during any future comment periods, including the following three.

Critically, as the identification of "sector-critical systems" at a financial institution would impose tougher regulations, defining the term fairly will be an important element of the comment process. As of now, the regulators are contemplating flagging as sector-critical those systems that support the clearing or settlement of five percent or more of the value of the transactions in a certain market and those that support five percent or more of the total U.S. deposits. Specially designating certain entities as systemically important furthers the regulatory goal of protecting the entire financial system from contagion following an attack. The additional standards accompanying

[4] The agencies have existing cybersecurity supervisory programs for financial institutions and their vendors under the Graham-Leach-Bliley Act, the Uniform Rating System for Information Technology, and the Federal Financial Institution Examination Council's Information Technology Handbook. According to the advanced notice of proposed rulemaking, the agencies would integrate into the existing supervisory framework the set of enhanced standards for the entities and services that potentially pose heightened cyber risk to the safety and soundness of the financial system.

such a designation, however, will undoubtedly impose significant implementation and compliance costs on these institutions.

It is therefore essential for the regulators to appropriately set the stringency of the second layer of sector-critical standards. In weighing the perceived benefit to the industry of these additional standards with their very real costs, covered entities should only be held to a standard of reasonableness.[5] In the cybersecurity context, the legal concept of "reasonableness" is fluid; reasonable standards are not overly prescriptive and are therefore adaptive to both changes in risk and technology environments. As proposed, the standards require covered entities to "implement[] the most effective, commercially available controls" to substantially minimize the risk of a disruption or failure in sector critical systems due to a cyber-event. While not overly prescriptive, if not framed in the broader context of "reasonableness," such a standard could essentially mandate unlimited spending.

A second potential sector-critical standard would require an incredibly quick recovery time of just two hours for such systems in the aftermath of a disruptive, corruptive, or destructive cyber-event. This recovery time would be required to be validated through rigorous stress testing. It is unsurprising that the agencies requested comment on the costs associated with and the feasibility of this two-hour recovery time for all sector-critical systems.

Finally, subjecting third-party service providers to both tiers of the proposed standards—as is being considered—is likely to increase the cost of business for financial institutions with a web of third-party relationships as those providers seek to offset their compliance and operating expenses.

NEXT STEPS

As mentioned above, the comment period closed in mid-January. The agencies plan to use the comments to develop a more detailed proposal, which would also be subject to notice and comment prior to any final rulemaking.

As malicious cyber-attacks evolve in sophistication and increase in number, agencies are working hard to ensure their regulated entities implement up-to-date cybersecurity controls. At the same time, financial institutions are faced with a constantly shifting goal post of regulatory expectations that is difficult and costly to achieve. Comment periods are critical for the private sector to demonstrate their concerns about the scope and impact of regulations in this area from an operational perspective. As the federal agencies considering these standards issued advance notice, covered financial institutions had a unique opportunity to truly shape the final regulations. Fortunately for entities who may not have previously commented, the next iteration of the agencies' proposed regulations will also be subject to a comment period.

[5] *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 256 (3rd Cir. 2015).