The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **MARCH 2022**

EDITOR'S NOTE: BANKING HISTORY IN THE MAKING
Victoria Prussen Spears

OFAC ISSUES SANCTIONS GUIDANCE TO VIRTUAL CURRENCY INDUSTRY
Abena Mainoo, Chase D. Kaniecki, Michael G. Sanders, John Lightbourne and William S. Dawley

FEDERAL BANK REGULATORS SET OUT REGULATORY ROADMAP FOR CRYPTO-ASSETS
Clifford S. Stanford, Brian D. Frey, Brendan Clegg and Jessica Garcia Keenum

U.S. FEDERAL BANKING AGENCIES ISSUE RULE REQUIRING BANKS TO NOTIFY REGULATORS OF CYBER INCIDENTS WITHIN 36 HOURS
Daniel Silver, Megan Gordon, Celeste Koeleveld, Philip Angeloff, Brian Yin and Shannon O'Brien

FINANCIAL INSTITUTIONS NEED TO KEEP UP WITH THE CHANGING BUSINESS OF RANSOMWARE
Michael A. Mancusi, Kevin M. Toomey, Nancy L. Perkins, Anthony Raglani, Daniel E. Raymond and Kara Ramsey

OCC ADVISES BANKS TO CAREFULLY EVALUATE VENTURE CAPITAL FUND INVESTMENTS
David F. Freeman, Jr., Kevin M. Toomey and Anthony Raglani

U.S. BANK REPORTING HANDBOOK UPDATED BY OCC
Jeffrey P. Taft and Matthew Bisanz

NAVIGATING FAIR LENDING AND REDLINING CONSIDERATIONS UNDER THE BIDEN ADMINISTRATION
Abigail M. Lyle and Nicole Skolnekovich

NEW YORK IMPOSES COMMUNITY REINVESTMENT ACT REQUIREMENTS ON MORTGAGE BANKERS
Bob Jaworski

FIFTH CIRCUIT HOLDS DIFFICULT ECONOMIC CIRCUMSTANCES INSUFFICIENT TO CLAIM DURESS; LENDERS ENTITLED TO THREATEN TO EXERCISE CONTRACTUAL RIGHTS AS NEGOTIATING LEVERAGE
Gregory G. Hesse and Jennifer E. Wuebker

CURRENT DEVELOPMENTS
Steven A. Meyerowitz

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 3** **March 2022**

Editor's Note: Banking History in the Making
Victoria Prussen Spears 109

OFAC Issues Sanctions Guidance to Virtual Currency Industry
Abena Mainoo, Chase D. Kaniecki, Michael G. Sanders, John Lightbourne and William S. Dawley 112

Federal Bank Regulators Set Out Regulatory Roadmap for Crypto-Assets
Clifford S. Stanford, Brian D. Frey, Brendan Clegg and Jessica Garcia Keenum 118

U.S. Federal Banking Agencies Issue Rule Requiring Banks to Notify Regulators of Cyber Incidents Within 36 Hours
Daniel Silver, Megan Gordon, Celeste Koeleveld, Philip Angeloff, Brian Yin and Shannon O'Brien 122

Financial Institutions Need to Keep Up with the Changing Business of Ransomware
Michael A. Mancusi, Kevin M. Toomey, Nancy L. Perkins, Anthony Raglani, Daniel E. Raymond and Kara Ramsey 126

OCC Advises Banks to Carefully Evaluate Venture Capital Fund Investments
David F. Freeman, Jr., Kevin M. Toomey and Anthony Raglani 130

U.S. Bank Reporting Handbook Updated By OCC
Jeffrey P. Taft and Matthew Bisanz 134

Navigating Fair Lending and Redlining Considerations Under the Biden Administration
Abigail M. Lyle and Nicole Skolnekovich 138

New York Imposes Community Reinvestment Act Requirements on Mortgage Bankers
Bob Jaworski 143

Fifth Circuit Holds Difficult Economic Circumstances Insufficient to Claim Duress; Lenders Entitled to Threaten to Exercise Contractual Rights as Negotiating Leverage
Gregory G. Hesse and Jennifer E. Wuebker 148

Current Developments
Steven A. Meyerowitz 152

LexisNexis®

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)
ISSN: 0005-5506 (Print)

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.

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

MATTHEW BENDER

(2022–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

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. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries 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, 631.291.5541. 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.

U.S. Federal Banking Agencies Issue Rule Requiring Banks to Notify Regulators of Cyber Incidents Within 36 Hours

By Daniel Silver, Megan Gordon, Celeste Koeleveld, Philip Angeloff, Brian Yin and Shannon O'Brien*

The authors of this article discuss a final rule issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation requiring banking organizations to notify their primary federal regulator of significant computer-security incidents no later than 36 hours after determining the incident has occurred.

The Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation ("FDIC"), (the "Agencies"), have issued a final rule[1] requiring banking organizations to notify their primary federal regulator of significant computer-security incidents no later than 36 hours after determining the incident has occurred. The rule also requires bank service providers to notify their banking organization customers of any computer-security incident that has caused, or will likely cause, significant disruption. The rule imposes substantial new cyber security reporting requirements on banks with an effective compliance date of May 1, 2022.

Current rules only require reporting of certain categories of cyber incidents (such as breaches of sensitive customer information) and generally permit longer reporting periods. For example, banks must report incidents involving sensitive customer information to their primary federal regulator as soon as possible, but there is no specific deadline. Indeed, the Agencies noted in guidance accompanying the rule that notifications made under existing standards were often delayed—and in many cases banks did not report cyber incidents at all. Thus, the Agencies determined that heightened notification standards were warranted to allow for better coordination and supervision of incident response.

---

* Daniel Silver (daniel.silver@cliffordchance.com), Megan Gordon (megan.gordon@cliffordchance.com) and Celeste Koeleveld (celeste.koeleveld@cliffordchance.com) are partners at Clifford Chance US LLP. Philip Angeloff (philip.angeloff@cliffordchance.com) is counsel and Brian Yin (brian.yin@cliffordchance.com) is an associate at the firm. Shannon O'Brien (shannon.obrien@cliffordchance.com) is a law clerk at the firm (not yet admitted to the Bar).

[1] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

BANKING ORGANIZATIONS' OBLIGATION TO REPORT

Under the final rule, banking organizations must report to their primary federal regulator any "computer-security incident" that rises to the level of a "notification" incident as soon as possible and no later than 36 hours after the incident occurs. "Banking organizations" include federal and state licensed banks, federal and state savings associations, U.S. branches of foreign banks, and bank and thrift holding companies.

What Types of Incidents Do I Have to Report?

The rule only requires banking organizations to notify their regulator of a computer-security incident that rises to the level of a "notification" incident. A notification incident is an incident that has, or is reasonably likely to, "materially disrupt or degrade" a banking organization's:

- Ability to provide services to "a material portion of its customer base;"
- Business lines, the failure of which "would result in a material loss of revenue, profit or franchise value;" or
- Operations, the failure of which "would pose a threat to the financial stability of the United States."

The Agencies provided several examples of what they consider to be "notification" incidents:

- A large-scale distributed denial of service attack that disrupts customer accounts for an extended period (four hours in the provided example);
- A failed system upgrade that results in widespread user outages for customers and employees;
- A computer hacking incident that disables banking operations for an extended period; or a ransom malware attack that encrypts a core banking system of backup data.

Notably, these examples make clear that the reporting requirement does not just apply to external attacks—internal incidents may also require reporting if they result in material disruptions or degradations to customer service.

When Is a Report Required?

The rule requires reports to be made within 36 hours, but this timeframe does not begin until a banking organization determines a notification incident has occurred. Guidance from the Agencies makes clear that they do not consider the clock to necessarily start when the incident occurs. Rather, the Agencies anticipate that banking organizations will need to take a reasonable

amount of time to investigate and determine that an incident rises to the level of a notification incident before the 36-hour clock starts.

Several commenters objected to the 36-hour timeframe, advocating for a 72-hour requirement to align with the reporting requirements of the New York State Department of Financial Services ("NYDFS") Cybersecurity Regulation and the EU General Data Protection Regulation ("GDPR"). However, the Agencies ultimately determined the shorter 36-hour timeframe to be appropriate in light of the high threshold for reporting and the relatively limited information that is required to be included in a report.

What Goes in a Report?

The rule requires banking organizations to provide their regulator with only a "simple notice" when they suffer a reportable incident. This notice is limited to "general information" about the incident that is known at the time the notification is made. There are no specific requirements with regards to what information is contained in the notification. In the report accompanying the rule, the Agencies explained that they intentionally kept the notification requirements minimal to facilitate prompt reporting and to lessen the administrative burden on affected organizations.

Are Reports Public?

The notification, and any information related to the incident, would be subject to the applicable agency's confidentiality rules, which provide protections for confidential, proprietary, supervisory, and sensitive personally identifiable information. However, the Agencies are still required to respond to individual Freedom of Information Act requests, which could implicate the reported information, on a case-by-case basis.

BANK SERVICE PROVIDERS' OBLIGATION TO REPORT

The final rule also affects bank service providers, who often provide technological infrastructure services that may be subject to cyber incidents. Under this regulation, a bank service provider will be required to notify each affected banking organization as soon as possible when it determines a computer-security incident has occurred that has, or is reasonably likely to, "materially disrupt or degrade" covered services provided for four or more hours. A "covered service" is any service that is subject to the Bank Service Company Act, which includes check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, online and mobile banking, data processing, and other clerical, bookkeeping, accounting, statistical, or similar functions.

The Agencies expect bank service providers to work together with their banking organizations to designate a method of communication and point of contact that works best for both parties. In the absence of a point of contact, notification should be made to the chief executive officer and chief information officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

The Agencies intend for this notification requirement to be "simple and flexible" and expect bank service providers to make their best effort to notify the banking organizations as soon as possible, so the banking organization can determine if the incident qualifies as a notification incident, triggering its own reporting requirement.

TAKEAWAYS

This rule represents a significant new regulatory obligation for banking organizations and bank service providers. While the reports themselves need not be detailed, ensuring that accurate information is provided quickly in the aftermath of a cyber incident can be difficult. Importantly, however, the Agencies narrowed the definition of a reportable incident in the final rule to only include incidents that cause actual, rather than potential harm, and excluded violations of internal policies that do not otherwise have a disruptive impact.

The Agencies estimate there will be approximately 150 notification incidents reported annually but acknowledge this number may increase in the future. The Agencies arrived at this estimate after reviewing Suspicious Activity Report ("SAR") filings from 2019 and 2020, which they acknowledge do not capture the full scope of incidents addressed by the final rule, and by analyzing the frequency at which notification incidents have already been voluntarily reported by banking organizations.

The final rule becomes effective April 1, 2022, but has a compliance date of May 1, 2022, to allow organizations additional time to implement the rule. Before the rule becomes effective, affected financial institutions should update their incident response plans to ensure that information regarding significant cyber incidents is promptly escalated to internal stakeholders who can determine if notification is required. Banks should also work with their service providers to develop notification protocols, including a designated point of contact, preferred method of communication, and specify the key information to be included in a report.

Relevant service agreements should be updated to incorporate these notification requirements.