

# The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

June 2024

**Editor's Note: ESG**

Victoria Prussen Spears

**The Continued Evolution of the Anti-ESG Landscape for Financial Institutions**

Randy Benjenk and Emily Hooker

**Fintech Corporations: Defining the Practice and Regulation of Innovative Financial Enterprises – Part II**

Lerong Lu

**It's Not Your Fault, But It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks**

Kayleigh S. Shuler

**Looking Ahead to the Federal Trade Commission's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions**

Alexander D. Boyd and Colin H. Black

**U.S. Office of the Comptroller of the Currency Begins to Revamp Bank Merger Review Process**

Michael D. Lewis and Matthew S. Katz

**The Benefits of Term Debt Tranches in Fund Finance Products, and What to Consider When Utilizing Term Debt**

Kiel A. Bowen, Mark C. Dempsey and Andrew L. Hogan

**New York Department of Financial Services Adopts Final Guidance on Assessment of Character and Fitness of Directors, Senior Officers and Managers**

Jarryd E. Anderson, Jessica S. Carey and Roberto J. Gonzalez

**Declined: Consumer Financial Protection Bureau Proposes Rule to Limit Nonsufficient Funds Fees**

Andrew E. Bigart, Max Bonici, Michael M. Aphibal, David A. McGee and Brandon Wong



LexisNexis

# THE BANKING LAW JOURNAL

---

VOLUME 141

NUMBER 6

June 2024

---

<b>Editor's Note: ESG</b> Victoria Prussen Spears	237
<b>The Continued Evolution of the Anti-ESG Landscape for Financial Institutions</b> Randy Benjenk and Emily Hooker	240
<b>Fintech Corporations: Defining the Practice and Regulation of Innovative Financial Enterprises – Part II</b> Lerong Lu	259
<b>It's Not Your Fault, But It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks</b> Kayleigh S. Shuler	270
<b>Looking Ahead to the Federal Trade Commission's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions</b> Alexander D. Boyd and Colin H. Black	273
<b>U.S. Office of the Comptroller of the Currency Begins to Revamp Bank Merger Review Process</b> Michael D. Lewis and Matthew S. Katz	277
<b>The Benefits of Term Debt Tranches in Fund Finance Products, and What to Consider When Utilizing Term Debt</b> Kiel A. Bowen, Mark C. Dempsey and Andrew L. Hogan	282
<b>New York Department of Financial Services Adopts Final Guidance on Assessment of Character and Fitness of Directors, Senior Officers and Managers</b> Jarryd E. Anderson, Jessica S. Carey and Roberto J. Gonzalez	286
<b>Declined: Consumer Financial Protection Bureau Proposes Rule to Limit Nonsufficient Funds Fees</b> Andrew E. Bigart, Max Bonici, Michael M. Aphibal, David A. McGee and Brandon Wong	293

**QUESTIONS ABOUT THIS PUBLICATION?**

---

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Matthew T. Burke at ..... (800) 252-9257  
Email: ..... matthew.t.burke@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call or email:

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.

---

This publication is designed to provide authoritative information in regard to the subject matter covered. It 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 RELX Inc. Matthew Bender, the Matthew Bender Flame Design, and A.S. Pratt are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2024 Matthew Bender & Company, Inc., a member of LexisNexis. All Rights Reserved. No copyright is claimed by LexisNexis or Matthew Bender & Company, Inc., 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.

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

MATTHEW  BENDER

# *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**

**CARLETON GOSS**

*Partner, Hunton Andrews Kurth LLP*

**DOUGLAS LANDY**

*White & Case LLP*

**PAUL L. LEE**

*Of Counsel, Debevoise & Plimpton LLP*

**TIMOTHY D. NAEGELE**

*Partner, Timothy D. Naegele & Associates*

**STEPHEN J. NEWMAN**

*Partner, Steptoe & Johnson LLP*

**ANDREW OLMEM**

*Partner, Mayer Brown 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 2024 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](mailto: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](mailto: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.

# It's Not Your Fault, But It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks

*By Kayleigh S. Shuler\**

*In this article, the author explains how a vendor's data incident can be nearly as time-consuming, costly and reputationally damaging as an internal incident.*

For organizations that watched (or worse, lived through) the fallout from recent large-scale vendor incidents, the prospect of learning that a trusted vendor has experienced a data incident is almost as distressing as the idea of the organization experiencing an incident itself.

That's because a vendor incident – meaning an incident that occurs at or is otherwise caused by a third-party service provider – can be nearly as time-consuming, costly and reputationally damaging as an internal incident.

## **CHALLENGES OF VENDOR INCIDENTS**

Vendor incidents can come with all the usual challenges of any security event – operational disruptions, public relations pressures and concerns about data compromise – but often come with the added element of being “in the dark” until a vendor decides to share details about what happened and what they're doing about it.

Additionally, depending on the vendor's level of cooperation, the ultimate responsibility to notify individuals may land on the company, even though it is not at fault.

All the while, an individual who learned that their data may have been compromised will likely point the finger back at whomever they entrusted their data to, regardless of whether that company is truly where the breach occurred.

## **INCREASING REGULATORY ATTENTION**

Regulatory bodies, particularly those in the financial industry, are increasingly taking note of this type of incident and raising the level of attention they pay to vendor management. Questions that often come after a company notifies regulators of a vendor incident include:

- What level of diligence did your organization conduct before trusting a vendor with data?
- If the vendor made security-related promises – such as to delete data

---

\* The author, an attorney with Polsinelli PC, may be contacted at [kshuler@polsinelli.com](mailto:kshuler@polsinelli.com).

after contract termination – did your organization confirm those promises were kept?

- Why was a vendor holding so much data for so long?

In 2023, we saw regulatory efforts to gain more insight into these relationships and the risks they pose in the National Credit Union Administration's (NCUA) approval of a final rule that requires a federally insured credit union to report "reportable cyber incidents" to the NCUA as soon as possible, and in no event later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.<sup>1</sup> Under the rule, the NCUA suggests that if a third party reports experiencing a breach of a credit union's sensitive member information, that credit union likely needs to report to incident to NCUA.<sup>2</sup> Credit unions have apparently heeded that advice. According to NCUA Chairman Todd M. Harper, "[i]n the first 30 days after the rule became effective, the NCUA received 146 incident reports, more than it had received in total in the previous year. More than 60 percent of these incident reports involve third-party service providers and credit union service organizations."<sup>3</sup>

Regulators overseeing banks have so far approached the issue from a slightly different and less direct direction but with a similar result. In guidance issued June 6, 2023, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency (the Banking Agencies) provided detailed guidance to banking organizations on vendor management throughout the life cycle of a vendor relationship. This guidance included oversight and accountability procedures for the life of the relationship.<sup>4</sup> This guidance added to an existing rule issued from the Banking Agencies which requires bank service providers to notify bank customers as soon as possible upon experiencing certain types of incidents.

---

<sup>1</sup> 12 CFR § 748.1(c).

<sup>2</sup> See Appendix A: Examples of Substantial Incidents that Likely Would Qualify as Reportable Cyber Incidents, available at <https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/cyber-incident-notification-requirements/appendix-a>.

<sup>3</sup> See testimony of NCUA Chairman Todd M. Harper Before the Senate Banking, Housing, and Urban Affairs Committee, available at [https://ncua.gov/newsroom/testimony/2023/ncua-chairman-todd-m-harpers-written-testimony-senate-banking-housing-and-urban-affairs-committee#:~:text=In%20the%20first%2030%20days,union%20service%20organizations%20\(CUSOs\)](https://ncua.gov/newsroom/testimony/2023/ncua-chairman-todd-m-harpers-written-testimony-senate-banking-housing-and-urban-affairs-committee#:~:text=In%20the%20first%2030%20days,union%20service%20organizations%20(CUSOs)).

<sup>4</sup> See Interagency Guidance on Third-Party Relationships: Risk Management, available at <https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf>.

## LOOKING AHEAD

Looking ahead, we can expect continued vendor incident scrutiny on both vendors and the organizations they serve. For its part, the NCUA is currently seeking congressional authority to directly examine third-party vendors, which it cannot do under existing law.

In testimony before Congress, the NCUA has stated that its inability to directly regulate credit union providers “creates a regulatory blind spot”<sup>5</sup> and that without this power, “NCUA is unable to effectively protect credit unions and their members.”<sup>6</sup> If Congress agrees, the NCUA may be given authority to demand information from vendors or impose corrective action plans on them, which vendors can largely ignore under current law.

Given the frequency with which vendor incidents are occurring and the increased regulatory interest in them, organizations should think through what they can do to position themselves for a strong response. For instance, consider: If a regulator inquired about how we vetted a vendor, are we comfortable with our answer? Is our vendor management program robust? For those on the vendor side of the coin, the challenges are similar, but the key questions are different. Here, consider: if customers impose additional security vetting, are we prepared to provide the accurate and digestible information they’ll need to feel comfortable partnering with us?

In all cases, increasing regulatory attention to vendor security should be top of mind.

---

<sup>5</sup> See testimony of NCUA Director of Office of Financial Technology and Access Charles A. Vice before the Subcommittee on Digital Assets, Financial Technology and Inclusion.

<sup>6</sup> Harper testimony, *supra* note 3.