The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION JULY-AUGUST 2020

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 137 **NUMBER 7** **July-August 2020**

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.

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 © 2020 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

MATTHEW BENDER

(2020-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
BARKLEY CLARK
Partner, Stinson Leonard Street LLP

MICHAEL J. HELLER
Partner, Rivkin Radler LLP

SATISH M. KINI
Partner, Debevoise & Plimpton LLP

DOUGLAS LANDY
Partner, Milbank, Tweed, Hadley & McCloy LLP

PAUL L. LEE
Of Counsel, Debevoise & Plimpton LLP

TIMOTHY D. NAEGELE
Partner, Timothy D. Naegele & Associates

STEPHEN J. NEWMAN
Partner, Stroock & Stroock & Lavan 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 2020 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 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, 646.539.8300. 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.

Banks: 5 Tips to Avoid Being Blindsided by a Lawsuit for a Customer's Misdeeds

Alex C. Lakatos [*]

Why do plaintiffs sue banks when it was bank customers who ran the Ponzi scheme? As bank robber Willie Sutton said when asked why he robbed banks: "[B]ecause that's where the money is." This article offers tips and guidance to minimize a bank's risk when it learns of a customer's wrongdoing.

When a Ponzi scheme collapses, financial institutions that happened to provide accounts or other financial services to the Ponzi schemers are often hit with lawsuits seeking to hold the banks liable for the losses caused by the scheme.

Typically, plaintiffs – who may be investors in the scheme or court-appointed receivers who are tasked to collect funds for the investors' benefit – argue that the bank was negligent in failing to prevent the scheme or that the bank intentionally abetted the scheme, or both. Plaintiffs routinely ask the court to infer the bank's intent based on "Monday morning quarterbacking," in which they argue that the fraud was so obvious, and the bank's compliance shortcomings so egregious, that the bank must have known about the fraud. In addition, plaintiffs who argue that the bank acted intentionally often allege that the bank had a rogue employee, one who willingly cooperated with the Ponzi schemers, perhaps to increase the employee's book of business or respond to sales pressure.

History demonstrates that the market collapse accompanying the COVID-19 pandemic very likely will result in an increase in Ponzi scheme enforcement actions. In economic downturns, U.S. government regulators, such as the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency, bolster their efforts to oversee that financial institutions are using every tool in their toolkit to discover and report suspicious activity. Similar events occurred after the 2008 market collapse, where the Securities and Exchange Commission ("SEC") filed a significant number of enforcement actions to bring down Ponzi schemes brought to light by the market collapse.

---

[*] Alex C. Lakatos is a partner in the Washington, D.C., office of Mayer Brown's Litigation & Dispute Resolution and Financial Services Regulatory & Enforcement practices. He may be contacted at alakatos@mayerbrown.com. The author wishes to thank James B. Danford Jr., an associate at the firm, for his assistance with this article.

Financial institutions that act promptly when they learn that one of their customers is accused of orchestrating a Ponzi scheme (or similar fraud) can materially limit their exposure and position themselves to effectively defend against lawsuits that may follow. This article provides some practical guidance.

THINK LIKE A PLAINTIFF/RECEIVER

A key to risk mitigation is to think about how a plaintiff would approach proving its case.

Act under a cloak of privilege. Consider having a lawyer oversee the investigation, including the BSA/AML teams' investigation, to maintain privilege. Banks often ask their financial investigations unit or other non-privileged persons to investigate whether the bank acted appropriately where fraudsters took advantage of the bank's services. These investigations, however, are not privileged and are subject to the overly intrusive discovery tactics that the bank will most likely face from a plaintiff or receiver. An experienced outside counsel will be able to limit risk and assist the bank in handling sensitive information that may surface during an investigation.

Understand the facts. First determine which are the main accounts involved, whether the fraudsters have other accounts at the bank, who at the bank serviced the accounts, whether the bank had all of the necessary materials to open the account (such as a company's articles of incorporation or similar documents), who had authorization to make transactions on the accounts, and what unusual activity occurred (if any). If certain transactions seem particularly concerning, conduct a deeper dive, which may include speaking with the relevant employees. Identifying this information in the beginning will save the bank time and money once it engages in a more thorough review of the circumstances.

Combat the rogue employee theory. Utilize internal investigations to see if you have a rogue employee, a potential rogue employee, or an employee who may be unfairly accused of being a rogue. Identify likely arguments you may see leveled against your employees. For example, was any employee uniquely assigned to work for the fraudsters, (such as a personal banker)? Consider what motivations plaintiffs could argue that a bank employee had to overlook bad conduct by a fraudster, such as financial incentives, promotion pressure, or a personal relationship with the fraudsters. Even if there is no obvious "rogue" employee, plaintiffs may seek to use these motivations to paint a bank employee as a bad actor. Review personnel files of key individuals to ensure there are no negative incidents that overlap with a time they serviced a fraudster. If there are

facts that might help a plaintiff accuse an employee who you conclude was not complicit in the fraud, gather counterevidence while memories and documents are fresh.

Address actual rogue employees. Depending on the severity of the suspected employee misconduct, it may be appropriate to place a problematic employee on leave or probation while your investigation plays out. Ensure that the employee is not in a position to destroy any data or conduct any further misconduct. If you ultimately conclude that you have a rogue employee, you likely will need to terminate them while, if possible, preserving their testimony and maintaining their cooperation.

Combat Monday morning quarterbacking. To begin, consider if any actions violated, or arguably violated, bank policies and procedures concerning Bank Secrecy Act ("BSA")/anti-money laundering ("AML") compliance or "know your customer" ("KYC") rules. Plaintiffs often try to conflate violations of internal bank rules with knowledge of the Ponzi scheme or recklessly ignoring its existence. Consider speaking with internal and external subject matter experts (e.g., outside counsel, the bank's risk consultant) about what the bank's policies require, particularly in the context of the fraudsters' actions. It may also be beneficial to review the timing and substance of employee training on the specific policies at issue. A good understanding of the policies and procedures will assist the bank to determine its potential exposure and whether any employee failed to adhere to any particular policy.

PRESERVE KEY DOCUMENTS, INFORMATION, AND PEOPLE

Upon learning that bank customers were involved in a Ponzi scheme, immediately preserve documents and information.

Formal hold notice. Consider whether the bank should circulate a formal hold notice. Note that if the bank does so, and makes clear that it is doing so because it anticipates potential litigation, a bank's internal investigation is also likely to benefit from the protections of the work product doctrine, which protects materials prepared in anticipation of litigation.

Key categories of documents include:

- *Account records*. Preserve account records that will be relevant to the investigation and potential litigation, such as account opening forms and documents, account statements, transaction documents, and signature cards.
- *Alerts*. Preserving BSA and fraud alert information is also vital. For example, were there investigations by the bank's financial crimes unit or

did the bank's automated account monitoring system generate any alerts relevant to the fraudsters' transactions? Knowing why certain alerts did or did not trigger is important to determining exposure related to the fraudsters' actions.

- *SARs*. While suspicious activity reports ("SARs") and materials reflecting whether a SAR was filed are privileged, the documents reviewed by the bank's BSA/AML investigators that were generated in the ordinary course of business are not. Unusual activity reports that may – or may not – lead to a SAR also may fall outside the scope of SAR privilege. The scope of SAR privilege is a complex question that may vary between jurisdictions. Experienced counsel can assist in determining which documents can be appropriately withheld on SAR privilege grounds.
- *Communications*. Review if any relevant communications exist. This includes emails, phone logs, transcriptions of phone conversations, and the like. These communications may be between the bank and the fraudsters or may be internal within the bank, such as a personal banker's call to the bank's internal transaction fraud support personnel or a comment made by a banker or teller in their respective computer programs. It also includes any communications between financial institutions, such as a request under Section 314(b) of the USA PATRIOT Act (Section 314(b) requests may be protected by privilege under certain circumstances).
- *Policies and procedures*. Preserve past policies and procedures. First, the investigators should review and familiarize themselves with the policies that were in place at the time of the transactions. This period may span over several years, as Ponzi schemes are generally carried out over a significant period of time. Evolution in the law, in threats faced by banks, and in banks' own learning of better ways to carry out their activities may warrant changes in bank policies. For this reason, make sure the bank has all of the policies and procedures relevant to the period the fraudsters committed their misdeeds, particularly those concerning negotiable instruments, withdrawals, wire transfers, and reporting unusual activity. This also means making sure there are no unique policies and procedures for the particular branch or branches the fraudsters used to conduct their scheme.
- *Preserve witnesses*. First, get interview memoranda when memories are fresh. Determine which bankers, tellers, managers, or other personnel serviced the fraudsters. What information about the fraudsters can these individuals recall? In what format have they communicated with

the fraudsters (text messages, email, phone calls, or in-person visits)? Do they recall any unusual or inconsistent activity related to the fraudsters' accounts? Are there any instances that, though maybe not violating protocol, can be exploited by the plaintiff? For example, consider whether the bank employee ever met with the fraudsters outside of the branch store location. Anything that demonstrates the fraudsters' relationship was more than a normal banking-customer relationship should spur further investigation.

Also, employees might stop working for the bank while it is investigating the fraudsters. Consider cooperation agreements for exiting employees, or at least obtain oral commitments from outgoing employees to cooperate and notify the bank if they are contacted. At a minimum, obtain updated contact information of the employee upon their departure. Their testimony may be vital to the bank's defense.

BE AWARE OF ADVERSE WITNESSES

An early understanding of who may be an adverse witness is key to an effective and efficient investigation and defense. Among others, adverse witnesses may include former bank employees or the fraudsters themselves.

Former employees. From former bank employees, the plaintiff may seek pre-suit interviews and perhaps pre-suit declarations. Later, plaintiffs may elicit through deposition or trial testimony that certain protocols were not followed, that the bank should have known about the Ponzi scheme, or that certain bank employees were complicit. Accordingly, consider whether any former employee would be motivated to speak unfavorably against the bank. An employee's relationship with the bank may have ended under less-than-optimal circumstances or the employee was otherwise disgruntled. If such former employees exist, develop a strategy for whether and how to approach them. Approaching them may be imprudent because it may expose the bank's concerns. However, obtaining the views of relevant former employees, and even offering them representation, may be the basis for a valuable transparent relationship.

Fraudsters. Fraudsters as witnesses can cause major disruptions to the bank's defense. For example, the fraudsters may say that the bank was aware of their actions, that the fraudsters worked with specific bank personnel exclusively, or that they chose the bank because of purported lax security measures. As their history of committing fraud suggests, and as experience teaches, fraudsters may say negative things about the bank for personal gain, such as entering into plea agreements that reward the fraudsters with a lighter sentence or less restitution

in exchange for "cooperation" against the bank. This could result in the fraudsters cooperating with the SEC or other agencies in their efforts to seek restitution from the bank.

If managed correctly, however, fraudsters can, in certain cases, be an asset to the bank. Especially to the extent that these individuals maintain their innocence, they may be willing to provide the bank with a declaration that they never informed any bank employees about their activities, which bolsters a bank's lack of knowledge defense. They also may provide information that demonstrates that their relationship with the bank was nothing more than a normal banking-customer relationship or that the fraudsters chose the bank solely for geographic convenience.

Generally, dealing with adverse witnesses is an action better handled by outside counsel as opposed to an in-house legal team. For example, outside counsel can schedule one-on-one meetings with individuals who the bank otherwise likely would not communicate with. This includes former bank employees who may have left the bank on unpleasant terms, the fraudsters themselves, or the fraudsters' counsel.

BE AWARE OF HOW PRE-SUIT DOCUMENT PRODUCTIONS MAY BE UTILIZED AGAINST THE BANK

The SEC, Commodity Futures Trading Commission ("CFTC"), the U.S. Department of Justice ("DOJ"), and local U.S. Attorneys offices are often involved in investigating and prosecuting fraudsters. Each may subpoena various financial institutions for records relevant to the case – and may share the bank's documents with court appointed receivers. Accordingly, assume any documents produced may be shared with a receiver seeking to recover assets for the investors.

Further, plaintiff investors may bring actions against the fraudsters, or a receiver may sue "winning investors" to try to increase the size of the receivership estate. In these actions, the plaintiff may seek certain information from the bank. View such requests as a precursor for a potential lawsuit against the bank in the near future.

STAY VIGILANT AND FOLLOW THE PONZI SCHEMER'S CASE

Stay informed regarding the status of suits and prosecutions against the Ponzi schemers, including by routinely reviewing the relevant dockets and media coverage. This may involve monitoring multiple cases. For instance, the SEC may bring a civil case, the DOJ may simultaneously prosecute a criminal case

against the Ponzi schemers, and the receiver/investors may simultaneously sue them civilly. A receiver also may bring ancillary proceedings to seize the fraudsters' assets.

Filings and discovery in these cases may be helpful to the bank. For example, sworn declarations by SEC or CFTC enforcement officers or accountants may provide a detailed description of the bank's alleged role in providing banking services to the Ponzi schemers.

Similarly, a temporary restraining order or asset freeze order may detail the accounts at issue and the relevant time period. Orders appointing a receiver or expanding the receivership can help the bank better understand the underlying allegations of how the scheme operated or anticipate claims. The record also may contain hearing, deposition, or trial transcripts that further shed light on the bank's potential exposure. It is common for a fraudster to invoke their Fifth Amendment rights, particularly as their Ponzi scheme case progresses.

Therefore, early transcripts may be the only means of capturing the fraudsters' statements, other than by speaking with the fraudsters' counsel or by requesting that the fraudsters agree to provide a declaration (which can sometimes be obtained through negotiations). Banks also should review receiver status reports and motions to approve disbursement of funds. These often showcase settlements or amounts seized and repaid to investors, thus offsetting potential damages levied on the bank.

CONCLUSION

Unfortunately, losing investors and court-appointed receivers will continue to look to financial institutions as "deep pockets" from whom they can recoup their losses when a Ponzi scheme collapses, even in cases where the financial institution has done nothing improper. Banks that take the steps above promptly, when they become aware their customers are implicated in a Ponzi scheme, can decrease their risk of being sued and increase their likelihood of effectively defeating unwarranted litigation against them.