The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

MARCH 2022

LexisNexis

THE BANKING LAW JOURNAL

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

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.

Financial Institutions Need to Keep Up with the Changing Business of Ransomware

By Michael A. Mancusi, Kevin M. Toomey, Nancy L. Perkins, Anthony Raglani, Daniel E. Raymond and Kara Ramsey*

The authors of this article discuss an updated Financial Crimes Enforcement Network Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, which underscores the need for financial institutions to be on guard for signs that their customers are attempting to make or receive ransomware payments.

The Financial Crimes Enforcement Network ("FinCEN") issued an updated version of its Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (the "Advisory").[1] The Advisory emphasizes that financial institutions should be on guard for signs that their customers are attempting to make or receive ransomware payments—even as the logistics of the ransomware business become increasingly complicated.

BACKGROUND

The updated Advisory, which replaces FinCEN's October 1, 2020, advisory of the same name, comes against the backdrop of increasing ransomware attacks against U.S. institutions and infrastructure and a rising enforcement response from the U.S. government as the Biden administration continues its "whole-of-government" approach to ransomware.[2]

The same day that FinCEN published its Advisory, the U.S. Department of the Treasury announced that its Office of Foreign Assets Control ("OFAC") had sanctioned two ransomware operators, a Ukrainian citizen and a Russian citizen, and the virtual currency exchange Chatex for their respective roles in ransomware operations.[3]

---

* Michael A. Mancusi (michael.mancusi@arnoldporter.com) and Kevin M. Toomey (kevin.toomey@arnoldporter.com) are partners at Arnold & Porter Kaye Scholer LLP. Nancy L. Perkins (nancy.perkins@arnoldporter.com) is counsel at the firm. Anthony Raglani (anthony.raglani@arnoldporter.com) and Daniel E. Raymond (daniel.raymond@arnoldporter.com) are senior associates and Kara Ramsey (kara.ramsey@arnoldporter.com) is an associate at the firm.

[1] FinCEN Advisory, FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[2] Press Release, White House, FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

[3] Press Release, U.S. Dep't of the Treasury, Treasury Continues to Counter Ransomware as

Relatedly, the Department of Justice ("DOJ") announced the creation of a National Cryptocurrency Enforcement Team "to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors." DOJ stated that the team will also assist in tracing and recovering assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.[4]

THE FINCEN ADVISORY

FinCEN's Advisory makes clear that, although most cybercriminals require that ransomware payments be made in convertible virtual currencies ("CVCs") (e.g., Bitcoin),[5] nearly every ransomware payment will involve the use of at least one depository institution as an intermediary. Financial institutions are therefore in a position to play a pivotal role in identifying and reporting ransomware attacks and assisting law enforcements efforts to combat ransomware.[6]

To encourage and facilitate effective action by financial institutions, FinCEN has identified four types of ransomware "red flags" to which financial institutions should be alert.

1. Unprecedented CVC Transactions

Financial institutions should be alert for circumstances in which (1) a customer has no or limited history of CVC transactions and then transfers

---

Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471.

[4] Press Release, Department of Justice, Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

[5] According to FinCEN's analysis, as of June 2021, Bitcoin was the most common ransomware-related payment method. FinCEN has also identified Monero as an increasingly used CVC. FinCEN, Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 (Oct. 21, 2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf [hereinafter, FinCEN, Financial Trend Analysis].

[6] The Advisory also makes clear that entities involved in directly or indirectly facilitating ransomware payments, e.g. digital forensic incident response ("DFIR") companies or cybersecurity liability insurance companies ("CICs"), also need to be on guard for these red flags. In the first half of 2021, DFIR firms submitted the majority (roughly 63 percent) of ransomware-related suspicious activity reports ("SARs"). FinCEN, Financial Trend Analysis. Similarly, over that same period, CVC exchanges actually filed 19 percent of ransomware SARs while depository institutions filed 17 percent of ransomware-related SARs. *Id.*

funds to a CVC exchange, or (2) a customer shows little knowledge of CVC but inquires about or purchases CVC—especially in large amounts or through rush requests.

In addition, financial institutions should note anytime a customer provides information that a payment is in response to a ransomware incident.

2. Transactions Involving Digital Forensic Response Companies or Cybersecurity Insurers

Digital forensic incident response ("DFIR") companies frequently assist ransomware victims in responding to ransomware attacks; these companies may also help facilitate the ransomware payment by taking the victim's money, converting it to CVC, and then transferring the CVC to the attacker.[7]

Cybersecurity liability insurance companies ("CICs") also often play a role in ransomware transactions, by reimbursing policy holders for remediation efforts, including the use of a DFIR company.

Financial institutions should be alert for any instance in which an organization sends an irregular transaction to a DFIR or CIC, especially if the DFIR is known to facilitate ransomware payments and especially if the organization is in a sector at a high risk for ransomware attacks (e.g., government, financial, educational, healthcare, etc.). Similarly, financial institutions should monitor transactions where a DFIR or CIC customer receives funds from a counterparty and then quickly sends an equivalent amount to a CVC exchange.

3. Suspicious CVC Transactions

A financial institution should be alert for signs that a customer is:

- Using an encrypted network (e.g., Tor) to communicate with the recipient of the CVC transaction;
- Using a CVC exchange that is based in a foreign country, particularly in a high-risk jurisdiction lacking adequate anti-money laundering ("AML")/countering the financing of terrorism ("CFT") regulations;
- Initiating a transfer of funds using a mixing service;[8]
- Receiving CVC and then initiating multiple rapid trades across multiple CVCs (especially CVCs with enhanced anonymity features) with no apparent purpose, followed by a transaction off the platform;

---

[7] FinCEN, Financial Trend Analysis.

[8] A "mixer" or "tumbler" is a service which combines the CVC of various users and then redistributes those funds to a desired CVC address. Mixers pose AML concerns because they make it harder to track CVC transactions.

or

- Appearing to act as an unregistered money service business by executing large numbers of offsetting transactions between CVCs.

4. Publicly-Identified Ransomware Signs

Additional red flags emerge on an ongoing basis, such as (1) changing "IT enterprise activity connected to ransomware cyber indicators or known cyber threat actors," and (2) whether a customer's CVC address or an address with which a customer conducts transactions is connected to ransomware variants,[9] payments, or related activity. FinCEN identifies several sources of information on these emerging indicators, such as the Cybersecurity & Infrastructure Security Agency Technical Alerts and FinCEN's Cyber Indicator Lists, which it encourages financial institutions to monitor.[10]

CONCLUSION

To help thwart the emerging threats and challenges posed by ransomware, financial institutions must stay current with changing virtual currency technologies and associated trends and typologies and may need to adjust their AML monitoring programs in order to meet their reporting obligations.

---

[9] A ransomware "variant" is a version of ransomware that is named based on changes to the software or to denote which individual or entity is behind the malware. In its most recent analysis, FinCEN has identified 68 ransomware variants linked to SAR filings; the most commonly reported variants were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos. FinCEN, Financial Trend Analysis.

[10] *See, e.g.,* FinCEN Advisory, FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments n.34 (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.