The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

JUNE 2022

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 NUMBER 6 June 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.

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. GAO Urges New Virtual Currency Regulations to Counter Human Trafficking and Drug Cartels

By Sean P. McDonnell and Gina M. Parlovecchio*

The authors discuss a U.S. Government Accountability Office report warning of the role that virtual currencies continue to play in human and drug trafficking and urging tighter regulation of certain kinds of virtual currency transactions.

The U.S. Government Accountability Office ("GAO") has issued an 84-page report[1] warning of the role that virtual currencies continue to play in human and drug trafficking and urging tighter regulation of certain kinds of virtual currency transactions.

The report specifically identifies gaps in registration requirements for virtual currency kiosks—commonly described as "Crypto ATMs"—that may hamper law enforcement's ability to investigate money laundering, drug and human trafficking and other criminal activity.

To address this issue, GAO recommends that the Financial Crimes Enforcement Network ("FinCEN") and Internal Revenue Service ("IRS") review the existing registration requirements applicable to virtual currency kiosks and begin to require additional data from registered kiosk operators.

Given GAO's role as a key federal watchdog agency, its report is likely to further bolster ongoing efforts by the Biden administration and the U.S. Treasury Department to implement more stringent regulations of virtual currencies across a variety of settings.

Persons who are operating or considering operating money services businesses that facilitate virtual currency transactions should be building compliance programs and enhancing internal controls now to anticipate and prepare for increased regulatory and law enforcement scrutiny.

---

[*] Sean P. McDonnell (smcdonnell@mayerbrown.com) is a partner in Mayer Brown's office in Washington, D.C., and a member of the global Litigation & Dispute Resolution practice. Gina M. Parlovecchio (gparlovecchio@mayerbrown.com) is a partner in the firm's New York office and a member of the global White Collar Defense & Compliance and Regulatory & Investigations practices.

[1] https://www.gao.gov/products/gao-22-105462.

THE REPORT'S FINDINGS

Statistical Support

Federal law enforcement agencies have long raised concerns about the potential for virtual currencies to facilitate criminal activity, particularly cross-border offenses such as sanctions evasion, money laundering and human and drug trafficking. The GAO's recent report—a public version of a law enforcement sensitive document that was first circulated within government in September 2021—provides some statistical support for that assessment.

According to the GAO, the number of filed suspicious activity reports involving virtual currency and suspected trafficking activities increased fivefold (from 252 to almost 1,432) from calendar year 2017 to 2020. Virtual currency seizures are also up significantly; in 2021, the Department of Justice ("DOJ") seized more than $3.5 billion in virtual currency through civil forfeiture processes. Approximately $1 billion of that amount was composed of proceeds from illicit activity conducted on Silk Road, a Dark Web marketplace that was shut down following a DOJ investigation in 2016.

Moving Targets

Despite these significant seizures, GAO remains pessimistic about the ability of law enforcement to permanently disrupt virtual currency-facilitated criminal transactions involving the Dark Web. As the report explains, "the prevalence of smaller Dark Web marketplaces creates stability in the overall dark market for illicit purchases because when law enforcement shuts down one marketplace, criminals can easily move operations to other established marketplaces."

The GAO report also details the ongoing, systematic use of virtual currency to facilitate money laundering activities by drug cartels and other transnational criminal organizations. According to GAO, "transnational criminal organizations are increasingly using virtual currency because of its perceived anonymity and as a more efficient method to move money across international borders." One common laundering method discussed in the report involves the use of virtual currency kiosks to convert bulk amounts of illicit cash into virtual currency, which is then moved abroad (eliminating the detection risk inherent in smuggling bulk cash across borders).

Spotty Registration and Compliance

Since 2013, FinCEN guidance has provided that any party that accepts or transmits virtual currency, or buys or sells virtual currency, will be considered a money transmitter under the terms of the Bank Secrecy Act ("BSA") and is subject to obligations to employ "Know Your Customer" measures, report suspicious transactions to FinCEN, file currency transaction reports for fiat transactions of $10,000 or more in cash and maintain an effective Anti-Money Laundering/Combating the Financing of Terrorism ("AML/CFT") program, as all money services businesses ("MSBs") are required to do.

Accordingly, FinCEN and Treasury Department guidance treats virtual currency kiosk operators as MSBs, subject to registration requirements. But compliance with these registration requirements remains spotty. Based on public sources of information, GAO determined that there are currently over 30,000 virtual currency kiosks active in the United States, operated by nearly 290 separate businesses. Of those operators, nearly half remained unregistered.

The GAO report also found that the degree to which kiosk operators comply with existing know-your-customer and anti-money launder regulations varies widely, "with some kiosks implementing weak customer identification standards or not complying at all with BSA obligations." According to GAO, law enforcement efforts to identify unregistered or non-compliant kiosks have been hindered by gaps in the types of data that FinCEN collects as part of the registration process. Though kiosk operators are generally required to register as MSBs, they are not required to report the locations of their kiosks to FinCEN. As a result, law enforcement agencies have a limited ability to distinguish between registered and unregistered kiosks, and they generally lack the means to "identify kiosks in areas that have been designated as high risk for financial crimes and could involve human and drug trafficking." The absence of reliable location information, GAO observed, further impedes law enforcement's ability to prioritize investigations into those kiosks and operators most likely to be involved in illicit activity.

LOOKING FORWARD

To address these issues, the GAO recommends that FinCEN and IRS revise their MSB registration requirements for all virtual currency exchanges and administrators that operate virtual currency kiosks, including by adding a requirement that operators identify all of the specific locations of their kiosks. Although FinCEN and IRS have not yet officially announced any changes to the registration requirements, the GAO report notes that both agencies "concurred with the recommendation," suggesting that rule changes may be imminent. The GAO report is also part of a broader trend of increased enforcement attention for virtual currencies generally.

Based on the foregoing, we anticipate that FinCEN, IRS and other components of the U.S. Treasury Department will continue to ramp up regulatory scrutiny of virtual currency exchanges and kiosk operators, including by strengthening existing MSB registration requirements. We also expect federal law enforcement agencies will devote increasing amounts of resources to examining those operators that they perceive to be skirting the rules.

Indeed, the DOJ has already begun to criminally charge unlicensed operators of virtual currency kiosks who fail to meet FinCEN and U.S. Treasury's registration and reporting requirements.

MSBs that facilitate virtual currency transactions should be building compliance programs and enhancing internal controls now to anticipate and prepare for this increased regulatory and law enforcement scrutiny.